Math 661
Algebraic Number Theory
Problem Set 2

(1) Mimic the proof we went over in class that showed that $\mathbb{Z}[i]$ is Euclidean and show that $\mathbb{Z}[\sqrt{-2}]$ is also Euclidean. (This shows therefore that $\mathbb{Z}[\sqrt{-2}]$ is a PID and an UFD.)

(2) Show that $\mathbb{Z}[\sqrt{2}]$ is Euclidean with respect to the function $N : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}^{\geq 0}$ given by $N(m + n\sqrt{2}) = |m^2 - 2n^2|$. (Hint: An arbitrary element of $\mathbb{Q}(\sqrt{2})$ can be written as $\dfrac{a + b\sqrt{2}}{c}$ for suitable integers a, b, and c, after multiplying the denominator by its conjugate and clearing demominators. Conversely, any real number of the form $\dfrac{a + b\sqrt{2}}{c}$ where a, b, and c are integers with $c \neq 0$ is in $\mathbb{Q}(\sqrt{2})$. Note that the function N extends to a function from $\mathbb{Q}(\sqrt{2})$ to $\mathbb{Q}^{\geq 0}$ given by $N(\frac{a+b\sqrt{2}}{c}) = |\frac{a^2-2b^2}{c^2}|$, for integers a, b, and c, and this satisfies $N(1) = 1$ and $N(xy) = N(x)N(y)$ for x and y in $\mathbb{Q}(\sqrt{2})$. To show that $\mathbb{Z}[\sqrt{2}]$ is Euclidean, we need to show that given an arbitrary $\dfrac{a + b\sqrt{2}}{c}$ in $\mathbb{Q}(\sqrt{2})$, there exists $p + q\sqrt{2}$ in $\mathbb{Z}[\sqrt{2}]$ such that $N(\dfrac{a + b\sqrt{2}}{c} - p - q\sqrt{2}) < 1$. Study the norm function to determine how to choose the integers p and q to satisfy this criterion.)

(3) Solve $x^3 - y^2 = 2$ for integer values of x and y. (Hint: Recall from Problem 1 that $\mathbb{Z}[\sqrt{-2}]$ is a UFD. First show that in any solution, both x and y must be odd, by considering the equation modulo n for suitable n. Then mimic the solution procedure from class for $x^3 - y^2 = 1$.)

(4) We will show that $\mathbb{Z}[\sqrt{-n}]$ is not a UFD for $n \geq 3$ in this exercise:
   (a) Assume that $n > 0$ and $\mathbb{Z}[\sqrt{-n}]$ is a UFD. Show that if $-n$ is a square mod p, then p cannot be irreducible in $\mathbb{Z}[\sqrt{-n}]$.
   (b) Note that $-n$ is necessarily a square mod 2 (why is that?) and conclude from this that $\mathbb{Z}[\sqrt{-n}]$ cannot be a UFD if $n \geq 3$.

(5) We'll contrast quadratic and cubic extensions of $\mathbb{Q}$:
   (a) Show that any quadratic (i.e., degree 2) extension of $\mathbb{Q}$ is of the form $\mathbb{Q}(\sqrt{d})$ for some square free integer d.
   (b) Give an explicit example of a cubic (i.e., degree 3) extension of $\mathbb{Q}$ that is not of the form $\mathbb{Q}(\sqrt[3]{d})$ for any integer d. (Hint: Consider Galois extensions of $\mathbb{Q}$.)

(6) Construct an explicit example of an irreducible element in $\mathbb{Z}[\sqrt{-13}]$ that is not prime. You need to prove all your assertions. (Hint: The corresponding question for $\mathbb{Z}[\sqrt{-5}]$ is sketched out in many sources, including Baker's notes, page 17. Use the obvious norm function on $\mathbb{Z}[\sqrt{-13}]$ to prove facts about various elements being irreducible, not being associates of one another, etc.)

(7) Let R be a commutative ring, and let M be a maximal ideal of R. Suppose that $1 + x$ is a unit for every $x \in M$. Show that R is a local ring. (Hint: Let N be another maximal ideal of R. Then the ideal generated by N and M must contain 1. Work with this.)

(8) Let Q be a point in $\mathbb{C}^n$ with coordinates $(a_1, \ldots, a_n)$, and let R be the subring of the rational function field $\mathbb{C}(x_1, \ldots, x_n)$ consisting of all f/g, where f and g are polynomials in $x_1, \ldots, x_n$ with $g(Q) \neq 0$. Show that R is a local ring. Identify its (unique) maximal ideal. (Hint: one possibility is to use Problem 7 above.)

(9) We will show here that any algebraic integer that has the property that all its conjugates (including itself) have absolute value (i.e., modulus) 1 must be a root of unity.

(a) Suppose that all roots of a monic polynomial $f \in \mathbb{Q}[x]$ have absolute value 1. Show that the absolute value of the coefficient of x^r is bounded by $\binom{n}{r}$. (Hint: Write each coefficient as a suitable function of the roots.)

(b) Show that there are only finitely many algebraic integers α of fixed degree n, all of whose conjugates (including itself) have absolute value 1. (Hint: Use Part 9a above: there are only finitely many equations that such an α can satisfy.)

(c) Show that any algebraic integers α all of whose conjugates (including itself) have absolute value 1 must be some k-th root of unity. (Hint: Use Part 9b to show that the powers of α cannot all be distinct.)

(10) John is now twice as old as he was when Mary was three years older than he is now, but he is only half as old as Mary is at present. How old are they now[1]?

[1] I wanted the problem count to come out to be 10 exactly. ☺☺