Université Paris Sud — Année 2008-2009

M1 — Arithmétique

TD n° V

Exercice A

Pour $P \subset Q$ des $\mathbb{Z}$-modules, on note

$$[Q : P] \ := \ \#(Q/P)$$

qu'on appelle l'*indice de* P *dans* Q.

1) Soit α un nombre algébrique, P son polynôme minimal, $\alpha_1 = \alpha, \ldots, \alpha_n$ les racines de ce dernier, et $K = \mathbb{Q}[\alpha]$. On rappelle la formule :

$$\delta_{K/\mathbb{Q}}(\alpha) \ = \ \prod_{i<j}(\alpha_j - \alpha_i)^2 \ = \ (-1)^{\frac{d(d-1)}{2}} \mathrm{N}_{K/\mathbb{Q}}(P'(\alpha))$$

(cf. III.3.2.1.5.)

On suppose $P = X^d + aX + b$ irréductible et $d \geq 2$. Calculer $\delta_{K/\mathbb{Q}}(\alpha)$. Expliciter la formule quand $d = 2$ ou 3.

2) Soit $K/\mathbb{Q}$ un corps de nombres de degré d, d'anneau d'entiers $\mathcal{O}_K$ et $M \subset \mathcal{O}_K$ un sous-$\mathbb{Z}$-module libre de $\mathcal{O}_K$ de base $(f_i)_{1 \leq i \leq d}$.

a) Montrer que M est p-clos si et seulement si

$$p \ \not| \ [\mathcal{O}_K : M] \ .$$

On dit aussi parfois dans ce cas que M est *p-maximal*.

b) Montrer l'égalité entre idéaux de $\mathbb{Z}$:

$$\delta_{\mathcal{O}_K/\mathbb{Z}} \ \cdot \ [\mathcal{O}_K : M]^2 \ = \ \delta^{\mathbb{Z}}_{K/\mathbb{Q}}(M) \ .$$

c) En déduire que si $\delta^{\mathbb{Z}}_{K/\mathbb{Q}}(M)$ est sans facteur carré, alors $f_1, \ldots, f_n$ est une $\mathbb{Z}$-base de $\mathcal{O}_K$.

d) Soit p un nombre premier. Montrer que

$$p \mid \frac{\delta^{\mathbb{Z}}_{K/\mathbb{Q}}(M)}{\delta_{\mathcal{O}_K/M}},$$

si et seulement si il existe des entiers $a_1, \ldots, a_n$ tels que $(a_1, \ldots, a_n, p) = 1$ et $(a_1 f_1 + \cdots + a_n f_n)/p \in \mathcal{O}_K$. **Indication** *Traduire en termes d'éléments d'ordre p dans $\mathcal{O}_K/M$.*

3) Soient p un nombre premier, $K := \mathbb{Q}[\alpha]$ et P le polynôme minimal de α. On suppose de plus que P est d'Eisenstein en p. Montrer que $\mathbb{Z}[\alpha]$ est p-maximal. **Indication** *On pourra montrer l'identité*

$$p\mathcal{O}_K = (p, \alpha)^{\dim_{\mathbb{Q}} K} .$$

4 .a) Déterminer $\mathcal{O}_K$ lorsque $K = \mathbb{Q}(\alpha)$, avec $\alpha^3 = 2$. Mmontrer en particulier que $\mathbb{Z}[\alpha]$ est 2 et 3-maximal.
b) Même question avec $\alpha^3 - \alpha - 1 = 0$.

Exercice B. −Critère de Kummer

On va montrer le théorème suivant :

Théorème Théorème de Kummer ***Soit K un corps de nombre de degré d, $\mathcal{O}_K$ son anneau d'entiers, $\alpha \in \mathcal{O}_K$ tel que $K = \mathbb{Q}[\alpha]$ et P le polynôme minimal de α.***

