Université P. et M. Curie (Paris VI), Deuxième semestre 2004/2005

Michel Waldschmidt

Master de sciences et technologies 1ère année - Mention : Mathématiques et applications
Spécialité : Mathématiques Fondamentales MO11 : Théorie des nombres (12 ECTS)

*Examen écrit:* 13 Septembre 2005

Durée: 3 heures
*Seul document autorisé: le polycopié*

**1.** Soit $p$ l'un des 4 nombres premiers 2, 3, 5, 7 et soit $\Phi_p$ le polynôme cyclotomique d'indice $p$. Quels sont les degrés des facteurs irréductibles dans la décomposition de $\Phi_p$ sur chacun des corps $\mathbf{F}_2$, $\mathbf{F}_3$, $\mathbf{F}_5$, $\mathbf{F}_7$?
*(N.B.: Il y a donc 16 réponses à donner).*
Dans chacun des cas où $\Phi_p$ n'est pas irréductible, expliciter sa décomposition en facteurs irréductibles.

**2.** Soit $L/K$ une extension de corps et soit $\alpha$ un élément de $L$ algébrique sur $K$. On suppose que le degré de $\alpha$ sur $K$ est impair. Vérifier $K(\alpha) = K(\alpha^2)$.

**3.** Soit $\mathbf{Z}_k$ l'anneau des entiers du corps quadratique imaginaire $k = \mathbf{Q}(\sqrt{-31})$.
a) Quel est le discriminant de $\mathbf{Z}_k$?
b) Donner une base de $\mathbf{Z}_k$ comme $\mathbf{Z}$-module.
c) Quelles sont les unités de $\mathbf{Z}_k$?
d) Écrire la décomposition de l'idéal (2) de $\mathbf{Z}_k$ en idéaux premiers.
e) Soit $\mathfrak{p}$ un idéal premier de $\mathbf{Z}_k$ contenant 2.
Quelle est la norme de $\mathfrak{p}$?
Quel est le corps résiduel de $\mathfrak{p}$?
Expliciter une uniformisante pour la valuation ultramétrique $v_{\mathfrak{p}}$.
Calculer $v_{\mathfrak{p}}(\sqrt{-31})$.

**4.** Soient $a$ et $b$ deux nombres entiers et $p$ un nombre premier. Montrer que le polynôme $(X^2-a)(X^2-b)(X^2-ab)$ a une racine dans $\mathbf{F}_p$.
Peut-on affirmer que si $f$ est un polynôme unitaire dans $\mathbf{Z}[X]$ qui a une racine dans $\mathbf{F}_p$ pour tout nombre premier, alors $f$ a une racine dans $\mathbf{Z}$?

**5.** Soit $k$ le corps de décomposition sur $\mathbf{Q}$ du polynôme $X^4 - 2$.
a) Quel est le degré de $k$ sur $\mathbf{Q}$?
b) Quel est le rang du groupe des unités de $k$?
c) Quel est le groupe de Galois de $k$ sur $\mathbf{Q}$?
d) Combien $k$ a-t-il de sous-corps?

**6.** Quand $f$ est une fonction arithmétique on lui associe une série de Dirichlet

$$D(f;s) = \sum_{n\geq 1} \frac{f(n)}{n^s}\cdot$$

a) En utilisant la fonction zêta de Riemann, expliciter les séries de Dirichlet associées à chacune des fonctions arithmétiques suivantes:

- $f_\alpha(n) = n^\alpha$, quand $\alpha$ est un nombre complexe.
- $\delta(n) = \begin{cases} 1 & \text{pour } n = 1 \\ 0 & \text{pour } n \geq 2 \end{cases}$
- $\kappa(n) = \begin{cases} 1 & \text{si } n \text{ est un carré,} \\ 0 & \text{sinon,} \end{cases}$
- $g_\alpha(n) = \sum_{d|n} d^\alpha$, quand $\alpha$ est un nombre complexe.

b) On désigne par $\varphi$ l'indicatrice d'Euler et par $\mu$ la fonction de Möbius:

$$\varphi(n) = \sum_{\substack{1\leq k\leq n \\ (k,n)=1}} 1 \text{ et } \mu(n) = \begin{cases} (-1)^{\omega(n)} & \text{si } n \text{ est sans facteur carré,} \\ 0 & \text{sinon,} \end{cases}$$

avec $\omega(n) = \sum_{p|n} 1$.
Vérifier

$$\sum_{d|n} \mu(d) = \delta(n) \qquad \text{et} \qquad \sum_{d|n} \mu(d)\frac{n}{d} = \varphi(n).$$

c) Expliciter les séries de Dirichlet associées aux fonctions $\mu$ et $\varphi$.