MAT415: HOMEWORK SET #4

DUE: MONDAY MARCH 30, 2015

The following problems build on each other. If you can't figure out a problem, feel free to assume it and move on to the next one.

(1) Let p be an odd prime, and let $K_p = \mathbb{Q}[x]/(f_p(x))$ where

$$f_p(x) = \sum_{i=0}^{p-1} x^i.$$

Prove that $f_p(x)$ is irreducible using Eisenstein's criterion for $f_p(x+1)$. Hence K_p is a field. It is called the p'th cyclotomic field.

(2) Prove that K_p is Galois over $\mathbb{Q}$ with Galois group naturally isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times$ given by $a \to \sigma_a$ where $\sigma_a(x) = x^a$.

(3) Prove that $(1-x)$ has norm p, and that $(1-x)^p$ is divisible by p in the ring of integers $\mathcal{O}_{K_p}$. Conclude that p is totally ramified in K_p.

(4) By computing the Discriminant of $\mathbb{Z}[x]$, prove that $\mathbb{Z}[x]$ has index a power of p in $\mathcal{O}_{K_p}$.

(5) Using the basis $(1-x)^i, i = 0, 1, 2 \ldots, p-2$, or otherwise, prove that $\mathbb{Z}[x] = \mathcal{O}_{K_p}$.

(6) Let

$$p_* = \begin{cases} p & \text{if } p \equiv 1 \mod 4 \\ -p & \text{otherwise.} \end{cases}$$

Prove that $\mathbb{Q}(\sqrt{p_*})$ is the unique quadratic subfield of K_p. **Hint: Use Galois theory, and in particular the automorphism in the Galois Group corresponding to complex conjugation**

(7) For a prime number $q \neq p$, proe that q is unramified, prove that the number of primes above q in K_p, and the size of their decomposition groups, depend only on $q \mod p$.

(8) Using the above, prove that q splits in $\mathbb{Q}(\sqrt{p_*})$ iff q is a quadratic residue modulo p.

(9) Prove the law of quadratic reciprocity: q is a quadratic residue modulo p iff p_* is a quadratic residue modulo q.