MAT4250 EXERCISE SHEET 2

1. The class number and Dirichlet's unit theorem

Exercise 1. Compute the regulator of a real quadratic number field.

Now let K be the field $K := \mathbf{Q}(\theta)$, where $\theta^3 = 11$. We aim to compute the class group of K. You may assume without proof that $\mathcal{O}_K = \mathbf{Z}[\theta]$.

If $\mathfrak{b}$ is a fractional ideal of K, let us write $[\mathfrak{b}]$ for the class of $\mathfrak{b}$ in Cl_K.

Exercise 2.

(a) Compute the discriminant d_K. Show that the only ramified primes in K are 3 and 11.
(b) Show that any class $[\mathfrak{b}]$ in Cl_K is represented by an integral ideal $\mathfrak{a}$ of norm $\mathcal{N}(\mathfrak{a}) < 17$.

Thus, in order to find generators for Cl_K, it suffices to check all prime ideals of $\mathcal{O}_K$ of norm < 17. To do this, it is enough to determine the prime ideals of $\mathcal{O}_K$ that lie above a rational prime p such that $p < 17$. In other words, we must compute $p\mathcal{O}_K$ for $p < 17$. We start out by considering the unramified primes.

Exercise 3. Verify the following table:

p	$p\mathcal{O}_K$	Norm
2	$\mathfrak{p}_2\mathfrak{p}_2'$	$\mathcal{N}(\mathfrak{p}_2) = 2$, $\mathcal{N}(\mathfrak{p}_2') = 4$
5	$\mathfrak{p}_5\mathfrak{p}_5'$	$\mathcal{N}(\mathfrak{p}_5) = 5$, $\mathcal{N}(\mathfrak{p}_5') = 5^2$
7	$\mathfrak{p}_7 = (7)$	$\mathcal{N}(\mathfrak{p}_7) = 7^3$
13	$\mathfrak{p}_{13} = (13)$	$\mathcal{N}(\mathfrak{p}_{13}) = 13^3$.

Exercise 4. We will now describe also the ramified primes, thus giving a complete list of the possible generators of Cl_K.

(a) Let $k \in \mathbf{Z}$ be an integer. Show that $N_{K/\mathbf{Q}}(\theta + k) = k^3 + 11$ and $N_{K/\mathbf{Q}}(\theta^2 - k) = k^3 + 121$.
(b) Use (a) to show that $\mathfrak{p}_{11} := (\theta)$ and $\mathfrak{p}_3 := (\theta - 2)$ are prime ideals of norms 11 and 3, respectively.
(c) Show that $\mathfrak{p}_3^3 = (3)$. Conclude that we have found all prime ideals in $\mathcal{O}_K$ of norm < 17.
(d) Show that $[\mathfrak{p}_5] = [\mathfrak{p}_2]^{-1}$, and that Cl_K is generated by $[\mathfrak{p}_2]$.

Therefore, in order to determine Cl_K it only remains to understand $\mathfrak{p}_2$. By Exercise 4 (a), the element $\theta^2 - 5$ has norm -4. Hence the ideal $(\theta^2 - 5)$ must be equal to either $\mathfrak{p}_2^2$ or $\mathfrak{p}_2'$, as these are the only ideals of norm 4.

Exercise 5. Prove that $(\theta^2 - 5)$ cannot be equal to $\mathfrak{p}_2'$.

Hence $\mathfrak{p}_2^2 = (\theta^2 - 2)$, so that the generator of Cl_K has order either 1 or 2 (depending on whether $\mathfrak{p}_2$ is principal or not). We will show that the order is in fact 2, which yields $\mathrm{Cl}_K \cong \mathbf{Z}/2$.

Exercise 6.

(a) Show that $\mathcal{O}_K^\times \cong \mu_2 \oplus \mathbf{Z}$. Show also that $v := 1 + 4\theta - 2\theta^2$ is a unit. You may assume without proof that v is in fact a fundamental unit.

We will now prove that the order of $[\mathfrak{p}_2]$ in Cl_K is 2. To do this, assume to the contrary that $\mathfrak{p}_2$ is principal, say $\mathfrak{p}_2 = (\alpha)$. As $\mathfrak{p}_2^2 = (\theta^2 - 5)$, we then have

$$\alpha^2 = (\theta^2 - 5)w$$

for some $w \in \mathcal{O}_K^\times$. By (a), we can write $w = \pm v^d$ for some integer d. Write $d = 2n + \delta$, where $\delta = 0$ or 1, and let $x := \pm v^\delta(\theta^2 - 5)$. Then x is congruent to a square modulo any prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. We will use this to obtain a contradiction.

(b) Prove that $x = -v^\delta(\theta^2 - 5)$, for instance by considering x modulo $\mathfrak{p}_3 = (\theta - 2)$,

(c) Show that there is a prime ideal $\mathfrak{p}_{19}$ of norm 19 dividing $(\theta + 3)$.

(d) Consider x modulo $\mathfrak{p}_{19}$ in order to obtain a contradiction.

2. Extensions of Dedekind domains, ramification theory

Exercise 7. Let p be a rational prime. Show that $p = n^2 + 3m^2$ $(n, m \in \mathbf{Z})$ if and only if $p = 3$ or $p \equiv 1 \pmod 3$.

Exercise 8. Let K be a number field. Show that $|d_K| \neq 1$. Conclude that there are no unramified extensions of $\mathbf{Q}$.

Exercise 9. Suppose that L/K is a Galois extension of number fields such that $G = \mathrm{Gal}(L/K)$ is not cyclic. Can a prime in K be inert (i.e., remains a prime ideal in $\mathcal{O}_L$) in this extension?