Université Paris Sud **Année 2006-2007**

M1 **Arithmétique**

Examen du 15 juin 2007

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.

Les exercices A, B et C sont indépendants.
Documents non autorisés. Rappels :

Soient X une extension finie de $\mathbb{Q}$ et $\mathcal{O}_X$ l'anneau de ses entiers.

- **Soient $\mu(X)$ le groupe des racines de l'unités de X et U_X le groupe des unités de X (c'est-à-dire le groupe multiplicatif des éléments inversibles de l'anneau $\mathcal{O}_X$). Si $\mathbb{R}\otimes_{\mathbb{Q}}X \simeq \mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$, le groupe $U_X/\mu(X)$ est un groupe abélien libre de rang r_1+r_2-1.**
- **Si $\mathfrak{p}$ est un idéal maximal de $\mathcal{O}_X$, si $\mathfrak{p}\cap\mathbb{Z}$ est l'idéal engendré par p et si le corps $\mathcal{O}_X/\mathfrak{p}$ a p^f éléments, on a $N_{X/\mathbb{Q}}(\mathfrak{p}) = (p^f)$.**
- **Soient $\mathcal{D}_{X/\mathbb{Q}}$ la différente et $\mathfrak{d}_X$ le discriminant de l'extension $X/\mathbb{Q}$. On a $\mathfrak{d}_X = N_{X/\mathbb{Q}}(\mathcal{D}_{X/\mathbb{Q}})$.**
- **Si $\mathfrak{p}$ est un idéal maximal de $\mathcal{O}_X$ au-dessus du nombre premier p, si $X_{\mathfrak{p}}$ est le complété de X relativement à p et $\mathfrak{m}$ l'idéal maximal de l'anneau des entiers de $X_{\mathfrak{p}}$, on a**

$$v_{\mathfrak{p}}(\mathcal{D}_{X/\mathbb{Q}}) \;=\; v_{\mathfrak{m}}(\mathcal{D}_{X_{\mathfrak{p}}/\mathbb{Q}_p})$$

- **Soit $\lambda\in\mathcal{O}_X$ tel que $X=\mathbb{Q}(\lambda)$ et soit P le polynôme minimal de λ sur $\mathbb{Q}$. Il existe un idéal non nul I de $\mathbb{Z}$ tel que**

$$(N_{X/\mathbb{Q}}(P'\lambda)) = I^2\mathfrak{d}_X$$

- **Si Y est une extension finie de X, on a**

$$\mathcal{D}_{Y/\mathbb{Q}} \;=\; \mathcal{D}_{Y/X}\;\cdot\;\mathcal{D}_{X/\mathbb{Q}}\,.$$

Exercice A

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 $M/\mathbb{Q}$.

Exercice B

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 C

1) Soient p un nombre premier et G un groupe cyclique d'ordre p. On note $\mathbb{Z}[G]$ 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. **Construire**
a) un isomorphisme de l'anneau $\mathbb{Z}[X]/(X^p-1)$ sur A,

b) un isomorphisme de l'anneau des entiers du corps $\mathbb{Q}(e^{2i\pi/p})$ sur $\tilde{A}$.

2) Soient $E = \mathbb{Q}(e^{2i\pi/23})$ **et** $L = E \cap \mathbb{R}$.
a) Déterminer le degré des extensions $E/\mathbb{Q}$ et $L/\mathbb{Q}$.

b) Montrez que l'extension $L/\mathbb{Q}$ est cyclique.

3) On note U_E **le groupe des unités de** E **et** U_L **celui des unités de** L.
a) Montrer que l'on a des isomorphismes

$$U_E \ \simeq \ (\mathbb{Z}/a\mathbb{Z}) \times \mathbb{Z}^b \text{ et } U_L \ \simeq \ (\mathbb{Z}/a'\mathbb{Z}) \times \mathbb{Z}^{b'}$$

où a, b, a', b' sont des entiers que l'on déterminera.

b) Montrer que U_E/U_L est un groupe fini.

4) On pose $V_L = \mathbb{Q} \otimes_{\mathbb{Z}} U_L$ **(attention : n'importe quel groupe abélien peut-être considéré comme un** $\mathbb{Z}$**-module. Quand c'est le groupe multiplicatif des éléments inversibles d'un anneau commutatif, il est noté multiplicativement et, par conséquent, si** $u, v \in U_L$, **on a** $1\otimes u + 1\otimes v = 1\otimes uv$**). On note** $\rho \ : \ U_L \ \to \ V_L$ **l'application qui envoie** u **sur** $1\otimes u$. **Montrez que**
a) ρ est un homomorphisme de groupes dont le noyau est un groupe cyclique d'ordre 2,

b) V_L est un $\mathbb{Q}$-espace vectoriel de dimension 10,

c) l'image $\tilde{U}$ de ρ est un réseau de V_L (c'est-à-dire un sous-$\mathbb{Z}$-module de type fini qui engendre V_L).

Dans la suite, $G = \mathrm{Gal}(L/\mathbb{Q})$ **et** A **et** $\tilde{A}$ **sont comme dans la question 1. On note** $\tilde{K}$ **le corps des fractions de** $\tilde{A}$.
5) Pour tout $\alpha \in A$ **de la forme**

$$\alpha = \sum_{\sigma\in G} a_\sigma\sigma,$$

avec les $a_\sigma \in \mathbb{Z}$, **et tout** $u \in U_L$, **on pose**

$$\alpha.u \ := \ \Pi_{\sigma\in G}\sigma(u)^{a_\sigma} \ .$$

a) Montrer que ceci muni U_L d'une structure de A-module.

b) En déduire une structure de $\tilde{A}$-module sur $\tilde{U}$ et de $\tilde{K}$-espace vectoriel sur V_L.

c) Montrer que V_L est de dimension 1 sur $\tilde{K}$.

d) Montrer que pour tout $u \in V_L$ différent de l'élément-neutre, $\{\lambda \in \tilde{K} \mid \lambda u \in \tilde{U}\}$ est un idéal fractionnaire $\mathfrak{a}_u$ de l'anneau de Dedekind $\tilde{A}$ et que l'application $\lambda \mapsto \lambda u$ est une bijection de $\mathfrak{a}_u$ sur $\tilde{U}$.

6) On pose $u_0 := 2\cos(2i\pi/23)$.
a) Montrez que $u_0 \in U_L$. **Indication** *On pourra poser* $\varepsilon = e^{2i\pi/23}$, *montrer que* $u_0 = \varepsilon^{-1}(\varepsilon^4 - 1)/(\varepsilon^2 - 1)$ *et vérifier que, pour toute valuation ultramétrique* v *de* E, *on a* $v(\varepsilon^4 - 1) = v(\varepsilon^2 - 1)$.

b) Montrer que le sous-groupe de U_L engendreé par les $\sigma(u_0)$ pour $\sigma \in G$ est d'indice fini dans U_L.