

Algebraic Number Theory
Math 514B Spring 2008

Problem Set 1

Due: Tuesday, Jan. 29th

1. a) Let $K \subset L$ be a finite extension of number fields, and let \tilde{L} be the Galois closure of L over K . Show that $Spl_{L/K} = Spl_{\tilde{L}/K}$. (Hint: Let \mathfrak{p} be a prime of K , and let P be a prime of L over \mathfrak{p} . Let $K_{\mathfrak{p}}$ be the \mathfrak{p} -adic completion of K , and let $\bar{K}_{\mathfrak{p}}$ be its algebraic closure. Pick an embedding $\alpha : L \hookrightarrow \bar{K}_{\mathfrak{p}}$ as K -algebras. Show that the condition that a prime \mathfrak{p} is in either Spl is equivalent to saying that every conjugate of L has the property that its image under α is contained in $K_{\mathfrak{p}}$.)

- b) Consider the result that if L, E are finite Galois extensions of a number field K , then

$$Spl_{L/K} \subset Spl_{E/K} \iff E \subset L.$$

Does this assertion remain true if L is permitted not to be Galois? If E is permitted not to be Galois? If both are permitted not to be Galois? In each case, either give a proof or a counterexample.

2. Fix a rational prime p .

- a) Show that for each positive divisor n of $p-1$ (i.e. $p \equiv 1 \pmod{n}$) there exists a cyclic Galois extension K/\mathbb{Q} of degree n such that p is the only finite ramified prime.
- b) Explicitly write down a cubic polynomial that generates a normal cubic extension K of \mathbb{Q} for which 7 is the only finite ramified prime.
- c) Explicitly write down a cubic polynomial that generates a normal cubic extension K of \mathbb{Q} for which 3 is the only finite ramified prime.

3. Fix an integer $n > 1$ along with a rational prime p not dividing n . Denote $R = \mathbb{Z}[\zeta_n]$ as the integral closure of \mathbb{Z} in $K = \mathbb{Q}(\zeta_n)$, and \mathfrak{p} as a prime in R lying over p .

- a) Show that $R/\mathfrak{p}R \cong \mathbb{F}_p[\zeta_n]$, and that p is unramified in R .
- b) Show that $\zeta_n \in \mathbb{F}_p$ if and only if $p \equiv 1 \pmod{n}$. Conclude that p splits completely in R if and only if $p \equiv 1 \pmod{n}$.