Homework 4 for Math 581F
Due FRIDAY October 26, 2007

Each problem has equal weight, and parts of problems are worth the same amount as each other.

1. (a) Find by hand and with proof the ring of integers of each of the following two fields: $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(i)$.
   (b) Find the ring of integers of $\mathbb{Q}(x^5 + 7x + 1)$ using a computer.

2. Let $\mathcal{O}_K$ be the ring of integers of a number field K, and let $p \in \mathbb{Z}$ be a prime number. What is the cardinality of $\mathcal{O}_K/(p)$ in terms of p and $[K : \mathbb{Q}]$, where (p) is the ideal of $\mathcal{O}_K$ generated by p?

3. Explicitly factor the ideals generated by each of 2, 3, and 13 in the ring of integers of $\mathbb{Q}(\sqrt[3]{2})$. (Thus you'll factor three separate integral ideals as products of prime ideals.) You may assume that the ring of integers of $\mathbb{Q}(\sqrt[3]{2})$ is $\mathbb{Z}[\sqrt[3]{2}]$, but do *not* simply use a computer command to do the factorizations.

4. Let $K = \mathbb{Q}(\zeta_{13})$,where ζ_{13} is a primitive 13th root of unity. Note that K has ring of integers $\mathcal{O}_K = \mathbb{Z}[\zeta_{13}]$.
   (a) Factor 2, 3, 5, 7, 11, and 13 in the ring of integers $\mathcal{O}_K$. You may use a computer.
   (b) For $p \neq 13$, find a conjectural relationship between the number of prime ideal factors of $p\mathcal{O}_K$ and the order of the reduction of p in $(\mathbb{Z}/13\mathbb{Z})^*$.
   (c) Compute the minimal polynomial $f(x) \in \mathbb{Z}[x]$ of ζ_{13}. Reinterpret your conjecture as a conjecture that relates the degrees of the irreducible factors of $f(x) \pmod{p}$ to the order of p modulo 13. Does your conjecture remind you of quadratic reciprocity?

5. Let p be a prime. Let $\mathcal{O}_K$ be the ring of integers of a number field K, and suppose $a \in \mathcal{O}_K$ is such that $[\mathcal{O}_K : \mathbb{Z}[a]]$ is finite and coprime to p. Let $f(x)$ be the minimal polynomial of a. We proved in class that if the reduction $\overline{f} \in \mathbb{F}_p[x]$ of f factors as
$$\overline{f} = \prod g_i^{e_i},$$
where the g_i are distinct irreducible polynomials in $\mathbb{F}_p[x]$, then the primes appearing in the factorization of $p\mathcal{O}_K$ are the ideals $(p, g_i(a))$. In class, we did not prove that the exponents of these primes in the factorization of $p\mathcal{O}_K$ are the e_i. Prove this.

6. (a) Give an example of a cubic *Galois* extension K of $\mathbb{Q}$. Use Sage to factor each prime $p < 100$ (or more) in $\mathcal{O}_K$ and record the number of prime factors of each p.
   (b) Give an example of a cubic *non-Galois* extension K of $\mathbb{Q}$. Use Sage to factor each prime $p < 100$ (or more) in $\mathcal{O}_K$ and record the number of prime factors of each p.
   (c) Come up with a more refined conjecture about the proportion of primes p for which the number of prime factors is 1, 2 or 3 in each of the above two cases.