18.786. (Fall 2011) Homework # 3 (due Tue Oct 4)

1. (Neukirch I.7.1) Let $D > 1$ be a square-free integer and d the discriminant of the real quadratic number field $K = \mathbb{Q}(\sqrt{D})$. Let x_1, y_1 be the uniquely determined rational integer solution of the equation

$$x^2 - dy^2 = -4 \quad (\text{resp. } x^2 - dy^2 = 4)$$

for which $x_1, y_1 > 0$ are as small as possible if $x^2 - dy^2 = -4$ has rational integer solutions (resp. otherwise). Then show that

$$\epsilon_1 = \frac{x_1 + y_1\sqrt{d}}{2}$$

is a fundamental unit of K. (The pair of equations $x^2 - dy^2 = \pm 4$ is called Pell's equation.)

2. (Neukirch I.7.4) Let ζ be a primitive 5-th root of unity. Show that the units in $\mathbb{Z}[\zeta]$ are

$$\{\pm\zeta^k(1+\zeta)^n | 0 \le k < 5, \ n \in \mathbb{Z}\}.$$

3. Find a unit in $\mathbb{Q}(\sqrt[3]{6})$. Find a unit in $\mathbb{Q}(\sqrt[3]{22})$ as well. (I mean, a unit in the ring of integers for each field different from $\{\pm 1\}$. You may get help from a computer/calculator if you like, but be sure to explain your method whether it's based on theory, algorithm, or something else.)

4. Prove that $h_{\mathbb{Q}(\sqrt{-5})} = 2$ and that $h_{\mathbb{Q}(\sqrt{-23})} = 3$. (A similar problem is in Milne's Exercise 4.4. Let me cite his hint for you: Compute the Minkowski bound to find a small set of generators for the class group. In order to show that two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent, it is often easiest to verify that $\mathfrak{a}\mathfrak{b}^{m-1}$ is principal, where m is the order of $\mathfrak{b}$ in the class group.)

5. Let ζ be a primitive p-th root of unity. We accept that $\mathbb{Z}[\zeta]$ is the ring of integers for $\mathbb{Q}(\zeta)$. Show that $\frac{\zeta^s - 1}{\zeta^t - 1} \in \mathbb{Z}[\zeta]^\times$ (where $s, t \ge 1$ and p does not divide st) and that the prime ideal $(p) \subset \mathbb{Z}$ is totally ramified in $\mathbb{Q}(\zeta)$. (You may try to show $(p) = (1-\zeta)^{p-1}$ as ideals of $\mathbb{Z}[\zeta]$. Don't forget to check that $(1-\zeta)$ is a prime ideal of $\mathbb{Z}[\zeta]$.)

6. (a variant of Neukirch I.8.3) Let L/K and L'/K be finite extensions of number fields. (One could consider the case where K is the field of fractions of a Dedekind domain and L, L' are finite separable over K.) Show that a prime ideal $\mathfrak{p}$ of K (of $\mathcal{O}_K$, to be precise) is totally split in both L/K and L'/K if and only if it is totally split in the composite extension LL'/K. (Note: By using this you can easily solve Neukirch I.8.4, which is sometimes useful. You need not write the solution for I.8.4.)

$***$ As I did not have enough time to set up terminology, let me do it here. The setup is that we have $A \subset K$, $B \subset L$ as in class, where L is a finite separable extension of L, A is Dedekind and B is the integral closure of A in L. Let $\mathfrak{p}$ be a nonzero prime of A and $\mathfrak{P} \supset \mathfrak{p}$ a prime of B. We say

- $\mathfrak{p}$ is **ramified** in L (or in B) if $e_{\mathfrak{P}} = 1$ for some $\mathfrak{P} \supset \mathfrak{p}$.
- $\mathfrak{p}$ **splits** completely (or totally split) in L if $e_{\mathfrak{P}} = f_{\mathfrak{P}} = 1$ for all $\mathfrak{P} \supset \mathfrak{p}$.

$***$ For problem 4, here is another hint. By applying the Minkowski bound, it boils down to examining ideals $\mathfrak{a}$ of $\mathcal{O}_F$ (the ring of integers) with bounded norm. As long as you can find all primes of $\mathcal{O}_F$ with small norms, you can list the finitely many possibilities for $\mathfrak{a}$ by using the fact that if $\mathfrak{a} = \prod_{i=1}^r \mathfrak{P}_i^{e_i}$ then $N(\mathfrak{a}) = \prod_{i=1}^r N(\mathfrak{P}_i)^{e_i}$. The primes of $\mathcal{O}_F$ with small norms can be identified by examining how the ideals (2), (3), ... factorize in $\mathcal{O}_F$.