

### Number Fields: Example Sheet 2 of 3

1. Let  $\mathfrak{a}$  and  $\mathfrak{b}$  be ideals in  $\mathcal{O}_K$ . Determine the factorisations into prime ideals of  $\mathfrak{a} + \mathfrak{b}$  and  $\mathfrak{a} \cap \mathfrak{b}$  in terms of those for  $\mathfrak{a}$  and  $\mathfrak{b}$ . Show that if  $\mathfrak{a} + \mathfrak{b} = \mathcal{O}_K$  then  $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$  and there is an isomorphism of rings  $\mathcal{O}_K/\mathfrak{a}\mathfrak{b} \cong \mathcal{O}_K/\mathfrak{a} \times \mathcal{O}_K/\mathfrak{b}$ .
2. Let  $K = \mathbb{Q}(\sqrt{-5})$ . Show by computing norms, or otherwise, that  $\mathfrak{p} = (2, 1 + \sqrt{-5})$ ,  $\mathfrak{q}_1 = (7, 3 + \sqrt{-5})$  and  $\mathfrak{q}_2 = (7, 3 - \sqrt{-5})$  are prime ideals in  $\mathcal{O}_K$ . Which (if any) of the ideals  $\mathfrak{p}, \mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{p}^2, \mathfrak{p}\mathfrak{q}_1, \mathfrak{p}\mathfrak{q}_2$  and  $\mathfrak{q}_1\mathfrak{q}_2$  are principal? Factor the principal ideal  $(9 + 11\sqrt{-5})$  as a product of prime ideals.
3. Let  $\mathfrak{a} \subset \mathcal{O}_K$  be a non-zero ideal, and  $m$  the least positive integer in  $\mathfrak{a}$ . Prove that  $m$  and  $N\mathfrak{a}$  have the same prime factors.
4. Let  $K = \mathbb{Q}(\sqrt{35})$  and  $\omega = 5 + \sqrt{35}$ . Verify the ideal equations  $(2) = (2, \omega)^2$ ,  $(5) = (5, \omega)^2$  and  $(\omega) = (2, \omega)(5, \omega)$ . Show that the class group of  $K$  contains an element of order 2. Find all ideals of norm dividing 100 and determine which are principal.
5. Let  $p$  be an odd prime and  $K = \mathbb{Q}(\zeta_p)$  where  $\zeta_p$  is a primitive  $p$ th root of unity. Determine  $[K : \mathbb{Q}]$ . Calculate  $N_{K/\mathbb{Q}}(\pi)$  and  $\text{Tr}_{K/\mathbb{Q}}(\pi)$  where  $\pi = 1 - \zeta_p$ .
  - (i) By considering traces  $\text{Tr}_{K/\mathbb{Q}}(\zeta_p^j \alpha)$  show that  $\mathbb{Z}[\zeta_p] \subset \mathcal{O}_K \subset \frac{1}{p}\mathbb{Z}[\zeta_p]$ .
  - (ii) Show that  $(1 - \zeta_p^r)/(1 - \zeta_p^s)$  is a unit for all  $r, s \in \mathbb{Z}$  coprime to  $p$ , and that  $\pi^{p-1} = up$  where  $u$  is a unit.
  - (iii) Prove that the natural map  $\mathbb{Z} \rightarrow \mathcal{O}_K/(\pi)$  is surjective. Deduce that for any  $\alpha \in \mathcal{O}_K$  and  $m \geq 1$  there exist  $a_0, \dots, a_{m-1} \in \mathbb{Z}$  such that
 
$$\alpha \equiv a_0 + a_1\pi + \dots + a_{m-1}\pi^{m-1} \pmod{\pi^m \mathcal{O}_K}.$$
  - (iv) Deduce that  $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$ .
6. Let  $K = \mathbb{Q}(\sqrt{-d})$  where  $d$  is a positive square-free integer. Establish the following facts about the factorisation of principal ideals in  $\mathcal{O}_K$ .
  - (i) If  $d$  is composite and  $p$  is an odd prime divisor of  $d$  then  $(p) = \mathfrak{p}^2$  where  $\mathfrak{p}$  is not principal.
  - (ii) If  $d \equiv 1$  or  $2 \pmod{4}$  then  $(2) = \mathfrak{p}^2$  where  $\mathfrak{p}$  is not principal unless  $d = 1$  or  $2$ .
  - (iii) If  $d \equiv 7 \pmod{8}$  then  $(2) = \mathfrak{p}\bar{\mathfrak{p}}$  where  $\mathfrak{p}$  is not principal unless  $d = 7$ .
 Deduce that if  $K$  has class number 1 then either  $d = 1, 2$  or  $7$ , or  $d$  is prime and  $d \equiv 3 \pmod{8}$ .
7. Let  $K = \mathbb{Q}(\sqrt{-m})$  where  $m > 0$  is the product of distinct primes  $p_1, \dots, p_k$ . Show that  $(p_i) = \mathfrak{p}_i^2$  where  $\mathfrak{p}_i = (p_i, \sqrt{-m})$ . Show that just two of the ideals  $\prod \mathfrak{p}_i^{r_i}$  with  $r_i \in \{0, 1\}$  are principal. Deduce that the class group  $\text{Cl}_K$  contains a subgroup isomorphic to  $(\mathbb{Z}/2\mathbb{Z})^{k-1}$ . [If you like, just do the case  $m \not\equiv 3 \pmod{4}$ .]

