Decomposition in Galois extensions

Exercise 1. [Cyclotomic extensions]

Let $n \geq 3$ be an integer, $K = \mathbb{Q}(\zeta_n)$ and p a prime number. Let $\chi : \mathrm{Gal}(K/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$ be the isomorphism such that for $\sigma \in \mathrm{Gal}(K/\mathbb{Q}), \sigma(\zeta_n) = \zeta_n^{\chi(\sigma)}$.

1. Show that p is ramified in K if and only if $p \mid n$. In that case, compute $e(\mathfrak{p}/p)$ and $f(\mathfrak{p}/p)$ for any prime $\mathfrak{p}$ of $\mathcal{O}_K$ above p, and also g_p, the number of prime ideals above p.
2. Assume that $p \nmid n$. Compute $\chi(\mathrm{Frob}_p)$, $f(\mathfrak{p}/p)$ and g_p for any prime $\mathfrak{p}$ of $\mathcal{O}_K$ above p.

Exercise 2. [A concrete example] Let $\zeta = \zeta_{15}$ and $K = \mathbb{Q}(\zeta)$.

1. Show that $\mathfrak{p} = (2, \zeta^4 + \zeta + 1)$ is a prime ideal of $\mathcal{O}_K$ above 2, and give $e(\mathfrak{p}/2)$ and $f(\mathfrak{p}/2)$.
2. What are the decompositions of $3\mathcal{O}_K$ and $5\mathcal{O}_K$?
3. Compute the decomposition and inertia subgroups $D(\mathfrak{p}/2)$ and $I(\mathfrak{p}/2)$. Do the same for 3 and 5.

Exercise 3. [Inertia and decomposition groups]

Let L/K be a Galois extension of number fields, and $\mathfrak{p}$ a non-zero prime ideal of $\mathcal{O}_K$. Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_L$ above $\mathfrak{p}$ and write e, f and g the ramification index and the inertial degree of $\mathfrak{P}/\mathfrak{p}$, and the number of primes of $\mathcal{O}_L$ above $\mathfrak{p}$ respectively.

1. Recall the definitions of the decomposition and inertia subgroups of $\mathfrak{P}/\mathfrak{p}$, and give their orders in terms of e, f, g.
2. Describe theses groups for every prime number p when $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{d})$.
3. Let $\mathfrak{P}_D = \mathfrak{P} \cap L^{D(\mathfrak{P}/\mathfrak{p})}$ and $\mathfrak{P}_I = \mathfrak{P} \cap L^{I(\mathfrak{P}/\mathfrak{p})}$.
   (a) Write the inclusions between the fields $K, L, L^{I(\mathfrak{P}/\mathfrak{p})}$ and $L^{D(\mathfrak{P}/\mathfrak{p})}$.
   (b) Show that $[L^{D(\mathfrak{P}/\mathfrak{p})} : K] = g$ and that $\mathfrak{p}$ splits completely in $L^{D(\mathfrak{P}/\mathfrak{p})}$.
   (c) Show that $[L^{I(\mathfrak{P}/p)} : L^{D(\mathfrak{P}/p)}] = f$ and that $\mathfrak{P}_D$ is inert in $L^{I(\mathfrak{P}/\mathfrak{p})}$.
   (d) Show that $[L : L^{I(\mathfrak{P}/\mathfrak{p})}] = e$ and that $\mathfrak{P}_I$ is totally ramified in L.
4. Let K' be an intermediate extension between K and L, and let $\mathfrak{p}' = \mathfrak{P} \cap K'$. Show that $\mathfrak{p}'$ is unramified over $\mathfrak{p}$ if and only if $K' \subset L^{I(\mathfrak{P}/\mathfrak{p})}$, and that $\mathfrak{p}'$ splits completely over $\mathfrak{p}$ if and only if $K' \subset L^{D(\mathfrak{P}/\mathfrak{p})}$.

Exercise 4. [Computing Galois groups with Frobenius]

1. Let P be a monic irreducible polynomial in $\mathbb{Z}[X]$, K its splitting field over $\mathbb{Q}$ and p a prime number such that $\overline{P} \in \mathbb{F}_p[X]$ is separable.
   Write
   $$\overline{P} = \pi_1 \dots \pi_g$$
   the decomposition of $\overline{P}$ in irreducible factors, and let $n_i = \deg \pi_i$.
   Show that $\mathrm{Gal}(K/\mathbb{Q})$, seen as a subgroup of $\mathfrak{S}_{\deg P}$, contains a permutation of type $(n_1, \dots, n_r)$.

2. Let $P = X^5 - X - 1$. Show that P is irreducible in $\mathbb{Q}[X]$ and that its Galois group is $\mathfrak{S}_5$.

Exercise 5. [Biquadratic extensions]

Let m, n be distinct square-free integers, p a prime number and let $L = \mathbb{Q}(\sqrt{m}, \sqrt{n})$. Write $K_1 = \mathbb{Q}(\sqrt{m})$, $K_2 = \mathbb{Q}(\sqrt{n})$ and $K_3 = \mathbb{Q}(\sqrt{k})$ with $k = \frac{mn}{\gcd(m,n)^2}$.

1. Show that p is totally ramified in L if and only if it is ramified in K_1, K_2 and K_3. When does this happen ?
2. Show that p splits completely in L if and only if it splits completely in K_1, K_2 and K_3. When does this happen ?
3. Can p be inert in L ?
4. What are the possible decompositions of $p\mathcal{O}_L$?