Étant donné un nombre premier p, on note $\tilde{P}$ l'image de P dans $\mathbb{F}_p[X]$ et

$$\tilde{P} = \prod_{i=1}^{g} \tilde{P}_i^{\eta_i}$$

la décomposition de $\tilde{P}$ en produit d'irréductibles dans $\mathbb{F}_p[X]$. Pour tout $1 \leq i \leq g$, on note $P_i \in \mathbb{Z}[x]$ un relèvement arbitraire de $\tilde{P}_i$. Si p ne divise pas $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ (c'est-à-dire encore si $\mathbb{Z}[\alpha]$ est p-clos ou encore p-maximal,) Alors :

a) Pour tout $1 \leq i \leq g$, $\mathfrak{p}_i := p\mathcal{O}_K + P_i(\alpha)\mathcal{O}_K$ est un idéal maximal de $\mathcal{O}_K$.

b)

$$p\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{p}_i^{\eta_i} .$$

1) Expliquer pourquoi on peut supposer $K = \mathbb{Q}[\alpha]$ avec $\alpha \in \mathcal{O}_K$.

Dans la suite, les hypothèses et notations sont celles du théorème. On note encore

$$f_i := \deg(\tilde{P}_i) \; \forall 1 \leq i \leq g .$$

De plus, pour tout couple (a, b) d'éléments de $\mathcal{O}_K$, on note

$$(a, b) := a\mathcal{O}_K + b\mathcal{O}_K$$

l'idéal engendré et Pour deux $\mathbb{Z}$-modules P et Q, on note $P + Q$ le $\mathbb{Z}$-module qu'ils engendrent.

2) Pour tout $1 \leq i \leq g$, **on pose** $k_i := \mathbb{F}_p[X]/(\tilde{P}_i)$.
a) Montrer que $K_i \cong \mathbb{F}_{p^{f_i}}$ et que (p, P_i) est un idéal maximal de $\mathbb{Z}[X]$.

b) Montrer que $[\mathcal{O}_K : \mathbb{Z}[\alpha] + \mathfrak{p}_i]$ divise

$$\mathrm{pgcd}\big([\mathcal{O}_K : \mathbb{Z}[\alpha]], [\mathcal{O}_K : p\mathcal{O}_K]\big) = 1 .$$

c) Montrer que l'homomorphisme

$$\phi : \mathbb{Z}[X] \to \mathcal{O}_K/\mathfrak{p}_i \; X \mapsto \alpha$$

est surjectif.

d) En déduire que soit $\mathfrak{p}_i = \mathcal{O}_K$, soit $\mathcal{O}_K/\mathfrak{p}_i$ est un corps de cardinal p^{f_i}.

3) Montrer que $\mathfrak{p}_i + \mathfrak{p}_j = \mathcal{O}_K$ si $i \neq j$.

4) Montrer que

$$\prod_{i=1}^{g} \mathfrak{p}_i^{\eta_i} \subset (p, \prod_{i=1}^{g} P_i(\alpha)^{\eta_i}) \subset p\mathcal{O}_K$$

et en déduire que

$$p\mathcal{O}_K \mid \prod_{i=1}^{g} \mathfrak{p}_i^{\eta_i} .$$

5) Montrer le théorème de Kummer.

Exercice C

Soit p un nombre premier impair fixé, ζ une racine primitive $p^{\text{ième}}$ de l'unité et $K := \mathbb{Q}(\zeta) \subset \mathbb{C}$ le $p^{\text{ième}}$ corps cyclotomique, $\mathcal{O}_K$ son anneau d'entiers. On dit que p est *régulier* si p ne divise pas le nombre de classes d'idéaux de K. On notera $x \mapsto \overline{x}$ la conjugaison complexe.

Théorème Théorème de Kummer, 1847 *Soit $p > 3$ un premier régulier, alors il n'existe pas de $(x, y, z) \in \mathbb{Z}^3$ non nuls vérifiant l'équation de Fermat : $x^p + y^p = z^p$.*

Ce résultat établit un cas particulier du "grand théorème de Fermat", démontré complètement par Wiles par de toutes autres méthodes. Nous montrerons une partie du théorème de Kummer : une solution (x, y, z) éventuelle doit vérifier $p \mid xyz$.

1) Montrer que $\mathcal{O}_K = \mathbb{Z}[\zeta]$.

2 ***Racines de l'unité*** **a)** Montrer que $\mu(K)$, l'ensemble des racines de l'unité contenues dans K, est formé des racines $2p^{\text{ième}}$ de 1.
b) Soit M l'ensemble des éléments $x \in Or_K$ tels que pour tout plongement σ de K dans $\mathbb{C}$ on ait $|\sigma(x)| = 1$. Montrer que M est fini, et en déduire que $M = \mu(K)$.

