Math 204A (Number Theory), UCSD, fall 2020
Problem Set 5 – due Thursday, November 12, 2020

1. In class, we used the fact that if K, L are number fields such that $K \cap L = \mathbb{Q}$ and the discriminants of K and L are relatively prime, then an integral basis for $\mathcal{O}_{KL}$ can be obtained by taking an integral basis $\alpha_1, \dots, \alpha_m$ of $\mathcal{O}_K$ and an integral basis $\beta_1, \dots, \beta_n$ of $\mathcal{O}_L$, then forming the products $\alpha_i \beta_j$ for $1 \leq i \leq m, 1 \leq j \leq n$.
   (a) Read a proof of this. No answer required except a citation.
   (b) Give an example with K, L quadratic in which $K \cap L = \mathbb{Q}$, the discriminants of K and L are not relatively prime, and this recipe *does not* an integral basis for $\mathcal{O}_{KL}$.
   (c) Give an example with K, L quadratic in which $K \cap L = \mathbb{Q}$, the discriminants of K and L are not relatively prime, and this recipe *does* give an integral basis for $\mathcal{O}_{KL}$.

2. (a) Show that for any number field $K \neq \mathbb{Q}$, at least one prime of $\mathbb{Q}$ must ramify in K. (Hint: recall what we know about discriminants from earlier homework.)
   (b) Let $K/\mathbb{Q}$ be a non-Galois cubic extension with squarefree discriminant, let L be the Galois closure of K, and let M be the quadratic subextension of L. Prove that no prime of M ramifies in L. (Optional: do the same for $K/\mathbb{Q}$ of degree n with Galois group S_n.)

3. Let K be the number field $\mathbb{Q}[\alpha]/(\alpha^3 - \alpha - 1)$. Let L be the Galois closure of K. The previous exercise implies that no prime of $\mathbb{Q}(\sqrt{-23})$ ramifies in L. Check this explicitly for the prime above 23. (Hint: you may query SageMath for the ring of integers of L.)

4. For each of the following statements, find an example of a prime p and two quadratic extensions K and L of $\mathbb{Q}$ exhibiting this particular behavior. Your four examples should be distinct.
   (a) The prime p can be totally ramified in K and L without being totally ramified in KL.
   (b) The fields K and L can both contain unique primes over p, while KL does not.
   (c) The prime p can be (unramified and) inert in both K and L without being inert in KL.
   (d) There can be (unramified) primes over p of inertia degree 1 in both K and L, but not in KL.

5. Let L/K be a finite separable extension of fields with Galois closure M and Galois group G. Put $H = \mathrm{Gal}(M/L)$. Prove that $\bigcap_{x \in G} x^{-1} H x = \{e\}$.

6. Let L/K be an extension of number fields with Galois closure M and Galois group G. Put $H = \mathrm{Gal}(M/L)$.

(a) Let $\mathfrak{p}$ be a prime ideal of K. Let $\mathfrak{q}$ be a prime ideal of M above $\mathfrak{p}$. Show that the action of G on the prime ideals of M above $\mathfrak{p}$ induces a bijection between the double coset space $H \backslash G / G_{\mathfrak{q}}$ and the set of primes of L above $\mathfrak{p}$ (this was stated in lecture).

(b) Suppose that $\mathfrak{p}$ does not ramify in M. Show that the inertia degree of the prime of L above $\mathfrak{p}$ corresponding to the double coset $HxG_{\mathfrak{q}}$ equals the index $[G_{\mathfrak{q}} : G_{\mathfrak{q}} \cap x^{-1}Hx]$.

(c) Optional: extend (b) to the case where $\mathfrak{p}$ may ramify in M.

7. With notation as in the previous exercise, assume that every element of G occurs as the Frobenius element for some unramified prime of M (this is a corollary of the Chebotarev density theorem). Show that if every prime of $\mathcal{O}_K$ which does not ramify in M has the property that all of the primes above it in L have the *same* inertial degree, then L/K is Galois. (Hint: the decomposition group of an unramified prime is cyclic, so it has only one subgroup of any given order.)