Number Fields: Example Sheet 2

(1) Let $\mathcal{O}$ be a Dedekind domain and $\mathfrak{a} \subset \mathcal{O}$ a non-zero ideal. Show that any ideal of the ring $R = \mathcal{O}/\mathfrak{a}$ can be generated by one element.

Hint: use the Chinese Remainder Theorem to reduce to the case where $\mathfrak{a} = \mathfrak{p}^n$ is a power of a prime ideal. Then show that the only non-zero proper ideals of $\mathcal{O}/\mathfrak{p}^n$ are $\mathfrak{p}/\mathfrak{p}^n, \ldots, \mathfrak{p}^{n-1}/\mathfrak{p}^n$. If $\pi \in \mathfrak{p} - \mathfrak{p}^2$ show that $\mathfrak{p}^\nu = [\pi^\nu] + \mathfrak{p}^n$, $\nu = 1, \ldots, n$.

(2) If $\mathcal{O}$ is a Dedekind domain, show that any ideal can be generated by at most two elements.

Hint: use the preceding exercise.

(3) 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 $\mathcal{O}_K$.

(a) Suppose d has more than one prime factor. If the odd prime p divides d then $[p] = \mathfrak{p}^2$, where $\mathfrak{p}$ is a non-principal prime ideal of $\mathcal{O}_K$.

(b) If $d \equiv 1$ or $d \equiv 2 \mod 4$, then $[2] = \mathfrak{p}^2$, with a non-principal prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ unless $d = 1$ or $d = 2$.

(c) If $d \equiv 7 \mod 8$ put $\omega = \frac{1+\sqrt{-d}}{2}$. Then $[2, \omega]$ is not a principal ideal, unless $d = 7$ in which case it is principal. Furthermore, $[2] = [2, \omega][2, \bar{\omega}]$, where $\bar{\omega} = \frac{1-\sqrt{-d}}{2}$.

Deduce that if K has class number one, then either $d = 1$, 2 or 7 or d is prime and $d \equiv 3 \mod 8$.

(4) Let K be a number field of degree n over $\mathbb{Q}$. Assume there is $\theta \in \mathcal{O}_K$ such that $1, \theta, \ldots, \theta^{n-1}$ is an integral basis of $\mathcal{O}_K$. Let $f(X) \in \mathbb{Z}[X]$ be the minimal polynomial of θ.

(a) Show that the map $\mathbb{Z}[X] \to \mathcal{O}_K$, $X \mapsto \theta$, induces an isomorphism $\mathbb{Z}[X]/[f(X)] \xrightarrow{\simeq} \mathcal{O}_K$.

(b) For any prime number p, show that $\mathcal{O}_K/[p]$ is isomorphic to $\mathbb{F}_p[X]/[\bar{f}(X)]$, where $\bar{f}(X) \in \mathbb{F}_p(X)$ denotes the image of $f(X)$ under the canonical map $\mathbb{Z}[X] \to \mathbb{F}_p[X]$.

(c) Let p be a prime number. Deduce from (b) that the ideal $[p] = p\mathcal{O}_K$ is a prime ideal if and only if $\bar{f}(X)$ is an irreducible polynomial in $\mathbb{F}_p[X]$.

(5) Let $K = \mathbb{Q}(\sqrt{d})$, where $d \neq 1$ is a non-zero square-free integer.

(a) Suppose $d \equiv 1 \mod 4$ and let p be an odd prime number. Show that $X^2 - X + \frac{1-d}{4}$ is irreducible in $\mathbb{F}_p[X]$ if and only if $X^2 - d$ is irreducible in $\mathbb{F}_p[X]$.

(b) Let p be an odd prime number. Show that the ideal $[p] = p\mathcal{O}_K$ is a prime ideal if and only if the congruence $X^2 \equiv d \mod p$ does not have a solution.

(c) Suppose $d \equiv -3 \mod 8$. Show that $X^2 - X + \frac{1-d}{4}$ is irreducible in $\mathbb{F}_2[X]$. Deduce that $[2] = 2\mathcal{O}_K$ is a prime ideal in $\mathcal{O}_K$.

(6) We denote by $M_d = \frac{2}{\pi}|d_{\mathbb{Q}(\sqrt{-d})}|^{\frac{1}{2}}$ the Minkowski constant of $K = \mathbb{Q}(\sqrt{-d})$. One has $M_7 \approx 1.7$, $M_{11} \approx 2.1$, $M_{19} \approx 2.8$, $M_{43} \approx 4.2$, $M_{67} \approx 5.2$ and $M_{163} \approx 8.1$.

