**Université Paris Sud** **Année 2005-2006**

**M1** **Arithmétique**

# Examen du 16 juin 2006

# 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 deux parties sont indépendantes.**
**Documents non autorisés. Notations et rappels :**

**Pour tout corps de nombres** $E$, **on note** $\mathcal{O}_E$ **l'anneau des entiers,** $d_E$ **son discriminant,** $Pic(\mathcal{O}_E)$ **le groupe des classes d'idéaux.**

**On dit qu'un sous-anneau** $A$ **de** $\mathcal{O}_E$ **dont le corps des fractions est** $E$ **est** *p-clos* **s'il est dense dans**

$$\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}_E \simeq \varprojlim_{n\in\mathbb{N}} \mathcal{O}_E/p^n .$$

**(cela revient à dire que, si** $S$ **est l'ensemble des entiers naturels premiers à** $p$, **alors** $S^{-1}A$ **est intégralement clos).**

**Pour tout idéal fractionnaire** $\mathfrak{a}$ **de** $\mathcal{O}_E$, **on note** $\overline{\mathfrak{a}}$ **son image dans** $Pic(\mathcal{O}_E)$. **Pour tout idéal** $\mathfrak{a}$ **de** $\mathcal{O}_E$, **on note** $N(\mathfrak{a})$ **sa norme (c'est donc le nombre d'éléments de l'anneau** $\mathcal{O}_E/\mathfrak{a}$**). On rappelle que, pour tout idéal fractionnaire** $\mathfrak{a}$, **il existe un idéal** $\mathfrak{b}$ **de** $\mathcal{O}_E$ **vérifiant**

$$\overline{\mathfrak{b}} = \overline{\mathfrak{a}} \text{ et } N(\mathfrak{b}) < \frac{d!}{d^d}(\frac{4}{\pi})^{r_2}\sqrt{d_E}$$

**où** $d = [E:\mathbb{Q}] = r_1 + 2r_2$ **avec** $r_1$ **le nombre de plongements réels.**

**Si** $[E:\mathbb{Q}] = 2$ **(on dit alors que l'extension** $E/\mathbb{Q}$ **est quadratique), on dit qu'un nombre premier** $p$ **est** *inerte* **si** $p\mathcal{O}_E$ **est un idéal premier de** $\mathcal{O}_E$ **et qu'il est** *décomposé* **s'il n'est ni inerte ni ramifié.**

**Pour tout nombre premier** $p \neq 2$ **et tout entier** $n$ **premier à** $p$, **le** *symbole de Legendre* $\left(\frac{n}{p}\right)$ **est défini par** $\left(\frac{n}{p}\right) = 1$ **si** $n$ **est un carré modulo** $p$ **et** $\left(\frac{n}{p}\right) = -1$ **sinon. On rappelle que :**

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} , \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} ,$$

**que, si $\ell$ est un nombre premier différent de $2$ et $p$,**

$$\left(\frac{\ell}{p}\right) \;=\; (-1)^{\frac{\ell-1}{2}\cdot\frac{p-1}{2}}\left(\frac{p}{\ell}\right)\;,$$

**et que, si**

$$S \;=\; \sum_{n=1}^{p-1}\left(\frac{n}{p}\right)e^{2i\pi/p},$$

**on a**

$$S^2 = (-1)^{(p-1)/2}p\;.$$

**Pour tout nombre premier $p$, si $a, b \in \mathbb{Q}_p$ sont non nuls, le** *symbole de Hilbert* $(a,b)_p$ **est égal à $1$ s'il existe $x, y, z \in \mathbb{Q}_p$, pas tous nuls tels que $z^2 = ax^2 + by^2$ et à $-1$ sinon. On rappelle que, si $p \neq 2$, $a = p^r u$ et $b = p^s v$, avec $r, s \in \mathbb{Z}$ et $u, v$ des unités $p$-adiques, on a**

$$(a,b)_p \;=\; (-1)^{\frac{p-1}{2}rs}(\frac{u}{p})^s(\frac{v}{p})^r\;.$$

**Exercice A**

**Dans ce problème, $L$ est un corps de nombres. On choisit $\alpha \in \mathcal{O}_L$ tel que $L = \mathbb{Q}(\alpha)$, on note $P$ le polynôme minimal de $\alpha$ sur $\mathbb{Q}$ et, pour tout nombre premier $p$, on note $P_p$ l'image de $P$ dans $\mathbb{F}_p[X]$.**

**1 .a)** Expliquer brièvement pourquoi, si $p$ est un nombre premier tel que $P_p$ est séparable, alors $p$ est non ramifié et $\mathbb{Z}[\alpha]$ est $p$-clos.

