Lent Term 2012 T.A. Fisher

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. 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 $(2) = \mathfrak{p}\overline{\mathfrak{p}}$ where $\mathfrak{p}$ is not principal unless $d = 1$ or 2.

   (iii) If $d \equiv 7 \pmod 8$ then $(2) = \mathfrak{p}\overline{\mathfrak{p}}$ 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 $d \equiv 3 \pmod 8$.

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

7. Find all solutions in integers x, y to the equation $y^2 = x^3 - 13$.

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 6 to find an example where $\mathcal{O}_K$ is a PID, but is not Euclidean.

9. Show that the equation $y^2 = x^5 - 10$ has no integer solutions.

10. Let $K = \mathbb{Q}(i, \sqrt{5})$. Show that $|D_K| \leq 400$ and that the primes 2 and 3 are inert in one of the quadratic subfields of K. Deduce that K has class number 1.

11. 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 $\mathcal{O}_K = \mathbb{Z}[\alpha] + 3\mathcal{O}_K$.

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

12. 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.*]

The following extra questions are on cyclotomic fields. We write $\zeta_m \in \mathbb{C}$ for a primitive mth root of unity.

13. Let p be an odd prime. Compute the discriminant of $(X^p - 1)/(X - 1)$. Show using Minkowski's bound that $\mathbb{Z}[\zeta_p]$ is a UFD for $p = 5$ and $p = 7$.

14. (i) 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* $a_{ij} \in \mathfrak{p}$.]

    (ii) Show that if a rational prime p ramifies in K then it ramifies in L.

    (iii) Let p be an odd prime. Show using (ii) that the only possible quadratic subfield of $\mathbb{Q}(\zeta_p)$ is $\mathbb{Q}(\sqrt{p^*})$ where $p^* = (-1)^{(p-1)/2}p$.

    (iv) Using your answer to Question 13, or otherwise, show that $\mathbb{Q}(\sqrt{p^*}) \subset \mathbb{Q}(\zeta_p)$.

    (v) Show that if q is a prime with $q \equiv 1 \pmod{p}$ then q splits completely in $\mathbb{Q}(\zeta_p)$. Deduce that $(p^*/q) = 1$. [*This is a special case of quadratic reciprocity.*]

15. Let $K = \mathbb{Q}(\sqrt{-23}) \subset L = \mathbb{Q}(\zeta_{23}) \subset \mathbb{C}$.

    (i) Use Dedekind's criterion to show that $2\mathcal{O}_K = \mathfrak{p}\mathfrak{q}$ and $2\mathcal{O}_L = \mathfrak{P}\mathfrak{Q}$ where $\mathfrak{p}$, $\mathfrak{q}$ and $\mathfrak{P}$, $\mathfrak{Q}$ are distinct prime ideals. Show that (after switching $\mathfrak{P}$ and $\mathfrak{Q}$ if necessary) we have $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}$ and $\mathfrak{q}\mathcal{O}_L = \mathfrak{Q}$.

    (ii) Let $\sigma_1, \ldots, \sigma_{11} : L \hookrightarrow \mathbb{C}$ be the field embeddings that fix K pointwise. Show that if $x \in \mathfrak{P}$ then $N_{L/K}(x) = \prod_{i=1}^{11} \sigma_i(x) \in \mathfrak{P}^{11}$.

    (iii) By taking norms show that if $\mathfrak{P}$ is principal then $\mathfrak{p}^{11}$ is principal. Deduce, using your answer to Question 2, that $\mathbb{Z}[\zeta_{23}]$ is not a UFD.

16. Let $K = \mathbb{Q}(\zeta_5)$. Show that $K \cap \mathbb{R} = \mathbb{Q}(\sqrt{5})$ has fundamental unit $\phi = 1 + \zeta_5 + \zeta_5^4$. Deduce (from results in lectures) that $\mathcal{O}_K^*$ is generated by $-\zeta_5$ and ϕ. Show that if $u \in \mathcal{O}_K^*$ is a 5th power modulo $(1 - \zeta_5)^3$ then it is a 5th power in $\mathcal{O}_K$. [*It may help to note that* $\phi \equiv 3 + \pi^2 \pmod{\pi^3}$ *where* $\pi = 1 - \zeta_5$.]