Math 223a: Algebraic Number Theory

Fall 2020

Problem set #5

due Friday, October 9 at 10:30am

Problem 1. Let $L|K$ be a degree n extension of number fields. Assume that its Galois closure M has Galois group $\mathrm{Gal}(M|K) \cong S_n$.

a) What is the density of prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ (ordered by norm) that split completely in $\mathcal{O}_L$?

b) What is the density of prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ (ordered by norm) that remain inert in $\mathcal{O}_L$?

Problem 2. Let K be a field extension of $\mathbb{Q}$ and let $n \geqslant 1$. Show that the following are equivalent:

a) For any two prime numbers p, p' such that $p \equiv \pm p' \mod n$, the ideals (p) and (p') split in the same way in $\mathcal{O}_K$.

b) The field K is contained in $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$.

Problem 3. Which nonzero integers a satisfy the following property?

There exists an integer $n \geqslant 1$ such that any two prime numbers p, p' with $p \equiv \pm p' \mod n$ split in the same way in $\mathbb{Q}(\sqrt{a})$.

Problem 4. Show that there is a number field K satisfying the following two properties:

a) There is an integer $n \geqslant 1$ such that for all primes $p \equiv p' \mod n$, there is a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ dividing p with residue field $\kappa(\mathfrak{p}) = \kappa(p) = \mathbb{F}_p$ if and only if there is a prime ideal $\mathfrak{p}'$ of $\mathcal{O}_K$ dividing p' with residue field $\kappa(\mathfrak{p}') = \kappa(p') = \mathbb{F}_{p'}$.

b) The field K is not contained in $\mathbb{Q}(\zeta_m)$ for any m.

(In more elementary terms: There is an irreducible polynomial $f(X) \in \mathbb{Z}[X]$ such that whether $f(X)$ has a root modulo p depends only on $p \mod n$ for some $n \geqslant 1$, but the splitting field of $f(X)$ is not contained in $\mathbb{Q}(\zeta_m)$ for any m.)

Problem 5. Let $K \subseteq \mathbb{Q}(\zeta_\infty)$ be a finite field extension of $\mathbb{Q}$. Show that a prime number p divides the conductor of K (smallest $n \geqslant 1$ such that $K \subseteq \mathbb{Q}(\zeta_n)$) if and only if it divides the discriminant of K.