 Number Fields – Example Sheet 3 P.P. Varjú

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

$$\langle 2 \rangle = \langle 2, \varepsilon + 1 \rangle^2, \quad \langle 5 \rangle = \langle 5, \varepsilon + 1 \rangle \langle 5, \varepsilon - 1 \rangle, \quad \langle \varepsilon + 1 \rangle = \langle 2, \varepsilon + 1 \rangle \langle 5, \varepsilon + 1 \rangle$$

hold in K. Using Minkowski's bound, show that the class number of K (i.e. the cardinality of the ideal class group $\mathrm{Cl}(\mathcal{O}_K)$) is 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 $n \in \mathbf{Z}$.

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

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

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

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 $\mathbf{Q}(\sqrt{d})$ for $d = -30$, -13, -10, 19 and 65.

5.
(1) Find the fundamental unit in $\mathbf{Q}(\sqrt{3})$. Determine all the integer solutions of the equations $x^2 - 3y^2 = m$ for $m = -1, 13$ and 121.
(2) Find the fundamental unit in $\mathbf{Q}(\sqrt{10})$. 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 $\mathbf{Q}(\sqrt{-d})$ has class number 1 for $d = 1$, 2, 3, 7, 11, 19, 43, 67, 163.

8. Let $K = \mathbf{Q}(\sqrt{-d})$ where $d > 3$ is a square-free integer.
(1) Show that if $\mathcal{O}_K$ is Euclidean, then it contains a principal ideal of norm 2 or 3. [*Hint: Suppose that* $\phi : \mathcal{O}_K \backslash \{0\} \to \mathbf{Z}_{\geq 0}$ *is a Euclidean function. Then choose* $x \in \mathcal{O}_K \backslash \{0, \pm 1\}$ *with* $\phi(x)$ *minimal.*]
(2) Use your answer to Question 7 to give an example where $\mathcal{O}_K$ is a PID, but is not Euclidean.

9. Let $K = \mathbf{Q}(\alpha)$ where α is a root of $f(X) = X^3 - 7X - 1$. [*Note that* $\mathrm{disc}(f) = 5 \times 269$ *is square-free.*] Compute $\mathrm{N}_{K/\mathbf{Q}}(n + \alpha)$ for $|n| \leq 3$. Hence show that $\langle 5 \rangle = P_1^2 P_2$ and $\langle 7 \rangle = Q_1 Q_2 Q_3$ where the P_i and Q_j are distinct principal prime ideals of $\mathcal{O}_K$. 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* $\mathcal{O}_K / 7\mathcal{O}_K \cong \mathbf{F}_7 \times \mathbf{F}_7 \times \mathbf{F}_7$.]

10. Let $K = \mathbf{Q}(\sqrt{d})$ 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 $\mathbf{Z}[\sqrt{d}]^\times \subset \mathcal{O}_K^\times$ has index 1 or 3. Give an example where the index is 3.

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

12. Let $K = \mathbf{Q}(\alpha)$ where α is a root of $f(X) = X^3 - 3X + 1$.

(1) Show that f is irreducible over $\mathbf{Q}$ and compute its discriminant.

(2) Show that $3\mathcal{O}_K = P^3$ where $P = \langle \alpha + 1 \rangle$ is a prime ideal in $\mathcal{O}_K$ with residue field $\mathbf{F}_3$. Deduce that $\mathcal{O}_K = \mathbf{Z}[\alpha] + 3\mathcal{O}_K$.

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

13. Let $K = \mathbf{Q}(e^{2\pi i/23})$.

(1) Show that there are distinct prime ideals Q, Q' of $\mathcal{O}_K$ such that $\langle 2 \rangle = QQ'$ and $\mathrm{N}(Q) = \mathrm{N}(Q') = 2^{11}$. *[You may use the fact from Part II Galois Theory that any finite field of order p^n contains a unique subfield of order p^d for each $d|n$.]*

(2) Using your answer to Question 2, deduce that the class number of K is divisible by 3.

14. Let $B_{r,s}(t) = \{(y_1, \ldots, y_r, z_1, \ldots, z_s) \in \mathbf{R}^r \times \mathbf{C}^s \mid \sum |y_i| + 2\sum |z_j| \leq t\}$. Show that

$$\mathrm{Vol}\, B_{r+1,s}(t) = \int_{-t}^{t} \mathrm{Vol}\, B_{r,s}(t - |y|)dy,$$

and

$$\mathrm{Vol}\, B_{r,s+1}(t) = \int_{|z| \leq t/2} \mathrm{Vol}\, B_{r,s}(t - 2|z|)dz.$$

Hence show by induction that

$$\mathrm{Vol}\, B_{r,s}(t) = 2^r \left(\frac{\pi}{2}\right)^s \frac{t^{r+2s}}{(r+2s)!}.$$

[You should do the second integral by choosing polar coordinates, $z = \rho e^{i\theta}$.]