Use the fact that the ideal class group is generated by the classes of prime ideals $\mathfrak{p}$ which appear in the factorisation of the primes $p \leq M_d$ to show that $\mathbb{Q}(\sqrt{-d})$ has class number one for $d = 1, 2, 3, 7, 11, 19, 43, 67$ and 163. (For the first three values of d you can cite an exercise on the first example sheet.) These values of d are indeed the only positive values for which $\mathbb{Q}(\sqrt{-d})$ has class number one.

(7) Show that the class number of $\mathbb{Q}(\sqrt{-5})$ is two. (Use exercise 3 and that the Minkowski constant of $\mathbb{Q}(\sqrt{-5})$ is ≈ 2.84.)

(8) Put $K = \mathbb{Q}(\sqrt{-6})$. Show that $\mathfrak{p} = [2, \sqrt{-6}]$ and $\mathfrak{q} = [3, \sqrt{-6}]$ are prime ideals of $\mathcal{O}_K$ satisfying $\mathfrak{p}^2 = [2]$ and $\mathfrak{q}^2 = [3]$ (cf. exercise 3). Find a relation between these two prime ideals and conclude that K has class number two. (You may use that the Minkowski constant of K is ≈ 3.12.)

(9) Prove that the prime 3 generates a prime ideal in the ring of integers of $\mathbb{Q}(\sqrt{-10})$. Show further that this number field has class number two. (You may use that the Minkowski constant of $\mathbb{Q}(\sqrt{-10})$ is ≈ 4.02.)

(10) Put $K = \mathbb{Q}(\sqrt{-17})$ and $\omega = 1 + \sqrt{-17}$. Prove that the prime 5 generates a prime ideal in the ring of integers of K. Show that the following relations hold in the group of fractional ideals of K:

$$[2] = [2, \omega]^2, \; 3 = [3, \omega][3, \bar{\omega}], \; [\omega] = [2, \omega][3, \omega]^2,$$

where $\bar{\omega} = 1 - \sqrt{-17}$. Deduce that the class group of K is cyclic of order four. (You may use that the Minkowski constant of K is ≈ 5.25.)

(11) Let $\theta \in \mathbb{C}$ be a root of $X^3 + X + 1$, and put $K = \mathbb{Q}(\theta)$. Show that the Minkowski constant of K is ≈ 1.58 (you may use an exercise on the previous example sheet). Deduce that K has class number one.

(12) (a) Show that if K is a number field of degree n over $\mathbb{Q}$, then

$$|d_K| \geq \left(\frac{n^n}{n!}\right)^2 \left(\frac{\pi}{4}\right)^n .$$

Deduce that $|d_K| > 1$ for every number field $K \neq \mathbb{Q}$.

(b) Show that there are constants $A > 1$, $c > 1$, such that for every number field K one has $|d_K| \geq \frac{1}{c} A^n$, where n is the degree of K over $\mathbb{Q}$. Deduce that for every $d > 0$ there is some $N \in \mathbb{Z}$ such that, if $K/\mathbb{Q}$ is a number field whose discriminant is bounded by d, then $[K : \mathbb{Q}] \leq N$.

(13) Let $\zeta \in \mathbb{C}$ be a primitive fifth root of unity and $K = \mathbb{Q}(\zeta)$. Use (without proof) that $1, \zeta, \zeta^2, \zeta^3$ is an integral basis of $\mathcal{O}_K$ to show that the discriminant of K is equal to 125. Compute the Minkowski constant and deduce that K has class number one.

(14) Let K be a number field. We define the Dedekind ζ-function $\zeta_K(s)$ by $\zeta_K(s) = \sum_{0 \neq \mathfrak{a} \subset \mathcal{O}_K} \frac{1}{N(\mathfrak{a})^s}$, where the summation is over all non-zero ideals $\mathfrak{a}$ of $\mathcal{O}_K$. Show that there is a formal identity

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1 - N(\mathfrak{p})^{-s}},$$

where the summation on the right is over all non-zero prime ideals of $\mathcal{O}_K$. (One can show that both sides converge for $Re(s) > 1$ and define holomorphic functions in this domain.) Now let $K = \mathbb{Q}(i)$. Use exercise (10) from example sheet 1 to prove that

$$\zeta_K(s) = \zeta_{\mathbb{Q}}(s) \cdot L(\chi, s) \text{ with } L(\chi, s) = \prod_p \frac{1}{1 - \chi(p)p^{-s}},$$

the product running over all odd prime numbers and $\chi(p) = (-1)^{\frac{p-1}{2}}$. Show that

$$L(\chi, s) = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)^s} = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} \pm \cdots$$

Comments, corrections and queries can be send to me at M.Strauch@dpmms.cam.ac.uk