Number Fields: Example Sheet 3 of 3

1. Let $K = \mathbb{Q}(\sqrt{d})$ where $d > 1$ is a square-free integer. Assume the result (proved in the *Number Theory* course) that Pell's equation $x^2 - dy^2 = 1$ has a solution in integers x, y with $y \neq 0$.

   (i) Show that $\mathcal{O}_K^\times = \{\pm\varepsilon^n : n \in \mathbb{Z}\}$ for some $\varepsilon = a + b\sqrt{d}$ with $a, b \in \frac{1}{2}\mathbb{Z}$ and $a, b > 0$. [You should not assume Dirichlet's unit theorem.]

   (ii) Let $\varepsilon = a + b\sqrt{d}$ be as in (i). Show that if $d \neq 5$ and $\varepsilon^n = a_n + b_n\sqrt{d}$ with $a_n, b_n \in \mathbb{Q}$ then $(b_n)_{n\geqslant 1}$ is a strictly increasing sequence.

2. Let $K = \mathbb{Q}(\sqrt{26})$ and let $\varepsilon = 5 + \sqrt{26}$. Use Dedekind's theorem to show that the ideal equations

$$(2) = (2, \varepsilon + 1)^2, \quad (5) = (5, \varepsilon + 1)(5, \varepsilon - 1), \quad (\varepsilon + 1) = (2, \varepsilon + 1)(5, \varepsilon + 1)$$

   hold in K. Using Minkowski's bound, show that K has class number 2. Verify that ε is the fundamental unit. Deduce that all solutions in integers x, y to the equation $x^2 - 26y^2 = \pm 10$ are given by $x + \sqrt{26}y = \pm\varepsilon^n(\varepsilon \pm 1)$ for $n \in \mathbb{Z}$.

3. Find the factorisations into prime ideals of (2) and (3) in $K = \mathbb{Q}(\sqrt{-23})$. Verify that $(\omega) = (2, \omega)(3, \omega)$ where $\omega = \frac{1}{2}(1+\sqrt{-23})$. Prove that K has class number 3.

4. Find the factorisations into prime ideals of (2), (3) and (5) in $K = \mathbb{Q}(\sqrt{-71})$. Verify that

$$(\alpha) = (2, \alpha)(3, \alpha)^2 \quad \text{and} \quad (\alpha + 2) = (2, \alpha)^3(3, \alpha - 1)$$

   where $\alpha = \frac{1}{2}(1 + \sqrt{-71})$. Find an element of $\mathcal{O}_K$ with norm $2^a \cdot 3^b \cdot 5$ for some $a, b \geqslant 0$. Hence prove that the class group of K is cyclic and find its order.

5. (i) Find the fundamental unit in $\mathbb{Q}(\sqrt{3})$. Determine all the integer solutions of the equations $x^2 - 3y^2 = m$ for $m = -1, 13$ and 121.

   (ii) Find the fundamental unit in $\mathbb{Q}(\sqrt{10})$. Determine all the integer solutions of the equations $x^2 - 10y^2 = m$ for $m = -1, 6$ and 7.

6. Compute the ideal class group of $\mathbb{Q}(\sqrt{d})$ for $d = -30$, -13, -10, 19 and 65.

7. Find all integer solutions of the equations $y^2 = x^3 - 13$ and $y^2 = x^5 - 10$.

8. Show that $\mathbb{Q}(\sqrt{-d})$ has class number 1 for $d = 1, 2, 3, 7, 11, 19, 43, 67, 163$.

9. Let $K = \mathbb{Q}(\sqrt{-d})$ where $d > 3$ is a square-free integer.

   (i) Show that if $\mathcal{O}_K$ is Euclidean, then it contains a principal ideal of norm 2 or 3. [*Hint: Suppose that* $\phi : \mathcal{O}_K \setminus \{0\} \to \mathbb{Z}_{\geqslant 0}$ *is a Euclidean function. Then choose* $x \in \mathcal{O}_K \setminus \{0, \pm 1\}$ *with* $\phi(x)$ *minimal.*]

   (ii) Use your answer to Question 8 to find an example where $\mathcal{O}_K$ is a PID, but is not Euclidean.

