

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

(ii) Use your answer to Problem Sheet 2, question 11 to give an example where  $\mathcal{O}_K$  is a PID, but is not Euclidean.

8. 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.

9. 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  $p = 7$ .

10. 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.]
11. Let  $K = \mathbb{Q}(\alpha)$  where  $\alpha$  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 are just for fun. Questions 18 and 19 need 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  $\mathfrak{P}$  is a prime ideal in  $\mathcal{O}_L$  then  $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$  is a prime ideal in  $\mathcal{O}_K$  and  $N\mathfrak{P}$  is a power of  $N\mathfrak{p}$ .
  - (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  $L/K$  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  $x_1, \dots, x_m$  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  $\mathfrak{a} = \mathfrak{b}$ .
17. Let  $L/K$  be an extension of number fields. Let  $p$  be a rational prime. Show using Questions 14(i) and 16 that
  - (i) If  $p$  is unramified in  $L$  then it is unramified in  $K$ .
  - (ii) If  $p$  is totally ramified in  $L$  then it is totally ramified in  $K$ .
18. Let  $K$  be a number field with  $K/\mathbb{Q}$  Galois. Let  $p$  be a rational prime with  $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$ , 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  $\text{Gal}(K/\mathbb{Q})$  acts transitively on  $\{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$ .
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 16 that  $\mathbb{Z}[\zeta_{23}]$  is not a UFD.
20. Let  $d \neq 0, 1$  be a square free integer,  $K = \mathbb{Q}(\sqrt{d})$ ,  $D = D_K$ . Define  $\chi_D(p) = \left(\frac{D}{p}\right)$  if  $p > 2$ , and  $p$  prime, and  $\chi_D(2) = 1$  if  $d = 1 \pmod{8}$ ,  $\chi_D(2) = -1$  if  $d = 5 \pmod{8}$ , and  $\chi_D(2) = 0$  otherwise. Extend this to a function on  $\mathbb{Z}$  by setting  $\chi_D(mn) = \chi_D(m)\chi_D(n)$ . Using quadratic reciprocity, show that  $\chi_D$  is  $D$ -periodic:  $\chi_D(a + Db) = \chi_D(a)$ ,  $a, b \in \mathbb{Z}$ . [Hint: You will find it easier to do the cases  $d = 3, 2, 1 \pmod{4}$  separately].