ENS de Lyon
M1 Introduction à la théorie des nombres

Examen partiel du 5 mars 2019

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. Démontrer que $\mathbf{Q}(-\sqrt{p})$ est l'unique extension quadratique de $\mathbf{Q}$ contenue dans $\mathbf{Q}(\zeta_p)$.
2. Démontrer que, si L/K est une extension de corps de nombres, alors
$$\mathrm{N}_{L/\mathbf{Q}} = \mathrm{N}_{K/\mathbf{Q}} \circ \mathrm{N}_{L/K}.$$
3. En déduire 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
$$n = x^2 + xy + \frac{p+1}{4}y^2.$$
4. Supposons que l'anneau $\mathbf{Z}[\zeta_p]$ soit principal et soit ℓ un nombre premier congru à 1 modulo p. En étufiant la factorisation de ℓ dans $\mathbf{Z}[\zeta_p]$, démontrer que ℓ est la norme d'un élément de $\mathbf{Z}[\zeta_p]$.
5. Déduire de ce qui précéde que l'anneau $\mathbf{Z}[\zeta_{23}]$ n'est pas principal (Kummer).

Exercice 2 — Soit K une extension galoisienne finie de $\mathbf{Q}$ et soit $\alpha \in \mathcal{O}_K$ un élément primitif, de polynôme minimal $f \in \mathbf{Z}[T]$.

Supposons qu'il existe un nombre premier p ne divisant pas le discriminant de f et tel que f soit irréductible modulo p. En étudiant la factorisation de p dans $\mathcal{O}_K$, démontrer que le groupe de Galois de l'extension $K/\mathbf{Q}$ est cyclique.

Exercice 3 — Soit A un anneau de Dedekind dont le groupe des classes d'idéaux $\mathrm{Cl}(A)$ est d'ordre 2. La première partie de cet exercice a pour objectif d'établir un théorème de Carlitz : *pour tout élément a de A non nul et non inversible, il existe un* unique *entier $n \geqslant 1$ tel que a soit le produit de n éléments irréductibles de A.* La seconde partie montre que la condition sur $\mathrm{Cl}(A)$ est nécessaire.

Première partie

1. Soit π un élément irréductible de A. Démontrer que l'idéal (π) est maximal parmi les idéaux principaux de A.
2. Soit π un élément irréductible de A tel que l'idéal (π) ne soit pas premier. Démontrer qu'il existe deux idéaux premiers non principaux $\mathfrak{p}$ et $\mathfrak{q}$ dans A tels que $(\pi) = \mathfrak{pq}$.
3. Soit $\mathcal{I}$ l'ensemble des idéaux non nuls de A. Démontrer qu'il existe une unique fonction $f : \mathcal{I} \to \mathbf{N}$ telle que

(i) pour tous $\mathfrak{a}, \mathfrak{b} \in \mathcal{I}$, $f(\mathfrak{ab}) = f(\mathfrak{a}) + f(\mathfrak{b})$;
(ii) pour tout $\mathfrak{p} \in \mathcal{I}$ premier, $f(\mathfrak{p}) = 2$ si $\mathfrak{p}$ est principal et $f(\mathfrak{p}) = 1$ sinon.

4. Soit $\pi_1, \ldots, \pi_n$ et $\pi'_1, \ldots, \pi'_m$ des éléments irréductibles de A tels que

$$\prod_{i=1}^{n} \pi_i = \prod_{i=1}^{m} \pi'_i.$$

Démontrer que l'on a $m = n$.

Seconde partie

Soit $K = \mathbf{Q}(\sqrt{-31})$.

5. Expliciter l'application $\mathcal{O}_K \to \mathbf{Z}, \quad x \mapsto \mathrm{N}_{K/\mathbf{Q}}(x)$.
6. Démontrer que 2 est un élément irréductible de $\mathcal{O}_K$.
7. Démontrer que 8 est le produit de deux éléments irréductibles de $\mathcal{O}_K$.
8. En déduire que le groupe $\mathrm{Cl}(\mathcal{O}_K)$ est non trivial et distinct de $\mathbf{Z}/2\mathbf{Z}$.

Exercice 4 — Soit p un nombre premier *congru à* 1 *modulo* 4 [a]. Cet exercice a pour objectif d'établir le théorème suivant de Dirichlet : 2 *est une puissance quatrième modulo* p *si et seulement si* p *est de la forme* $A^2 + 64B^2$ *avec* $A, B \in \mathbf{Z}$.

1. Soit p un nombre premier *congru à* 1 *modulo* 4 [b] tel que 2 soit une puissance quatrième dans $\mathbf{F}_p$. Démontrer que l'on a $p \equiv 1 \pmod 8$.
2. Soit p un nombre premier tel que $p \equiv 1 \pmod 8$.
   (i) Démontrer qu'il existe $a, b \in \mathbf{Z}$ tels que $p = a^2 + b^2$ et $2 \nmid a$, $4 | b$.
   (ii) Démontrer que a est un carré modulo p.
   (iii) Démontrer qu'il existe $x \in \mathbf{Z}$ tel que $b \equiv ax \pmod p$ et $x^2 \equiv -1 \pmod p$.
   (iv) Démontrer que l'on a
$$\left(\frac{a+b}{p}\right) \equiv (2ab)^{\frac{p-1}{4}} \pmod p.$$
   (v) En utilisant le symbole de Jacobi, établir l'égalité
$$\left(\frac{a+b}{p}\right) \equiv (-1)^{\frac{(a+b)^2-1}{8}} \pmod p$$
   (*Indication :* $2p = (a+b)^2 + (a-b)^2$)
   (vi) Déduire de ce qui précède l'égalité
$$2^{(p-1)/4} \equiv (-1)^{ab/4} \pmod p.$$
3. Achever la preuve du théorème de Dirichlet.

a. Cette condition manquait dans l'énoncé initial
b. Idem