Exercice 1. Soit $K = \mathbb{Q}[\alpha]$ avec $f_\alpha = X^3 - X^2 - 2X - 8$.

i. Vérifier que f_α est bien irréductible dans $\mathbb{Q}[X]$!

ii. Montrer que $\beta := \frac{1}{2}(\alpha + \alpha^2)$ est entier.

iii. Montrer que $D_{K/\mathbb{Q}}(1, \alpha, \alpha^2) = -4 \times 503$, puis que

$$D_{K/\mathbb{Q}}(1, \alpha, \beta) = D_{K/\mathbb{Q}}(1, \alpha, \frac{1}{2}\alpha^2) = \frac{1}{4} D_{K/\mathbb{Q}}(1, \alpha, \alpha^2) = -503.$$

En conclure que $\{1, \alpha, \beta\}$ est une base de $\mathcal{O}_K$ sur $\mathbb{Z}$.

iv. Montrer que pour tout $x \in \mathcal{O}_K$, le discriminant $D(1, x, x^2)$ est pair. En conclure que $\mathcal{O}_K$ n'est pas monogène comme $\mathbb{Z}$-algèbre.

Exercice 2. i. Vérifier que $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\zeta_8)$.

ii. Montrer que le noyau de l'application

$$(\mathbb{Z}/8\mathbb{Z})^\times \xrightarrow{\chi_{8,\mathbb{Q}}^{-1}} \mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) \xrightarrow{res} \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \xrightarrow{\psi_2} \{\pm 1\}$$

est $\{1, 7\}$.

iii. Montrer que pour p premier impair, le symbole de Legendre $\left(\frac{2}{p}\right)$ vaut 1 si $p \equiv 1, 7[8]$ et -1 si $p \equiv 3, 5[8]$.

Exercice 3. Soit $d \in \mathbb{Z} \setminus \{0, 1\}$ sans facteur carré.

i. Montrer qu'il y a une infinité de premiers décomposés dans $\mathbb{Q}(\sqrt{d})$. [raisonner par l'absurde et considérer un diviseur premier de $P^2 - d$ avec P le produit des premiers décomposés dans $\mathbb{Q}(\sqrt{d})$].

ii. Montrer qu'il y a une infinité de premiers congrus à 1 modulo 4. [prendre $d = -1$].

Exercice 4. Soit $K \subset \mathbb{C}$ un corps de nombres, n un entier et $\zeta_n = \exp(2i\pi/n)$.

i. Montrer que si l'idéal $\mathfrak{p} \in \mathrm{Max}(\mathcal{O}_K)$ se ramifie dans $K(\zeta_n)$, alors $n \in \mathfrak{p}$. La réciproque est-elle vraie ?

ii. Supposons $n \notin \mathfrak{p}$ et notons $N\mathfrak{p} := |k_\mathfrak{p}|$. Montrer que pour tout $\mathfrak{P} \in \mathrm{Max}(\mathcal{O}_{K(\zeta_n)})$ au-dessus de $\mathfrak{p}$, le degré résiduel $f(\mathfrak{P}|\mathfrak{p})$ est l'ordre de $N\mathfrak{p}$ dans le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$.