10. Let $K = \mathbb{Q}(\alpha)$ where α is a root of $f(X) = X^3 - 3X + 1$.
    (i) Show that f is irreducible over $\mathbb{Q}$ and compute its discriminant.
    (ii) Show that $3\mathcal{O}_K = \mathfrak{p}^3$ where $\mathfrak{p} = (\alpha + 1)$ is a prime ideal in $\mathcal{O}_K$ with residue field $\mathbb{F}_3$. Deduce that $\mathcal{O}_K = \mathbb{Z}[\alpha] + 3\mathcal{O}_K$. [*Hint: See Sheet 2, Question 6.*]
    (iii) Show that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Compute the class group of K.

11. Let $K = \mathbb{Q}(\alpha)$ where α is a root of $f(X) = X^3 - 7X - 1$. [*Note that* $\mathrm{Disc}(f) = 5 \times 269$ *is square-free.*] Compute $N_{K/\mathbb{Q}}(n + \alpha)$ for $|n| \leqslant 3$. Hence show that $(5) = \mathfrak{p}_1^2\mathfrak{p}_2$ and $(7) = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$ where the $\mathfrak{p}_i$ and $\mathfrak{q}_j$ are distinct principal prime ideals in $\mathcal{O}_K$. Find units generating a subgroup of $\mathcal{O}_K^\times$ of finite index. [*Hint: You can show that the units you have found are independent by considering their images in* $\mathcal{O}_K/7\mathcal{O}_K \cong \mathbb{F}_7 \times \mathbb{F}_7 \times \mathbb{F}_7$.]

The following extra questions may or may not be harder than the earlier questions. The final two require some Galois theory.

12. Let $K = \mathbb{Q}(\sqrt{d})$ where $d \neq 0, 1$ is a square-free integer. Describe the ring $\mathcal{O}_K/2\mathcal{O}_K$ as explicitly as you can. [*The answer depends on d mod* 8.] Show that $\mathbb{Z}[\sqrt{d}]^\times \subset \mathcal{O}_K^\times$ has index 1 or 3. Give an example where the index is 3.

13. Let p be an odd prime and let $\zeta_p = e^{2\pi i/p}$.
    (i) Compute the discriminant of $(X^p - 1)/(X - 1)$. Deduce that $\mathbb{Q}(\zeta_p)$ contains a quadratic field with discriminant $\pm p$. How does the sign depend on p?
    (ii) Show using the Minkowski bound that $\mathbb{Z}[\zeta_p]$ is a UFD for $p = 5$ and $p = 7$.

14. Show that there are no integer solutions to $x^2 - 82y^2 = \pm 2$. Deduce that $\mathbb{Q}(\sqrt{82})$ has class number 4.

15. Let L/K be an extension of number fields. Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals in $\mathcal{O}_K$. Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$, and $\mathfrak{P}$ a prime ideal in $\mathcal{O}_L$ with $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L$.
    (i) Show that if $\mathfrak{a}$ and $\mathfrak{b}$ are coprime, then $\mathfrak{a}\mathcal{O}_L$ and $\mathfrak{b}\mathcal{O}_L$ are coprime.
    (ii) Show that $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$ and that $N\mathfrak{P}$ is a power of $N\mathfrak{p}$.
    (iii) Let p be a rational prime. Deduce that if p is totally ramified in L then it is totally ramified in K.

16. Let K be a number field with $K/\mathbb{Q}$ Galois. Let p be a rational prime with $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_r^{e_r}$, where the $\mathfrak{p}_i$ are distinct prime ideals. Use the Chinese Remainder Theorem (Sheet 2, Question 1) to find $x \in \mathfrak{p}_1$ with $x \notin \mathfrak{p}_i$ for $2 \leqslant i \leqslant r$. By considering $N_{K/\mathbb{Q}}(x)$ show that $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$.

17. Let $K = \mathbb{Q}(\sqrt{-23}) \subset L = \mathbb{Q}(\zeta_{23})$. Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime dividing 2. Show that if $\mathfrak{p}\mathcal{O}_L$ is principal then $\mathfrak{p}^{11}$ is principal. Use your answer to Question 3 to deduce that the class number of L is divisible by 3.