

### 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 the class number of  $K$  (i.e. the cardinality of the ideal class group  $\text{Cl}(\mathcal{O}_K)$ ) is 2. Verify that  $\varepsilon$  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. (a) 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.

(b) 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.

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

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

9. Let  $K = \mathbb{Q}(\alpha)$  where  $\alpha$  is a root of  $f(X) = X^3 - 7X - 1$ . *[Note that  $\text{disc}(f) = 5 \times 269$  is square-free.]* Compute  $N_{K/\mathbb{Q}}(n + \alpha)$  for  $|n| \leq 3$ . Hence show that  $(5) = P_1^2 P_2$  and  $(7) = Q_1 Q_2 Q_3$  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  $\mathcal{O}_K/7\mathcal{O}_K \cong \mathbb{F}_7 \times \mathbb{F}_7 \times \mathbb{F}_7$ .]*

10. 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  $d \bmod 8$ .*] 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.

11. Let  $p$  be an odd prime and let  $\zeta_p = e^{2\pi i/p}$ .

- (a) Show that  $\mathbb{Q}(\zeta_p)$  contains a quadratic field with discriminant  $\pm p$ . How does the sign depend on  $p$ ?
- (b) Show using the Minkowski bound that  $\mathbb{Z}[\zeta_p]$  is a UFD for  $p = 5$  and  $p = 7$ .

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

- (a) Show that  $f$  is irreducible over  $\mathbb{Q}$  and compute its discriminant.
- (b) Show that  $3\mathcal{O}_K = P^3$  where  $P = (\alpha + 1)$  is a prime ideal in  $\mathcal{O}_K$  with residue field  $\mathbb{F}_3$ . Deduce that  $\mathcal{O}_K = \mathbb{Z}[\alpha] + 3\mathcal{O}_K$ .
- (c) Show that  $\mathcal{O}_K = \mathbb{Z}[\alpha]$ . Compute the class group of  $K$ .

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

- (a) Show that there are distinct prime ideals  $Q, Q'$  of  $\mathcal{O}_K$  such that  $(2) = QQ'$  and  $N(Q) = N(Q') = 2^{11}$ . [*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  $d|n$ .*]
- (b) Using your answer to Question 2, deduce that the class number of  $K$  is divisible by 3.