

HOMEWORK 5

DUE FRIDAY, NOVEMBER 8, 2024 AT 11:59PM

The homework is due in Gradescope at the stated time. You may submit handwritten text (scanned from paper or written on a tablet) or a typed PDF (e.g., created using LaTeX). If you choose the handwritten option, you have to also submit a hardcopy in class or put it in my mailbox.

Collaboration and research is fine, as long as you do the following.

- Try the problems yourself first!
- Write the solutions in your own words.
- Acknowledge all sources and collaborators.

1. Let L/K be an extension of number fields with Galois closure M and Galois group G . Set $H = \text{Gal}(M/L)$.
 - (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 .
2. 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.)
3. Let $N \geq 3$ be an integer and let Φ_N be the N -th cyclotomic polynomial. Prove that for every integer m , every prime divisor of $\Phi_N(m)$ not dividing N is congruent to 1 modulo N .

4. In class, I stated that for every number field K , there exist infinitely many primes p which split completely in K . Prove this for the cyclotomic field $K = \mathbb{Q}(\zeta_N)$ *without* using Dirichlet or Chebotaryov. (Hint: Channel your inner Euclid. Suppose there are only finitely many, take their product...)
5. Let L/K be an extension of number fields with Galois closure $\tilde{L}$. Let $\mathfrak{p}$ be a prime of K .
- (a) Prove that if $\mathfrak{p}$ is unramified in L , then it is unramified in $\tilde{L}$ also.
 - (b) Prove that if $\mathfrak{p}$ is unramified and totally split in L , then it is totally split in $\tilde{L}$ also.
- (Hint for both parts: put $G = \text{Gal}(\tilde{L}/K)$ and $H = \text{Gal}(\tilde{L}/L)$. Pick a prime $\mathfrak{q}$ of M above $\mathfrak{p}$ and consider how $G_{\mathfrak{q}}$ or $I_{\mathfrak{q}}$ intersects the various conjugates of H .)
6. Let m be an integer which is not a perfect square, and put $K = \mathbb{Q}(m^{1/4})$. Let L be the Galois closure of $K/\mathbb{Q}$. Let p be an odd prime not dividing m and let $\mathfrak{q}$ be a prime above p in L . For each possible value for the decomposition group $G_{\mathfrak{q}}$, describe the corresponding splitting of p in K .
7. (a) Let k be a field. Prove that the ring of formal power series $k[[t]]$ is a discrete valuation ring.
- (b) Prove that the subring of $\mathbb{R}[[t]]$ consisting of power series with positive radius of convergence is a discrete valuation ring.