Number Fields: Example Sheet 3 of 3

1. 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 $n \in \mathbb{Z}$.

2. 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.

3. 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 $a, b \geq 0$. Hence prove that the class group of K is cyclic and find its order.

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

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

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

8. 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* $\phi : \mathcal{O}_K - \{0\} \to \mathbb{N}$ *is a Euclidean function. Then choose* $x \in \mathcal{O}_K - \{0, \pm 1\}$ *with* $\phi(x)$ *minimal.*]

   (ii) Use your answer to Question 7 to find an example where $\mathcal{O}_K$ is a PID, but is not Euclidean.

9. 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.

10. Let p be an odd prime.

   (i) Compute the discriminant of $(X^p - 1)/(X - 1)$. Deduce that $\mathbb{Q}(\zeta_p)$ contains a quadratic field with discriminant $\pm p$.

   (ii) Show using the Minkowski bound that $\mathbb{Z}[\zeta_p]$ is a UFD for $p = 5$ and $p = 7$.

11. Let $K = \mathbb{Q}(\zeta_8)$ and $\mathfrak{p} = (1 - \zeta_8)$. Show that $N\mathfrak{p} = 2$ and that complex conjugation acts trivially on $\mathcal{O}_K/\mathfrak{p}^2$. Find a fundamental unit in K. [*Hint: First find a fundamental unit in* $\mathbb{Q}(\zeta_8) \cap \mathbb{R} = \mathbb{Q}(\sqrt{2})$. *Then imitate a proof in lectures.*]

12. 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 5.*]

    (iii) Show that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Compute the class group of K.

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

13. Let K be a number field. Show that there is a number field L containing K such that for every ideal $\mathfrak{a} \subset \mathcal{O}_K$ the ideal in $\mathcal{O}_L$ generated by $\mathfrak{a}$ (denoted $\mathfrak{a}\mathcal{O}_L$) is principal. [*Hint: Use that some power of* $\mathfrak{a}$ *is principal.*]

14. Let L/K be an extension of number fields.

    (i) Show that if $\mathfrak{a} \subset \mathcal{O}_L$ is an ideal then $N(\mathfrak{a} \cap \mathcal{O}_K)$ divides $N\mathfrak{a}$.

    (ii) Let $L = \mathbb{Q}(i, \sqrt{5})$. Show that $|D_L| \leq 400$ and that the primes 2 and 3 are inert in some quadratic field $K \subset L$. Deduce that L has class number 1.

15. Show that there are no integer solutions to $x^2 - 82y^2 = \pm 2$.

16. Let $K = \mathbb{Q}(\zeta_5)$ and $\mathfrak{p} = (1 - \zeta_5)$. Show that $\mathcal{O}_K^\times$ is generated by $-\zeta_5$ and $\phi = 1 + \zeta_5 + \zeta_5^4$. Show that if $a, b \in \mathbb{Z}$ with $\zeta_5^a \phi^{4b} \equiv 1 \bmod \mathfrak{p}^3$ then $a \equiv b \equiv 0 \bmod 5$. Deduce that if $u \in \mathcal{O}_K^\times$ is a 5th power mod $\mathfrak{p}^3$ then it is a 5th power in $\mathcal{O}_K$.

17. Let L/K be an extension of number fields. Show that if $\mathfrak{p}$ is a prime of $\mathcal{O}_K$ then $\mathfrak{p}\mathcal{O}_L \neq \mathcal{O}_L$. [*Hint: Let* $x_1, \ldots, x_m$ *generate* $\mathcal{O}_L$ *as an* $\mathcal{O}_K$*-module. If* $\mathfrak{p}\mathcal{O}_L = \mathcal{O}_L$ *then we can write* $x_i = \sum a_{ij} x_j$ *for some* $a_{ij} \in \mathfrak{p}$.] Deduce that if $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in $\mathcal{O}_K$ with $\mathfrak{a}\mathcal{O}_L = \mathfrak{b}\mathcal{O}_L$ then $\mathfrak{a} = \mathfrak{b}$.

18. 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 $2 \leq i \leq r$. By considering $N_{K/\mathbb{Q}}(x)$ show that $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$.

19. 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 $\mathfrak{p}\mathcal{O}_L = x\mathcal{O}_L$ for some $x \in \mathcal{O}_L$ then $\mathfrak{p}^{11}\mathcal{O}_L = N_{L/K}(x)\mathcal{O}_L$. Deduce by Questions 2 and 17 that $\mathbb{Z}[\zeta_{23}]$ is not a UFD.

20. Let $K = \mathbb{Q}(\zeta_{p^2})$ where p is an odd prime number. Prove there is a unique subfield F of K such that $[F : \mathbb{Q}] = p$. Prove that 2 splits completely in F if and only if $2^{p-1} \equiv 1 \pmod{p^2}$. [*The primes* $p = 1093$ *and* 3511 *are the only known primes satisfying this congruence.*]