Université Paris Sud — Année 2004-2005

M1 — Arithmétique

Examen du 14 juin 2005

Durée trois heures

La qualité de la rédaction entrera pour une grande part dans la notation. Les calculatrices, téléphones mobiles et documents ne sont pas autorisés.

Documents non autorisés.
Les exercices sont indépendants.

Exercice A

Soient r un entier ≥ 3, $p_1, p_2, \ldots, p_r$ des nombres premiers distincts et $N = p_1 p_2 \ldots p_r$. Soit $F = \mathbb{Q}(\sqrt{N}) \subset \mathbb{R}$. Soient $\mathcal{O}_F$ l'anneau des entiers de F et $\mathcal{O}_F^*$ le groupe des unités.

1) Montrez qu'il existe un unique $\eta \in F$ vérifiant $\eta > 0$ tel que $\mathcal{O}_F^*$ est le groupe engendré par -1 et η.

2) Montrez que l'anneau $\mathcal{O}_F$ n'est pas principal. **Indication** *Supposer le contraire, utiliser la décomposition de l'idéal $p_i\mathcal{O}_F$ pour montrer qu'il existe $a_i \in \mathcal{O}_F$ et $m_i \in \mathbb{Z}$ tels que $p_i = \eta^{m_i} a_i^2$; montrer que m_i est impair ; montrer alors que $p_1 p_2$ est un carré dans F et en déduire une contradiction.*

Exercice B

Dans ce problème, m est un entier ≥ 3.

1) Soient p un nombre premier, $\overline{\mathbb{Q}_p}$ une clôture algébrique de $\mathbb{Q}_p$ et v_p l'unique valuation de $\overline{\mathbb{Q}_p}$ telle que $v_p(p) = 1$. Soit $\varepsilon \in \overline{\mathbb{Q}_p}$ une racine primitive m-ième de 1. Calculer $v_p(\varepsilon - 1)$ (on distinguera suivant que m n'est pas une puissance de p ou que $m = p^r$, avec $r \in \mathbb{N}$).

2) On note $E \subset \mathbb{C}$ le corps de décomposition du polynôme $X^m - 1$ et $L = E \cap \mathbb{R}$. On note U le groupe des unités de L et U_E celui de E. On pose $d = [L : \mathbb{Q}]$.
a) Calculer d lorsque m est un nombre premier.

b) Dans le cas général, calculer le rang de U et U_E en fonction de d.

c) Montrer que U_E/U est un groupe fini.

3) Pour $k \in \mathbb{Z}$, **on pose** $u_k = \frac{\sin(2k\pi/m)}{\sin(2\pi/m)}$.

Montrer que, si k est premier à m, alors $u_k \in U$. **Indication** *Remarquer que, si* $\varepsilon = e^{2i\pi/k}$, *alors* $u_k = \frac{\varepsilon^k - \varepsilon^{-k}}{\varepsilon - \varepsilon^{-1}}$.

4) On pose $G = Gal(L/Q)$ **et on note** $A = \mathbb{Z}[G]$ **l'algèbre du groupe** G : **C'est donc l'anneau commutatif formé des éléments qui s'écrivent sous la forme** $\sum_{\sigma\in G} a_\sigma \sigma$, **avec les** $a_\sigma \in \mathbb{Z}$, **l'addition étant définie de façon évidente et la multiplication par la formule**

$$(\sum_{\sigma\in G} a_\sigma\sigma)(\sum_{\tau\in G} b_\tau\tau) = \sum_{\sigma,\tau\in G} a_\sigma b_\tau \sigma\tau = \sum_{\sigma\in G}(\sum_{h\in G} a_h b_{h^{-1}\sigma})\sigma.$$

On pose $t = \sum_{\sigma\in G}\sigma$, **on note** I **l'idéal de** A **engendré par** t **et** $\tilde{A}$ **l'anneau quotient** A/I.

a) Montrez que A est un $\mathbb{Z}$-module libre de rang d et $\tilde{A}$ un $\mathbb{Z}$-module libre de rang $d-1$.

b) Pour tout $\alpha = \sum a_\sigma\sigma \in A$ et tout $u \in L$ non nul, on pose $\alpha.u = \prod_{\sigma\in G}\sigma(u)^{a_\sigma}$. Montrez que ceci munit le groupe multiplicatif L^* d'une structure de A-module, que $\mathcal{O}_L^*$ est un sous-A-module de L^* et que $\{-1,1\}$ est un sous-A-module de $\mathcal{O}_L^*$.

c) Montrer que si $u \in \mathcal{O}_L^*$, on a $t.u \in \{-1,1\}$.

