Homework 11 : Due Wednesday, May 9

Problem 1: Let $R = \mathbb{Z}[\frac{1+\sqrt{-5}}{2}]$ be the smallest subring of $\mathbb{C}$ containing $\mathbb{Z} \cup \{\frac{1+\sqrt{-5}}{2}\}$. Since $\frac{1+\sqrt{-5}}{2}$ is not an algebraic integer (because $-5 \not\equiv 1 \pmod 4$), we know that R is not finitely generated as an additive abelian group, and in particular $R \neq \{a + b \cdot \frac{1+\sqrt{-5}}{2} : a, b \in \mathbb{Z}\}$. Show that R contains infinitely many rational numbers that are not integers, i.e. show that $R \cap (\mathbb{Q} \backslash \mathbb{Z})$ is infinite.
Note: As a result, one can show that Lemma 6.2.2 and Corollary 6.2.3 are false in R, and so all of the subsequent arguments in Chapter 6 would not work in this larger ring.

Problem 2: Let $d \in \mathbb{Z} \backslash \{1\}$ be square-free and let $R = \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Let $p \in \mathbb{N}^+$ be an odd prime (as usual, 2 is a special little snowflake that requires additional attention) and consider the ideal $\langle p \rangle \subseteq R$.
a. Suppose that $(\frac{d}{p}) = 0$. Show that

$$\langle p \rangle = \langle p, \sqrt{d} \rangle \cdot \langle p, \sqrt{d} \rangle$$

Conclude that $\langle p \rangle$ is not a prime ideal (one can show that the ideal on the right is a prime ideal, but you need not do this).
b. Suppose that $(\frac{d}{p}) = 1$ and fix $a \in \mathbb{Z}$ with $a^2 \equiv d \pmod p$. Show that

$$\langle p \rangle = \langle p, a + \sqrt{d} \rangle \cdot \langle p, a - \sqrt{d} \rangle$$

Conclude that $\langle p \rangle$ is not a prime ideal (one can show that the two ideals on the right are distinct prime ideals, but you need not do this).
c. Suppose that $(\frac{d}{p}) = -1$. Show that $\langle p \rangle$ is a prime ideal.
Note: These distinct possibilities ($\langle p \rangle$ remains prime, splits into distinct prime factors, or has a repeated prime factor) play an extremely important role in more advanced parts of algebraic number theory.

Problem 3: Let $R = \mathbb{Z}[\sqrt{-3}]$ be the smallest subring of $\mathbb{C}$ containing $\mathbb{Z} \cup \{\sqrt{-3}\}$. Notice that $-3 \equiv 1 \pmod 4$, so $R \neq \mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$. Let $J = \langle 2 \rangle$ and let $I = \langle 2, 1 + \sqrt{-3} \rangle$. It is straightforward to see that $1 + \sqrt{-3} \notin J$, and we showed on Homework 9 that $1 \notin I$. Thus $J \subsetneq I \subsetneq R$.
a. Show that $(R : J) = 4$ and write out the addition and multiplication tables for R/J.
b. Show that J is not a prime ideal of R.
c. Show that I is the unique prime ideal of R containing J.
d. Show that $I^2 = \langle 4, 2 + 2\sqrt{-3} \rangle$ and that $I^2 \subsetneq J$.
e. Show that J is can not be written as a product of prime ideals.
Note: Part e provides another reason why we prefer to work in $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$ rather than in R.