Decomposition of ideals, class groups

Exercise 1. [Cyclotomic fields]

Let $n \geq 3$ be an integer, ζ_n a primitive n^{th}-root of unity in $\mathbb{C}$ and $K = \mathbb{Q}(\zeta_n)$.

1. Let p be a prime not dividing n. What is the decomposition of Φ_n in $\mathbb{F}_p$?
2. Deduce the decomposition of $p\mathcal{O}_K$.
3. Let p be an odd prime number. Show that for any $i, j \in \{1, \dots, p-1\}$, $\frac{1-\zeta_p^i}{1-\zeta_p^j} \in \mathbb{Z}[\zeta_p]^\times$. What is the decomposition of $p\mathcal{O}_K$ in $\mathbb{Q}(\zeta_p)$?

Exercise 2. [Totally ramified primes]

We say that the prime number p is totally ramified in the number field K if $p\mathcal{O}_K = \mathfrak{p}^n$, where $n = [K : \mathbb{Q}]$, *i.e.* its ramification index is maximal.

1. Assume $K = \mathbb{Q}(\alpha)$ where the minimal polynomial of α over $\mathbb{Q}$ is Eisenstein at p. Show that p is totally ramified in K.
2. We now show the converse. Assume p is totally ramified in K.
   (a) Provide an explanation for why there exists $\alpha \in \mathfrak{p} \setminus \mathfrak{p}^2$.
   (b) Show that $(\alpha) = \mathfrak{p}I$ where I is an ideal of $\mathcal{O}_K$ relatively prime to $\mathfrak{p}$.
   (c) Let $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ be the minimal polynomial of α. Show that p divides a_0 but p^2 does not.
   (d) Prove by induction that p divides a_i for $0 \leq i < n$. *(Hint : Start by showing that p divides $a_i\alpha^{n-1}$ in $\mathcal{O}_K$ and take the norm.)*
   (e) Conclude.

Exercise 3. [Finiteness of the class group]

Let K be a number field of degree n, $\sigma_1, \dots, \sigma_n$ its embeddings and $\alpha_1, \dots, \alpha_n$ a $\mathbb{Z}$-basis of $\mathcal{O}_K$. We are going to show that $\mathrm{Cl}(\mathcal{O}_K) = I^+(\mathcal{O}_K)/\{(\alpha) \mid \alpha \in \mathcal{O}_K\}$, the class group of K is finite.

1. Let I be a non-zero ideal of $\mathcal{O}_K$ and m an integer such that $m^n \leq N(I) < (m+1)^n$. Show that there exist integers $k_1, \dots, k_n$, not all zero, such that $|k_i| \leq m$ for $1 \leq i \leq n$ and $\alpha = k_1\alpha_1 + \cdots + k_n\alpha_n \in I$.
2. Show that $|N_{K/\mathbb{Q}}(\alpha)| \leq CN(I)$, where
$$C := \prod_{i=1}^{n} \sum_{j=1}^{n} |\sigma_i(\alpha_j)|.$$
3. Deduce that each class in $\mathrm{Cl}(\mathcal{O}_K)$ admits a representative of norm less than C, and conclude.
4. Deduce an algorithm to compute $\mathrm{Cl}(\mathcal{O}_K)$, and use it to show that $\mathbb{Z}[\sqrt{d}]$ is principal for $d \in \{-2, -1, 2, 3\}$.
5. Prove that, in $\mathbb{Z}[\sqrt{6}]$, $(2) = (2 - \sqrt{6})^2, (3) = (3 - \sqrt{6})^2, (5) = (\sqrt{6} - 1)(\sqrt{6} + 1)$ and (7) and (11) are prime, and deduce that $\mathbb{Z}[\sqrt{6}]$ is principal.

6. Show that $\mathbb{Z}\left[\sqrt{-5}\right]$ has class number (the order of its class group) 2.

Exercise 4. [Constructible numbers]

We say a complex number is constructible if the point it represents in the plane can be constructed from the unit segment $[0, 1]$ using only the compass and the ruler.

1. Show that $\alpha \in \mathbb{C}$ is constructible if and only if there exist fields $K_0 = \mathbb{Q} \subset K_1 \subset \cdots \subset K_n = \mathbb{Q}(\alpha)$ such that $[K_i : K_{i-1}] = 2$ for $1 \leq i < n$.
2. Let L/K be a Galois extension of order 2^n. Show that there exist subfields $K_0 = K \subset K_1 \subset \cdots \subset K_n = L$ such that $[K_i : K_{i-1}] = 2$ for $1 \leq i < n$.
3. Show that if $\alpha \in \mathbb{C}$ is constructible, then its minimal polynomial has degree a power of 2. Does the reciprocal hold ?
4. Deduce that $\cos\left(\frac{2\pi}{3}\right)$ and π are not constructible (*i.e.* the angle trisection and the squaring of the circle problems cannot be solved by compass and ruler).
5. Prove the Gauss-Wantzel theorem : ζ_n is constructible if and only if n is of the form $2^r \prod_{i=1}^m p_i$, where the p_i's are Fermat primes, *i.e.* of the $2^{2^s} + 1$.

Remark : In particular, the heptadecagon, or regular 17-gon, is constructible by ruler and compass, as was shown by Gauss when he was only 19.