Dans toute la suite, on note $\tilde{U}$ **le quotient** $U/\{-1,1\}$, **que l'on voit comme un** $\tilde{A}$**-module (via l'application qui envoie** $(\tilde{\alpha},\tilde{u})$ **sur l'image de** $\alpha.u$ **si** $\tilde{\alpha}$ **est l'image dans** $\tilde{A}$ **de** $\alpha \in A$ **et** $\tilde{u}$ **l'image dans** $\tilde{U}$ **de** $u \in U$**).**

5) On suppose désormais que m est un nombre premier tel que $(m-1)/2$ est aussi un nombre premier (par exemple on peut prendre $m = 23$). Montrez que G est un groupe cyclique d'ordre d et que le choix d'un générateur de G permet de définir un homomorphisme surjectif de l'anneau des polynômes $\mathbb{Z}[X]$ sur A dont le noyau est l'idéal engendré par $X^d - 1$. En déduire que $\tilde{A}$ est un anneau de Dedekind isomorphe à l'anneau des entiers du corps de décomposition sur $\mathbb{Q}$ du polynôme $X^d - 1$.

6 .a) Montrez que $\tilde{U}$ est un $\mathbb{Z}$-module libre de rang $d-1$.

b) En déduire que, si $v \in \tilde{U}$ est différent de l'élément neutre, l'annulateur de v dans $\tilde{A}$ (c'est-à-dire l'idéal de $\tilde{A}$ formé des a tels que $a.v = 0$) est réduit à 0.

c) En déduire que si $u \in U$ est différent de 1 et -1, l'image $\tilde{U}_u$ dans $\tilde{U}$ du sous-groupe U_u de U engendré par les $\sigma(u)$ pour $\sigma \in G$ est un $\mathbb{Z}$-module libre de rang d et que U/U_u est un groupe fini.

7) Montrez que le $\mathbb{Z}$-module libre $\tilde{U}_{u_2}$ admet les images des u_k pour $2 \le k \le (m-1)/2$ comme base **Indication** *montrez que le sous-groupe de* U *engendré par les* u_k, *pour* $2 \le k < m$ *est stable par* $Gal(E/\mathbb{Q})$ *et donc aussi par* G.

Exercice C

On note θ l'unique nombre réel tel que $\theta^7 = 12$ et on pose $K = \mathbb{Q}(\theta)$. On pose $M = K(e^{2i\pi/7})$.

1) Pour tout nombre premier p, on choisit une valuation w_p de K telle que $w_p(p) = 1$. On identifie K à un sous-corps de l'anneau $K_p = \mathbb{Q}_p \otimes K$ en posant $a = 1 \otimes a$, pour tout $a \in K$.
a) Calculer $w_2(\theta)$, $w_3(\theta)$ et $w_7(\theta + 2)$.

b) Pour $p = 2, 3, 7$, montrer que K_p est un corps, calculer l'indice de ramification et le degré résiduel de l'extension $K_p/\mathbb{Q}_p$. Trouver $\theta_p \in K$ tel que l'anneau des entiers de K_p soit $\mathbb{Z}_p[\theta_p]$.

c) Montrer que l'on peut choisir w_5 pour que $w_5(\theta - 3) > 0$. Soit k le corps engendré sur $\mathbb{F}_5$ par une racine primitive 7-ème de l'unité. Calculer $[k : \mathbb{F}_5]$. Montrer que K_5 est le produit de deux corps et calculer le degré de chacun d'entre eux sur $\mathbb{Q}_5$.

d) Pour $p = 2, 3, 5$ et 7, expliquer comment l'idéal $p\mathcal{O}_K$ se décompose.

2) Déterminer l'idéal discriminant de l'extension $K/\mathbb{Q}$.

3) Montrer que $\mathcal{O}_K = \mathbb{Z}[\theta, \theta^4/2]$.

4) Montrer que M est un corps de décomposition du polynôme $X^7 - 12$ sur $\mathbb{Q}$ et calculer $[M : \mathbb{Q}]$.

5) Montrer que $M_7 = \mathbb{Q}_7 \otimes M$ est un corps, extension totalement ramifiée de $\mathbb{Q}_7$ et trouver une uniformisante de ce corps. Calculer le discriminant de l'extension $M_7/\mathbb{Q}_7$.

6) Déterminer l'idéal discriminant de $M/\mathbb{Q}$.