Math 661
Algebraic Number Theory
Problem Set 4

(1) Suppose that $\alpha \in \mathcal{O}_K$, where $K$ is an algebraic number field of degree $n$. Suppose that $\text{disc}(1, \alpha, \ldots, \alpha^{n-1})$ is a square free integer. Show that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. (Hint: Relate the discriminant of 1, $\alpha$, $\ldots$, $\alpha^{n-1}$ to the discriminant of a $\mathbb{Z}$-basis of $\text{disc}(O_K)$.)

(2) We will calculate the discriminant of a root $\alpha$ of an irreducible cubic $f(x) = x^3 + ax + b$, where $a$ and $b$ are in $\mathbb{Q}$.
   (a) If $a = 0$, use the fact that $f'(\alpha) = 3\alpha^2$ to show that $\text{disc}(\alpha) = -27b^2$.
   (b) Show that in general, we may write $f'(\alpha)$ as $-\dfrac{2a\alpha + 3b}{\alpha}$.
   (c) Assume that $a \neq 0$ for the next two parts. Show that $2a\alpha + 3b$ has minimal polynomial $\left(\dfrac{x-3b}{2a}\right)^3 + a\left(\dfrac{x-3b}{2a}\right) + b$ and use this to calculate $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}\left(\dfrac{x-3b}{2a}\right)$.
   (d) Show that $\text{disc}(\alpha) = -4a^3 - 27b^2$.
   (e) Show that $x^3 - x - 1$ is irreducible in $\mathbb{Q}[x]$ and use this to show that if $\alpha$ is a root, then $\mathcal{O}_{\mathbb{Q}(\alpha)} = \mathbb{Z}[\alpha]$. (Hint: for the irreducibility, try mod $p$ for a suitable prime $p$. For the second assertion, use Problem1 above.)

(3) Suppose that $\alpha \in \mathbb{C}$ is a root of $x^n + a$, and suppose that this polynomial is irreducible over $\mathbb{Q}$. Show that $\text{disc}(\alpha) = (-1)^{\frac{n(n-1)}{2}} n^n a^{n-1}$.

(4) Show that if $K_1$ and $K_2$ are quadratic extensions of $\mathbb{Q}$ such that $\text{disc}(\mathcal{O}_{K_1}) = \text{disc}(\mathcal{O}_{K_2})$ then $K_1 = K_2$. (Hint: Just take the standard $\mathbb{Z}$-basis of the ring of integers of a quadratic extension of $\mathbb{Z}$ and compute!)

(5) Use Minkowski's constant to show that the class group of $\mathbb{Q}(\sqrt{-13})$ is $\mathbb{Z}/2Z$. (Hint: Follow the example we did in class.)

(6) Solve the diophantine equation $x^2 + 13 = y^3$. (Hint: Use Problem 5 above and follow the example we did in class—you should find two solutions!)

(7) As I have mentioned in class, the foundational object of arithmetic geometry (which is the name given to the marriage of algebraic number theory and algebraic geometry) is the prime spectrum $\text{Spec}(R)$ of a commutative ring $R$. This exercise and the next concern $\text{Spec}(R)$. So, let $R$ be a commutative ring, and let $X$ denote the set of prime ideals of $R$.
   (a) For any ideal $I$ of $R$, let $V(I)$ denote the set of prime ideals of $R$ that contain $I$. Show that
      (i) $V(I) = V(\sqrt{I})$.
      (ii) $V(0) = X$.
      (iii) $V(R) = \emptyset$.
   (b) If $I_\alpha$ is any collection of ideals of $R$, then $V(\cup_\alpha I_\alpha) = \cap_\alpha V(I_\alpha)$.
   (c) If $I$ and $J$ are any two ideals of $R$, then $V(I \cap J) = V(I) \cup V(J)$.

   Thus, $X$, along with the subsets of the form $V(I)$ for $I$ an ideal of $R$, forms a topological space, with the $V(I)$ serving as closed sets. This topological space is denoted $\text{Spec}(R)$. When $R$ is a finitely generated algebra over $\mathbb{C}$, then $R$ corresponds to the coordinate ring of an affine variety, the maximal ideals of $R$ correspond to actual points on the variety, and more generally, the prime ideals correspond to irreducible sub varieties. Thus, in this case,

the "points" of $\mathrm{Spec}(R)$, i.e., the prime ideals of $R$, naturally correspond to the irreducible sub varieties of the variety. The object $\mathrm{Spec}(R)$ transfers this intuition to other commutative rings as well. In particular, one can consider $\mathrm{Spec}(\mathcal{O}_K)$ for $K$ a number field, and bring geometric intuition to bear on the set of prime ideals of $\mathcal{O}_K$.

(8) Continuing with the notation of Problem 7 above, for any $f \in R$, let $D(f)$ denote the complement of $V(\langle f \rangle)$ in $\mathrm{Spec}(R)$, so $D(f)$ is an open set.
   (a) Show that the $D(f)$ form a basis for the topology of $\mathrm{Spec}(R)$, i.e, that every open set is a union of sets of the form $D(f)$. (Hint: Any open set is the complement of $V(I)$ for some ideal of $I$. Given $p \notin V(I)$, $p$ cannot contain $I$, so there is some $f \in I$ such that $P$ does not contain $f$.)
   (b) Suppose that $\mathrm{Spec}(R) = \cup_\alpha D(f_\alpha)$. Show that the $f_\alpha$ must generate the unit ideal. (Hint: if $I$ is the ideal generated by the $f_\alpha$, show that $I$ cannot be contained in any maximal ideal.)
   (c) Suppose that $1 = r_1 f_1 + \cdots + r_n f_n$ for $r_i$, $f_j$ in $R$. Show that $\mathrm{Spec}(R) = \cup_j D(f_j)$.
   (d) Show that $\mathrm{Spec}(R)$ is quasi-compact. ("Quasi-compact" means that every open cover has a finite sub cover. Usually, this is what we'd mean by compact, but in arithmetic geometry, "compact" is used to denote spaces that are both quasi-compact and Haussdorf. To show that $\mathrm{Spec}(R)$ is quasi-compact, show that it is sufficient to consider covers of $\mathrm{Spec}(R)$ by sets of the form $D(f)$. Now apply the previous two parts.

The sets of the form $D(f)$ are called *basic open sets* of $\mathrm{Spec}(R)$. These are nice sets to work with, and objects associated to $\mathrm{Spec}(R)$ are often given by first defining them over these basic open sets, and then glueing them together using an inverse limit operation.