THE JOHNS HOPKINS UNIVERSITY
Faculty of Arts and Sciences
1 Homework - FALL SESSION 2007
110.617 - Number Theory

1. Show that a non-zero square is never followed by a cube, that is the only integral solution of the equation
$$x^2 + 1 = y^3$$
is the obvious one $x = 0$, $y = 1$.

   Hint: Investigate the equation in $\mathbb{Z}[i]$.

2. Show that $\mathbb{Z}[\sqrt{-2}]$ is a principal ideal domain.

3. Let $K = \mathbb{Q}\sqrt{d}$, with d a square-free integer. Find an integral basis for $\mathcal{O}_K$.

4. Show that every non-zero prime ideal in the ring of integers of a number field contains exactly one integer prime.

5. Let $u_1, u_2, \ldots u_n \in \mathcal{O}_K$ be linearly independent elements over $\mathbb{Q}$ ($K =$ number field, $[K : \mathbb{Q}] = n$, $\mathcal{O}_K =$ ring of integers). Let
$$M = u_1\mathbb{Z} + \ldots + u_n\mathbb{Z}, \qquad m = [\mathcal{O}_K : M].$$
Prove that
$$d_{K/\mathbb{Q}}(u_1, \ldots, u_n) = m^2 d_K$$
where d_K is the discriminant of K and $d_{K/\mathbb{Q}}(u_1, \ldots, u_n) := (\det(u_j^{\sigma_i}))^2$, for $\{\sigma_i,\ i = 1, \ldots n\}$ a set of embeddings of K extending a fixed inclusion $\mathbb{Q} \hookrightarrow \bar{\mathbb{Q}}$.

6. Let K and K_1 be two algebraic number fields of degree m and m_1 respectively, over $\mathbb{Q}$. Let $d = GCD(d_K, d_{K_1})$. Show that if $[KK_1 : \mathbb{Q}] = mm_1$, then $\mathcal{O}_{KK_1} \subseteq 1/d\mathcal{O}_K\mathcal{O}_{K_1}$.

   Hint: Show that any $a \in \mathcal{O}_{KK_1}$ can be written as
$$a = \sum_{i,j} \frac{m_{ij}}{r} a_i b_j$$
where $\{a_i\}$ and $\{b_j\}$ are $\mathbb{Z}$-bases of the ring of integers, $r, m_{ij} \in \mathbb{Z}$, $GCD(r, GCD(m_{ij})) = 1$ and $r \mid d_K$ and by symmetry $r \mid d_{K_1}$ (so that $r \mid d$).

7. Find an integral basis for $\mathbb{Q}(\sqrt{2}, \sqrt{-3})$.