3) Unités**On désire montrer que pour toute unité $\epsilon \in \mathcal{O}_K^*$, il existe $a \in \mathbb{Z}$ tel que $\epsilon = \zeta^a \epsilon_1$ avec $\epsilon_1 \in \mathbb{R}$.**

a) Montrer qu'il existe $b \in \mathbb{Z}$ tel que $\epsilon = \pm\zeta^b\overline{\epsilon}$.

b) On rappelle que $(1-\zeta)$ est un idéal maximal de $\mathcal{O}_K$. Montrer que $\epsilon \equiv \overline{\epsilon} \pmod{1-\zeta}$.

c) En déduire que $\epsilon = \zeta^b\overline{\epsilon}$ et conclure.

4) Soit $p > 3$ régulier, et soit $x, y, z \in \mathbb{Z}$ qui vérifient $x^p + y^p = z^p$ et $p \nmid xyz$.

a) Montrer que l'on peut supposer que x, y, z sont premiers entre eux 2 à 2, ainsi que $x \not\equiv y \pmod{p}$.

b) Montrer que

$$p = \prod_{j=1}^{p-1}(1-\zeta^j) \text{ et } z^p = \prod_{j=0}^{p-1}(x+\zeta^j y)\,.$$

c) En déduire que si $\zeta^i \neq \zeta^j$, les idéaux $(x+\zeta^i y)$ et $(x+\zeta^j y)$ sont premiers entre eux.

d) Montrer que $(x+\zeta y) = I^p$ où I est un idéal principal. En déduire qu'il existe $\alpha \in \mathcal{O}_K$ et $\epsilon \in \mathcal{O}_K^*$ tels que $x + \zeta y = \epsilon\alpha^p$.

e) Montrer que pour tout $\alpha \in \mathcal{O}_K$ il existe $\beta \in \mathbb{Z}$ tel que $\alpha^p \equiv \beta \pmod{p\mathcal{O}_K}$.

f) Montrer qu'il existe $k \in \mathbb{N}$ tel que $x + \zeta y - (x+\zeta^{-1}y)\zeta^k \equiv 0 \pmod{p\mathcal{O}_K}$.

g) Montrer que si $\sum_{i=0}^{p-2} a_i\zeta^i \equiv 0 \pmod{p\mathcal{O}_K}$ avec $a_i \in \mathbb{Z}$, alors $a_i \equiv 0 \pmod{p}$ pour tout i. En déduire que si $\sum_{i=0}^{p-1} a_i\zeta^i \in p\mathcal{O}_K$, *et qu'au moins un des a_i est nul mod p,* alors tous le sont.

h) Conclure.

Exercice D

Nous nous proposons d'étudier les solutions $(x, y) \in \mathbb{Z}^2$ de l'équation de Mordell, donnée par

$$E_k \,:\, y^2 = x^3 + k\,,$$

où $k \in \mathbb{Z}$. Nous prouverons le théorème :

Théorème Théorème de Mordell *Soit $k < -1$ un entier sans facteur carré congru à 2 ou $3 \pmod 4$. Supposons que le nombre de classes de $\mathbb{Q}(\sqrt{k})$ n'est pas divisible par 3. Alors l'équation $E_k : y^2 = x^3 + k$ admet une solution en nombres entiers si et seulement si, k est de la forme $\pm 1 - 3a^2$, $a \in \mathbb{N}^*$; dans ce cas, il y a deux solutions données par $(x, y) = (a^2 - k, \pm a(a^2 + 3k))$.*

Soient (x, y) un couple de solutions entières de l'équation E_k, où k satisfait les conditions de l'énoncé de Mordell.

1) Montrer que $(x, y) = 1$ et que x est impair.

2) Montrer que les idéaux $(y + \sqrt{k})$ et $(y - \sqrt{k})$ sont premiers entre eux. En déduire qu'il existe un idéal A principal tel que $(y + \sqrt{k}) = A^3$.

3) Montrer que les unités de $\mathcal{O}_{\mathbb{Q}(\sqrt{k})}$ sont ± 1 et conclure.