**b)** Montrer que si $L/\mathbb{Q}$ est non ramifiée en $p$ et si $\mathbb{Z}[\alpha]$ est $p$-clos, alors le polynôme $P_p$ est séparable.

**2) On pose $d = [L/\mathbb{Q}]$. Soit $p$ un nombre premier tel qu'il y a $d$ idéaux premiers de $\mathcal{O}_L$ au dessus de $p$.**

Montrer que, pour qu'il existe $\beta \in \mathcal{O}_L$ tel que $L = \mathbb{Q}(\beta)$ et $\mathbb{Z}[\beta]$ est $p$-clos, il faut et il suffit que $d \leq p$. **Indication** *Pour montrer que la condition est suffisante, on pourra commencer par vérifier que, si $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_d$ sont les idéaux premiers de $\mathcal{O}_L$ au-dessus de $p$, il existe $\beta \in \mathcal{O}_L$ tel que $\beta - i \in \mathfrak{p}_i$, pour $i = 1, 2, \ldots, d$).*

**3)** Soit $p$ un nombre premier et $Q$ un polynôme à coefficients dans $\mathbb{Z}_p$. Montrer que, si $a, b \in \mathbb{Z}_p$, alors $Q(a+b) - Q(a) - bQ'(a)$ appartient au carré de l'idéal engendré par $b$.

**4)** Soit $R$ un polynôme à coefficients dans $\mathbb{Z}_2$. Montrer que le polynôme $T = X(X^2-1) + 4R$ a exactement trois racines distinctes dans $\mathbb{Z}_2$. **Indication** *Pour $i = -1, 0, 1$, construire une suite d'entiers naturels $(u_{i,n})_{n\in\mathbb{N}}$ telle que $u_{i,0} = i$ et $T(u_{i,n})$ tend vers $0$ lorsque $n$ tend vers l'infini.*

**5)** Donner un exemple d'extension $L$ de $\mathbb{Q}$ de degré $3$ telle qu'il n'existe pas de $\beta \in \mathcal{O}_L$ vérifiant $L = \mathbb{Q}(\beta)$ et $\mathbb{Z}[\beta]$ est $2$-clos. Donner une base de $\mathcal{O}_L$ sur $\mathbb{Z}$.

**Exercice B**

**Dans tout ce problème, $N$ est un entier sans facteur carré congru à $2$ ou à $3$ modulo $4$. On choisit une racine carrée $\alpha \in \mathbb{C}$ de $N$ et on pose $E = \mathbb{Q}(\alpha)$.**

**1)** Montrer que $\mathcal{O}_E$ est un $\mathbb{Z}$-module libre de base $\{1, \alpha\}$ et calculer $d_E$.

**2)** Montrer que si $N > 0$, pour tout idéal fractionnaire $\mathfrak{a}$ de $\mathcal{O}_E$, il existe un idéal $\mathfrak{b}$ de $\mathcal{O}_E$ tel que $N(\mathfrak{b}) \leq \sqrt{N}$.

**3)** Montrer que $E \subset \mathbb{Q}(e^{2i\pi/4N})$.

**4 .a)** Déterminer les $p$ qui sont ramifiés dans l'extension $E/\mathbb{Q}$.
**b)** Pour chacun d'eux, si $\mathfrak{p}$ est l'idéal premier de $\mathcal{O}_E$ au-dessus de $p$, calculer $N(\mathfrak{p})$ et montrer que $\overline{\mathfrak{p}}^2 = 1$.

**5 .a)** Exprimer en fonction du symbole de Legendre le fait qu'un nombre premier $p$ non ramifié est inerte ou décomposé dans l'extension $E/\mathbb{Q}$, le nombre d'idéaux premiers de $\mathcal{O}_E$ au-dessus de $p$ et la norme de chacun d'eux.
**b)** Montrer que, si $p$ est inerte et $\mathfrak{p}$ est au-dessus de $p$, alors $\overline{\mathfrak{p}} = 1$.