8. Prove that if  $x \in K$  is integral over  $\mathcal{O}_K$  (i.e.  $x$  is a root of a monic polynomial with coefficients in  $\mathcal{O}_K$ ) then  $x \in \mathcal{O}_K$ .
9. Let  $K = \mathbb{Q}(\theta)$  where  $\theta$  is a root of  $X^3 - 4X + 7$ . Determine the ring of integers and discriminant of  $K$ . Determine the factorisation into prime ideals of  $p\mathcal{O}_K$  for  $p = 2, 3, 5, 7, 11$ . Find all non-zero ideals  $\mathfrak{a}$  of  $\mathcal{O}_K$  with  $N\mathfrak{a} \leq 11$ .
10. Let  $K = \mathbb{Q}(\alpha)$  where  $\alpha$  is a root of  $f(X) = X^3 + X^2 - 2X + 8$ . [*This polynomial is irreducible over  $\mathbb{Q}$  and has discriminant  $-4 \times 503$ .*]
  - (i) Show that  $\beta = 4/\alpha \in \mathcal{O}_K$  and  $\beta \notin \mathbb{Z}[\alpha]$ . Deduce that  $\mathcal{O}_K = \mathbb{Z}[\alpha, \beta]$ .
  - (ii) Show that there is an isomorphism of rings  $\mathcal{O}_K/2\mathcal{O}_K \cong \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2$ . Deduce that 2 splits completely in  $K$ .
  - (iii) Use Dedekind's criterion to show that  $\mathcal{O}_K \neq \mathbb{Z}[\theta]$  for any  $\theta$ .
11. (i) Let  $\mathfrak{a} \subset \mathcal{O}_K$  be a non-zero ideal. Show that every ideal in the ring  $\mathcal{O}_K/\mathfrak{a}$  is principal. [*Hint: Use Question 1 to reduce to the case  $\mathfrak{a}$  is a prime power.*]
  - (ii) Deduce that every ideal in  $\mathcal{O}_K$  can be generated by 2 elements.

The following extra questions may or may not be harder than the earlier questions.

12. Let  $K$  be a quadratic field and  $\mathfrak{a} \subset \mathcal{O}_K$  an ideal. Show that  $\mathfrak{a} = (\alpha, \beta)$  for some  $\alpha \in \mathbb{Z}$  and  $\beta \in \mathcal{O}_K$ . Let  $c = \gcd(\alpha^2, \alpha \operatorname{Tr} \beta, N\beta)$ . By computing the norm and trace show that  $\frac{\alpha\beta}{c} \in \mathcal{O}_K$ . Deduce that  $(\alpha, \beta)(\alpha, \bar{\beta})$  is principal where  $\bar{\beta}$  is the conjugate of  $\beta$ .
13. Let  $K$  be a number field and  $p$  a rational prime. It can be shown that  $p$  ramifies in  $K$  if and only if  $p$  divides the discriminant  $D_K$ . Explain how this follows from Dedekind's criterion in the case  $[K : \mathbb{Q}] = 2$ , or more generally when  $\mathcal{O}_K = \mathbb{Z}[\theta]$  for some  $\theta$ .
14. For  $\mathfrak{a}$  an ideal in  $\mathcal{O}_K$  let  $\phi(\mathfrak{a}) = |(\mathcal{O}_K/\mathfrak{a})^*|$ . Show that  $\phi(\mathfrak{a}) = N(\mathfrak{a}) \prod_{p|\mathfrak{a}} (1 - \frac{1}{Np})$ .
15. Prove Stickelberger's criterion, that  $D_K \equiv 0, 1 \pmod{4}$ . [*Hint: Start by writing  $D_K = (P - N)^2 = (P + N)^2 - 4PN$  where  $P$  is a sum over even permutations and  $N$  is a sum over odd permutations. Then show that  $P + N, PN \in \mathbb{Z}$ .*] Hence compute the ring of integers of  $\mathbb{Q}[X]/(f(X))$  where  $f(X) = X^3 - X + 2$ .