ENS de Lyon
M1 Introduction à la théorie des nombres

Examen partiel du 12 mars 2021

Ce sujet comporte deux exercices et un problème.

Exercice 1 — Soit p un nombre premier congru à 3 modulo 4. L'objectif de cet exercice est d'établir un critère de principalité pour l'anneau $\mathbf{Z}[\zeta_p]$.

1. Expliciter l'unique extension quadratique K de $\mathbf{Q}$ contenue dans $\mathbf{Q}(\zeta_p)$.
2. En considérant la tour d'extensions $\mathbf{Q}(\zeta_p)/K/\mathbf{Q}$, démontrer que, si un nombre entier $n \in \mathbf{Z}$ est la norme d'un élément de $\mathbf{Z}[\zeta_p]$, alors il existe des nombres entiers $x, y \in \mathbf{Z}$ tels que
$$n = x^2 + xy + \frac{p+1}{4}y^2.$$
3. Supposons que l'anneau $\mathbf{Z}[\zeta_p]$ soit principal et soit ℓ un nombre premier congru à 1 modulo p. En étudiant la factorisation de ℓ dans $\mathbf{Z}[\zeta_p]$, démontrer que ℓ est la norme d'un élément de $\mathbf{Z}[\zeta_p]$.
4. Déduire de ce qui précéde que l'anneau $\mathbf{Z}[\zeta_{23}]$ n'est pas principal (Kummer).

Exercice 2 — Soit p un nombre premier et soit a un nombre entier premier à p et sans facteur carré. On désigne par K un corps de nombres tel que $K = \mathbf{Q}(\alpha)$, où $\alpha^p = a$.

1. Supposons
$$a^{p-1} \not\equiv 1 \pmod{p^2}.$$
Démontrer que $\mathbf{Z}[\alpha]$ est alors l'anneau des entiers de K.
2. Supposons maintenant que l'on ait $\mathcal{O}_K = \mathbf{Z}[\alpha]$.
   (i) Démontrer que l'on peut écrire $p\mathcal{O}_K = \mathfrak{p}^p$, avec $\mathfrak{p} \subset \mathcal{O}_K$ premier.
   (ii) Vérifier que $\alpha - a$ appartient à $\mathfrak{p} \setminus \mathfrak{p}^2$, puis en déduire que $\mathrm{N}_{K/\mathbf{Q}}(\alpha - a)$ n'est pas divisible par p^2.
   (iii) En déduire
$$a^{p-1} \not\equiv 1 \pmod{p^2}.$$

— Problème —

L'objectif de ce problème est de raffiner l'étude de la divisibilité du discriminant d'un corps de nombres K par un nombre premier p donné, puis d'en déduire une nouvelle démonstration du théorème de Stickelberger : $D_K \equiv 0, 1 \pmod 4$.

Questions préliminaires

1. Considérons un espace vectoriel V de dimension finie sur un corps K, que l'on suppose muni d'une filtration décroissante
$$V = V_0 \supseteq V_1 \supseteq \ldots \supseteq V_n = (0)$$
par des sous-K-espaces vectoriels. Soit u un endomorphisme de V préservant cette filtration, c'est-à-dire tel que $u(V_i) \subseteq V_i$ pour tout $i \in \{0, \ldots, n\}$. Pour $i \in \{0, \ldots, n-1\}$, on désigne par u_i l'endomorphisme de V_i/V_{i+1} induit par u.

Démontrer l'identité

$$\mathrm{tr}(u) = \sum_{i=0}^{n-1} \mathrm{tr}(u_i).$$

2. Soit K un corps de nombres et soit L une clôture galoisienne de K. On rappelle que, si α est un élément primitif de K, alors L est un corps de décomposition du polynôme minimal de α sur $\mathbf{Q}$.

(i) Démontrer que le discriminant D_K de K est un carré dans L.

(ii) Démontrer qu'un nombre premier p est ramifié dans L si et seulement s'il est ramifié dans K.

Première partie

Soit K un corps de nombres. Considérons un nombre premier p et écrivons

$$p\mathcal{O}_K = \mathfrak{p}^e\mathfrak{a}$$

avec $e \geqslant 1$ et $\mathfrak{p} \nmid \mathfrak{a}$.

1. À l'aide d'un élément π de $\mathfrak{p} \setminus \mathfrak{p}^2$, construire pour tout $i \geqslant 0$, un isomorphisme de $\mathcal{O}_K$-modules

$$\mathcal{O}_K/\mathfrak{p} \xrightarrow{\sim} \mathfrak{p}^i/\mathfrak{p}^{i+1}.$$

2. Justifier l'existence d'éléments $\omega_1, \ldots, \omega_f$ dans $\mathfrak{a}$ relevant une $\mathbf{F}_p$-base de $\mathcal{O}_K/\mathfrak{p}$.

3. En déduire que la famille $(\pi^i\omega_j)_{0\leqslant i\leqslant e-1,\ 1\leqslant j\leqslant f}$ peut se compléter en une base d'un sous-$\mathbf{Z}$-module M de $\mathcal{O}_K$ tel que $p \nmid (\mathcal{O}_K : M)$.

4. En observant que les éléments de $\mathfrak{p}\mathfrak{a}$ sont nilpotents dans $\mathcal{O}_K/p\mathcal{O}_K$, démontrer que D_K est divisible par p^{e-1}.

5. Démontrer que l'on a

$$\mathrm{tr}\left(\mathcal{O}_K/\mathfrak{p}^e \xrightarrow{\cdot x} \mathcal{O}_K/\mathfrak{p}^e\right) = e\ \mathrm{tr}\left(\mathcal{O}_K/\mathfrak{p} \xrightarrow{\cdot x} \mathcal{O}_K/\mathfrak{p}\right)$$

pour tout $x \in \mathcal{O}_K$.

6. En déduire que, si e est divisible par p, alors D_K est divisible par p^e.

Seconde partie

Soit K un corps de nombres, de discriminant D_K. On se propose de donner une nouvelle démonstration du théorème de Stickelberger : *D_K est congru à 0 ou à 1 modulo 4.*

1. Supposons que D_K soit impair. En considérant une clôture galoisienne de K, démontrer que D_K est congru à 1 modulo 4.

2. Supposons que D_K soit pair. En étudiant la ramification de 2 dans K, démontrer que D_K est congru à 0 modulo 4.