Exercise 1. Let K be a number field.

(i) Show that there exists a monic irreducible polynomial $P \in \mathbb{Z}[X]$ and a root $\alpha \in \mathbb{C}$ such that $K = \mathbb{Q}(\alpha)$.

For the rest of the exercise, we assume that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. For $a, b \in \mathcal{O}_K$, we will denote by (a, b) the ideal of $\mathcal{O}_K$ generated by a and b. We let $p \in \mathbb{Z}$ be a prime number, and denote by $R \mapsto \overline{R}$ the reduction map $\mathbb{Z}[X] \to \mathbb{F}_p[X]$. Let us fix a polynomial $Q \in \mathbb{Z}[X]$ such that $\overline{Q} \in \mathbb{F}_p[X]$ is irreducible.

(ii) Assume that $\overline{Q}$ divides $\overline{P}$ in $\mathbb{F}_p[X]$. Show that the ideal $(p, Q(\alpha)) \in \mathcal{O}_K$ is prime.

(iii) Let $m \in \mathbb{N} \smallsetminus \{0\}$ be such that $\overline{Q}^m$ divides $\overline{P}$ in $\mathbb{F}_p[X]$. Show that

$$(p, Q(\alpha))^m = (p, Q(\alpha)^m).$$

(iv) Write $\overline{P} = \overline{P_1}^{n_1} \cdots \overline{P_s}^{n_s}$ where $P_1, \dots, P_s \in \mathbb{Z}[X]$ are such that $\overline{P_1}, \dots, \overline{P_s}$ are monic irreducible in $\mathbb{F}_p[X]$ and pairwise distinct. Show that

$$p\mathcal{O}_K = \prod_{i=1}^{s} (p, P_i(\alpha))^{n_i},$$

is the decomposition of the ideal $p\mathcal{O}_K$ as a product of prime ideals in $\mathcal{O}_K$.

Exercise 2. Consider the polynomial $P = X^3 + X + 1 \in \mathbb{Z}[X]$, and let $\alpha \in \mathbb{C}$ be a root of P. We recall from Exercise 4, Sheet 5 that $K = \mathbb{Q}(\alpha)$ is a number field of degree 3 whose absolute discriminant is 31, and that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

(i) Which prime numbers p ramify in K?

(ii) For every prime number p which ramifies in K, give an explicit description of the decomposition of $p\mathcal{O}_K$ as a product of prime ideals in $\mathcal{O}_K$. (Hint: use the previous exercise; compute $P(3)$ and $P(14)$.)

Exercise 3. Let K be a number field, and I an ideal of $\mathcal{O}_K$.

(i) Show that there exists an integer $n > 0$ such that the ideal I^n of $\mathcal{O}_K$ is principal.

(ii) Let $n > 0$ be an integer such that I^n is principal. Show that there exists a field extension L/K with $[L : K] \leq n$, and such that the ideal $I\mathcal{O}_L$ of $\mathcal{O}_L$ is principal.