Math 620, Fall, 1999
Homework Set 4: Cyclotomic Fields
due Friday, October 22, 1999

For purposes of this exercise set, let $\theta = e^{2\pi i/7}$, a primitive 7th root of unity, and let $\alpha = \theta + \theta^{-1}$.

1. Show that the cyclotomic field $\mathbb{Q}(\theta)$ contains a unique subfield E with $[E : \mathbb{Q}] = 3$, and that E is Galois over $\mathbb{Q}$ (with cyclic Galois group).

2. Show further that $E = \mathbb{Q}(\alpha)$ and that $\mathbb{Q}(\theta) = \mathbb{Q}(\alpha, \sqrt{-7})$. (Use Janusz, theorem 11.1, p. 59.)

3. Show that the minimal polynomial of α over $\mathbb{Q}$ is $f(x) = x^3 + x^2 - 2x - 1$. Using (1) and (2), deduce that the ring of algebraic integers in E is $\mathbb{Q}[\alpha]$ (hint: the integers in E have to be integers in $\mathbb{Q}(\theta)$ invariant under complex conjugation) and that the polynomial $f(x)$ must have a discriminant which is a perfect square and a power of 7. (In fact the discriminant of f is 49.) Deduce that 7 is the only prime of $\mathbb{Z}$ ramified in E.

4. If $p \neq 7$ is a prime of $\mathbb{Z}$, consider its splitting in E, $\mathbb{Q}(\sqrt{-7})$, and $\mathbb{Q}(\theta)$. Show that in $\mathbb{Q}(\sqrt{-7})$, p is either inert (with relative degree 2) or splits into two prime factors, depending on the Legendre symbol $\left(\frac{-7}{p}\right)$, and (using quadratic reciprocity) give a formula for this in terms of congruences. Similarly show that in E, p is either inert (with relative degree 3) or splits into three prime factors, and that in $\mathbb{Q}(\theta)$, if p splits into g prime factors each with relative degree f, the possibilities are $g = 6$ and $f = 1$, $g = 3$ and $f = 2$, $g = 2$ and $f = 3$, and $g = 1$ and $f = 6$. See if you can correlate the way p splits in the three fields and relate this to the arithmetic of the field $\mathbb{F}_p$. Also see if you can give examples of all 4 types of splitting, or if not, show why one type is excluded.