Algebraic Number Theory
MATH 512

Assignment 1

1. (a) Show that the quadratic extensions of $\mathbb{Q}$ lying in some fixed algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$ take the form $\mathbb{Q}(\sqrt{D})$, with $D \neq 1$ a square-free integer (i.e. not divisible by a square greater than 1). Here, square root means any square root taken in $\bar{\mathbb{Q}}$.

(b) Show further that if $D_1, D_2 \neq 1$ are square-free integers such that $\mathbb{Q}(\sqrt{D_1})$ is isomorphic to $\mathbb{Q}(\sqrt{D_2})$, then $D_1 = D_2$. (You may do this directly, or use any result from class.)

2. Let L be a number field and $\mathcal{O}_L$ its ring of integers. Show that the fraction field of $\mathcal{O}_L$ is indeed L.

3. Let L be a number field and a a non-zero element of L. State and prove a necessary and sufficient condition for a to be a unit of L (that is, a unit of the ring of integers $\mathcal{O}_L$) in terms of the minimal polynomial for a over $\mathbb{Q}$.

4. (a) Let α be a root of the polynomial $x^3 - 2$ in some algebraic closure of $\mathbb{Q}$, and let $L = \mathbb{Q}(\alpha)$. Show that $\{1, \alpha, \alpha^2\}$ is an integral basis for L, i.e. a $\mathbb{Z}$-basis for the ring of integers $\mathcal{O}_L$.

(b) Find the discriminant d_L of L.

5. Prove that there are infinitely many prime numbers $(2, 3, 5, 7, 11, \ldots)$ using only results from the class so far (which you should refer to by number), i.e. without appealing to Euclid's argument or using the Riemann ζ-function (or any other L-function).