ENS de Lyon
M1 Introduction à la théorie des nombres

Examen partiel du 28 février 2020

Exercice 1 — Soit K un corps de nombres et soit p un nombre premier. On désigne par $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ les diviseurs premiers de $p\mathcal{O}_K$.

1. Étant donné deux idéaux non nuls $\mathfrak{a}, \mathfrak{b}$ de $\mathcal{O}_K$ premiers entre eux, démontrer l'identité
$$\mathfrak{a} \cdot \mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}.$$
2. Démontrer que si un élément α de $\mathcal{O}_K$ appartient à $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$, alors l'entier $\mathrm{Tr}_{K/\mathbf{Q}}(\alpha)$ est divisible par p.

   (*Indication : on pourra considérer une extension galoisienne finie $L/\mathbf{Q}$ contenant K, établir que α est contenu dans tout diviseur premier de $p\mathcal{O}_L$ et utiliser sans justification l'identité* $\mathrm{Tr}_{K/\mathbf{Q}}(\alpha) = \sum_\sigma \sigma(\alpha)$, *où σ parcourt un ensemble de représentants de* $\mathrm{Gal}(L/\mathbf{Q})/\mathrm{Gal}(L/K)$ *dans* $\mathrm{Gal}(L|\mathbf{Q})$.)
3. Pour tout $i \in \{1, \ldots, r\}$, justifier l'existence d'une famille $\mathcal{B}_i$ d'éléments de $\bigcap_{j \neq i} \mathfrak{p}_j^{e_j}$ relevant une $\mathbf{F}_p$-base de $\mathcal{O}_K/\mathfrak{p}_i^{e_i}$.
4. Pour tout $i \in \{1, \ldots, r\}$, choisissons un élément π_i dans $\mathfrak{p}_i \setminus \mathfrak{p}_i^2$. Démontrer que la juxtaposition $\mathcal{B}$ des familles
$$\left(\pi_i^\ell \beta\right)_{0 \leqslant \ell \leqslant e_i - 1,\ \beta \in \mathcal{B}_i}$$
pour $i \in \{1, \ldots, r\}$ est (un relèvement d') une $\mathbf{F}_p$-base de $\mathcal{O}_K/p\mathcal{O}_K$.
5. En considérant le discriminant de la famille $\mathcal{B}$, déduire de ce qui précède que la valuation p-adique de D_K est supérieure où égale à $\sum_{i=1}^r (e_i - 1) f_i$.

Exercice 2 — Cet exercice a pour objectif de démontrer que l'anneau des entiers du corps de nombres $\mathbf{Q}(\sqrt{7}, \sqrt{10})$ n'est pas monogène.

On rappelle que, si $L/\mathbf{Q}$ est une extension galoisienne finie, p est un nombre premier non ramifié dans L et $\mathfrak{p}$ est un idéal premier non nul de $\mathcal{O}_L$ divisant p, l'*élément de Frobenius* $(\mathfrak{p}, L/\mathbf{Q})$ est l'unique élément σ de $\mathrm{Gal}(L|\mathbf{Q})$ tel que
$$\sigma(x) \equiv x^p \pmod{\mathfrak{p}}$$
pour tout $x \in \mathcal{O}_L$. Son ordre est égal au degré résiduel $f(\mathfrak{p}/p)$.

Question préliminaire

1. Avec les notations précédentes, considérons un sous-corps $L' \subset L$ galoisien sur $\mathbf{Q}$ et posons $\mathfrak{p}' = \mathfrak{p} \cap \mathcal{O}_{L'}$. Démontrer que la projection canonique $\mathrm{Gal}(L|\mathbf{Q}) \to \mathrm{Gal}(L'|\mathbf{Q})$ envoie $(\mathfrak{p}, L/\mathbf{Q})$ sur $(\mathfrak{p}', L'/\mathbf{Q})$.

Dans ce qui suit, nous posons $K = \mathbf{Q}(\sqrt{7}, \sqrt{10})$.

2. Démontrer que K est une extension galoisienne de $\mathbf{Q}$ de degré 4, de groupe de Galois isomorphe à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.
3. Expliciter la factorisation de $3\mathcal{O}_{\mathbf{Q}(\sqrt{7})}$ et $3\mathcal{O}_{\mathbf{Q}(\sqrt{10})}$.
4. Démontrer que $3\mathcal{O}_K$ est le produit de quatre idéaux premiers distincts.
5. En déduire que l'anneau $\mathcal{O}_K$ n'est pas monogène.

Exercice 3 — Soit m un nombre entier sans facteur cubique et soit $K = \mathbf{Q}(\alpha)$, avec $\alpha^3 = m$. Soit p un nombre premier. Le but de cet exercice est la description de la factorisation de $p\mathcal{O}_K$, c'est-à-dire la détermination du nombre de facteurs premiers de $p\mathcal{O}_K$, de leurs indices de ramifications et de leurs degrés résiduels.

Questions préliminaires

1. Si $m \equiv \varepsilon \pmod 9$ avec $\varepsilon \in \{-1, 1\}$, démontrer que $\gamma = \frac{1}{3}(1 + \varepsilon\alpha + \alpha^2)$ est un entier algébrique (*Indication : on pourra calculer son polynôme minimal*).
2. Soit $p > 3$ un nombre premier. Démontrer que le corps $\mathbf{F}_p$ contient une racine primitive cubique de l'unité si et seulement si -3 est un carré modulo p. On admettra que ceci est le cas si et seulement si $p \equiv 1, 7 \pmod{12}$.

Factorisation de $p\mathcal{O}_K$.

3. Supposons $p \neq 3$.
   (a) Si $p^2 \nmid m$, décrire la factorisation de $p\mathcal{O}_K$.
   (b) Si $p^2 | m$, écrivons $m = ab^2$ avec a sans facteur carré et posons $\beta = \alpha^2/b$. Démontrer que β est un élément de $\mathcal{O}_K$ tel que $K = \mathbf{Q}(\beta)$, puis décrire la factorisation de $p\mathcal{O}_K$.
4. Décrire la factorisation de $3\mathcal{O}_K$ lorsque $m \not\equiv \pm 1 \pmod 9$.
5. Supposons $m \equiv \pm 1 \pmod 9$. Démontrer que D_K n'est pas divisible par 9 et en déduire que $3\mathcal{O}_K$ se factorise sous la forme $\mathfrak{p}^2 \cdot \mathfrak{q}$, où $\mathfrak{p}$ et $\mathfrak{q}$ sont deux idéaux premiers distincts de degrés résiduels 1.

   (*Indication : on pourra utiliser le résultat de la question 5 de l'exercice 1).*