Math 620, Fall, 1999
Take-Home Final Problems
due Monday, December 20, 1999

Instructions: Your may use books and notes and refer to theorems proved in class or in the book. However, you should do your own work.

1. In this problem, you may use the facts that in the field $K = \mathbb{Q}(\sqrt{-5})$, the ring of integers is $R = \mathbb{Z}[\sqrt{-5}]$, and (cf. Assignment 5) $C(R)$ is of order 2, with generator the class of the prime ideal $\mathfrak{q} = (3, 2 + \sqrt{-5})$. Show that if p is a prime number, then p can be written in the form $p = x^2 + 5y^2$, with x, $y \in \mathbb{Z}$, if and only if either $p = 5$ or else $p \equiv 1$ or 9 (mod 20). (Hint: Study the splitting of p in R. Note that if p splits as $\mathfrak{p}\bar{\mathfrak{p}}$ in R, then there are two sub-cases, the case where $\mathfrak{p}$ (and thus also $\bar{\mathfrak{p}}$) is principal, and the case where it lies in the ideal class of $\mathfrak{q}$. But in the latter case, $\mathfrak{p} = c\mathfrak{q}$ with $c \in K^\times$, and thus $p = N_{K/\mathbb{Q}}(\mathfrak{p}) = N_{K/\mathbb{Q}}(c)N_{K/\mathbb{Q}}(\mathfrak{q}) = 3N_{K/\mathbb{Q}}(c)$, which constrains the value of p. Also observe by reducing the equation $p = x^2 + 5y^2$ mod 5 and mod 4 that if this equation has a solution in integers, then p is a quadratic residue mod 5 and cannot be congruent to 3 mod 4.)

2. Find the fundamental unit for the real quadratic field $K = \mathbb{Q}(\sqrt{10})$, and justify your answer. (Note: the purported answer on page 81 of Janusz is wrong, but the correct answer is easy to find by inspection.) Also show that the class number of K is 2 by using the Minkowski bound and studying the splitting of small primes. Finally, check that your value of the class number is correct by using the Class Number Formula. (Knowledge of the fundamental unit should come in.)

3. Let $K = \mathbb{Q}(\sqrt{-3})$, which contains a primitive cube root of unity, $\omega = (-1 + \sqrt{-3})/2$. You may use the fact that the ring of integers $R = \mathbb{Z}[\omega]$ of K is a Euclidean ring, hence a PID. First classify the non-zero prime ideals $\mathfrak{p}$ of R, or equivalently the irreducible elements of R up to multiplication by 6th roots of unity, (according to the prime numbers $p \in \mathbb{Z}$ that they sit over) by studying the splitting of prime numbers p in R.

Next, consider the extension field $L = K(\sqrt[3]{5})$ of K. Show that L is a cyclic Galois extension of K with Galois group G generated by $\sigma\colon \sqrt[3]{5} \mapsto \omega\sqrt[3]{5}$. Compute the Artin map $\varphi_{L/K}$ for L over K, in the sense of computing $\varphi_{L/K}(\mathfrak{p}) \in G$ for all but finitely many non-zero prime ideals $\mathfrak{p}$ of R.