Algebraic Number Theory
MATH 512

Assignment 2

1. Prove Corollary 5 of the course notes. You may assume Proposition 4.

2. Suppose A is a Dedekind domain with fraction field K, L is a finite Galois extension of K, and B is the integral closure of A in L. Assume that $B = A[\alpha]$ for some $\alpha \in B$, and let $f(x)$ be the minimal polynomial for α over K. Let $\mathfrak{p}$ be a prime of A that is unramified in B. Show that $\mathfrak{p}$ splits completely in B (i.e. there are $[L : K]$ primes of L above $\mathfrak{p}$) if and only if $f(x)$ has a root mod $\mathfrak{p}$.

3. Let $L = \mathbb{Q}(\zeta_{12})$. Throughout this question, you may use the equality of polynomials

$$x^{12} - 1 = (x-1)(x+1)(x^2+x+1)(x^2+1)(x^2-x+1)(x^4-x^2+1) \qquad (1)$$

and the fact that if $h(x)$ is one of the first five factors in the right-hand side of (1), then there is a divisor $m < 12$ of 12 such that $h(x)|x^m - 1$. You may also assume that $x^4 - x^2 + 1$ is the minimal polynomial for ζ_{12} over $\mathbb{Q}$.

(a) We know from class that the primes that ramify in L are 2 and 3. Use Dedekind's Theorem to find the ramification indices and residue degrees.

(b) For p not equal to 2 or 3, show that p splits completely in L if and only if $x^4 - x^2 + 1$ has a root mod p.

(c) Suppose $p \equiv 1 \bmod 12$. Show that there exists $a \in \mathbb{Z}$ such that $p|a^4 - a^2 + 1$.

(d) (i) Conversely, assume $p|a^4 - a^2 + 1$. Show first that the order of $\overline{a}$ in $\mathbb{F}_p^\times$ divides 12.

(ii) Suppose that the order is less than 12. Deduce that $a^{12} - 1 \equiv 0 \bmod p^2$, and show similarly that $(a+p)^{12} - 1 \equiv 0 \bmod p^2$.

(iii) Given that p divides neither a nor 12, derive a contradiction from (ii), so that you may conclude that the order of $\overline{a}$ in $\mathbb{F}_p^\times$ is 12.

(iv) Deduce that $p \equiv 1 \bmod 12$.

(The above exercise shows that the primes that split completely in L are exactly those congruent to 1 mod 12.)

4. Let M/K be a Galois extension of number fields, and L/K an intermediate Galois extension. Fix a prime $\mathfrak{P}$ of M and let $\mathfrak{q}$ and $\mathfrak{p}$ be the primes of L and K respectively below $\mathfrak{P}$. Let D be the decomposition group of $\mathfrak{q}|\mathfrak{p}$ and E that of $\mathfrak{P}|\mathfrak{p}$. Show that if $e(\mathfrak{P}|\mathfrak{q}) = f(\mathfrak{P}|\mathfrak{q}) = 1$, then restriction gives an isomorphism $E \to D$.

5. In an extension L/K of number fields, we say that a prime $\mathfrak{p}$ is non-split if there is only one prime of L above $\mathfrak{p}$. Prove that if L/K is a non-cyclic Galois extension, then only finitely many primes of K are non-split in L.