Math 204A (Number Theory), UC San Diego, fall 2022
Problem Set 5 – due Thursday, November 3, 2022

Submit *at most five* of the listed problems.

1. For p a prime number, a number field K is *monogenic at* p if there exists some $\theta \in \mathfrak{o}_K$ such that the ring homomorphism $\mathbb{Z}[x] \to \mathfrak{o}_K/p\mathfrak{o}_K$ taking x to the class of θ is surjective. Prove that if there exists a single prime of $\mathfrak{o}_K$ above p (ramified or not), then K is monogenic at p.

2. Produce (e.g., by looking in LMFDB) an example of a number field K for which
$$\mathfrak{o}_K/2\mathfrak{o}_K \cong \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2,$$
then use this to show that K is not monogenic at 2.

3. Let K be a number field and let R be a subring of $\mathfrak{o}_K$ which spans K as a $\mathbb{Q}$-vector space (i.e., an *order* of K). Let p be a prime number such that for every prime $\mathfrak{p}$ of $\mathfrak{o}_K$ above p,
   (i) the inertia degree is 1, and
   (ii) there exist some $\lambda \in R$ such that $v_{\mathfrak{p}}(\lambda) = 1$ and $v_{\mathfrak{q}}(\lambda) = 0$ for all primes $\mathfrak{q} \neq \mathfrak{p}$ of $\mathfrak{o}_K$ above p.

   Prove that the index $[\mathfrak{o}_K : R]$ is not divisible by p. (This generalizes the argument used for cyclotomic fields.)

4. Neukirch, exercise I.9.1: Let L/K be a Galois extension of number fields such that $\mathrm{Gal}(L/K)$ is not cyclic. Prove that there are only finitely many primes of K that remain inert in L.

5. Neukirch, exercise I.9.3: Let L/K be a (not necessarily Galois) extension of prime degree p with solvable Galois group. Suppose that $\mathfrak{p}$ is a prime ideal of K which does not ramify in L. Prove that if there are at least two primes of L above $\mathfrak{p}$ of inertia degree 1, then $\mathfrak{p}$ splits completely in L.

6. 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. (You may use SageMath to verify the asserted properties.)
   (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.

7. 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 $\bigcap_{x \in G} x^{-1}Hx = \{e\}$.

8. 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 $\mathfrak{p}$.

   (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.