**c)** Montrer que si $p$ est décomposé et si $\mathfrak{p}_1, \mathfrak{p}_2$ sont les idéaux premiers au-dessus de $p$, alors $\overline{\mathfrak{p}}_1\overline{\mathfrak{p}}_2 = 1$.

**6) On considère la série de Dirichlet**

$$\zeta_E(s) \ := \ \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

**où $a_n$ est égal au nombres d'idéaux de $\mathcal{O}_E$ de norme $n$.**
**a)** Montrer que $a_{mn} = a_m a_n$ si $m$ et $n$ sont premiers entre eux.

**b)** Pour tout nombre premier $p$ et tout $r \in \mathbb{N}$, calculer $a_{p^r}$ (on distinguera suivant que $p$ est ramifié, inerte ou décomposé).

**c)** Montrer que la série $\zeta_E(s)$ admet un produit eulérien

$$\zeta_E(s) \ = \ \Pi_{p \in P} \zeta_{E,p}(s)$$

où $P$ est l'ensemble des nombres premiers et où

$$\zeta_{E,p}(s) \ = \ \left\{ \begin{pmatrix} \frac{1}{1-p^{-s}} & \text{si } p \text{ est ramifié,} \\ \frac{1}{1-p^{-2s}} & \text{si } p \text{ est inerte,} \\ \frac{1}{(1-p^{-s})^2} & \text{si } p \text{ est décomposé.} \end{pmatrix} \right.$$

**Indication** *On pourra remarquer que*

$$\frac{1}{(1-X)^2} \ = \ \sum_{r=0}^{\infty} (r+1) X^r \ .$$

**7 .a)** Montrer que $\zeta_E(s) = \zeta(s)\zeta_1(s)$ où $\zeta(s)$ est la fonction zéta de Riemann et où $\zeta_1(s)$ est une série de Dirichlet que l'on déterminera.
**b)** On a vu que $E \subset \mathbb{Q}(e^{2i\pi/4N})$ et on sait que le groupe de Galois de $\mathbb{Q}(e^{2i\pi/4N})/\mathbb{Q}$ s'identifie au groupe $(\mathbb{Z}/4N\mathbb{Z})^*$. Montrer que $\zeta_1(s) = L(s,\chi)$ où $\chi$ est l'unique caractère de Dirichlet modulo $4N$ qui est tel que l'homomorphisme $(\mathbb{Z}/4N\mathbb{Z})^* \to \mathbb{C}^*$ qu'il induit se factorise à travers l'unique homomorphisme non trivial $\mathrm{Gal}(E/\mathbb{Q}) \to \mathbb{C}^*$.

**c)** Montrer que l'abscisse de convergence de $\zeta_E(s)$ est $1$ et que cette fonction se prolonge en une fonction méromorphe pour $\mathcal{R}](s) > 0$ avec comme seule singularité un pôle simple en $s = 1$.

**8) On suppose que** $N = 15$.
**a)** Montrer que le groupe $Pic(\mathcal{O}_E)$ est d'ordre inférieur ou égal à $3$ (utiliser (2) et (5)).

**b)** Montrer qu'il y a un seul idéal $\mathfrak{p}$ de $\mathcal{O}_E$ au-dessus de $3$, que $\overline{\mathfrak{p}}^2 = 1$ et que $\mathfrak{p}$ est le $\mathbb{Z}$-module libre de base $3$ et $\alpha$.

**c)** Supposons que $\overline{\mathfrak{p}} = 1$. Montrer que ceci implique qu'il existe $u, v \in \mathbb{Z}$ tels que $5v^2 - 3u^2 \in \{-1, 1\}$. **Indication** *Ecrire un générateur de* $\mathfrak{p}$ *sous la forme* $\beta = 3u + \alpha v$.

**d)** Calculer les symboles de Hilbert $(3,-5)_2$ et $(-3,5)_3$. En déduire que $\overline{\mathfrak{p}} \neq 1$.

**e)** Montrer que $Pic(\mathcal{O}_E)$ est un groupe d'ordre $2$.