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

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

Examen écrit: 6 Juin 2005
Ébauche de corrigé

1.
a) Le polynôme cyclotomique Φ_8 est de degré $\varphi(8) = 4$ et

$$\Phi_1(X)\Phi_2(X)\Phi_4(X)\Phi_8(X) = X^8 - 1.$$

Comme $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$ et $\Phi_4(X) = X^2 + 1$ on trouve $\Phi_8(X) = X^4 + 1$. On peut aussi le voir en utilisant le fait que ses racines sont les racines primitives d'ordre 8 de l'unité.
b) Quand p est un nombre impair sa classe modulo 8 est 1, 3, 5 ou 7 donc appartient à $(\mathbf{Z}/8\mathbf{Z})^\times$. La classe de 1 modulo 8 est d'ordre 1 (c'est l''élément neutre), les autres sont d'ordre 2.
c) Si p est impair les degrés des facteurs irréductibles de $\Phi_8(X)$ dans $\mathbf{F}_p[X]$ sont égaux à l'ordre de p modulo 8, donc valent tous 1 si $p \equiv 1 \pmod 8$ et 2 sinon. Si $p = 2$ ces degrés valent 1 puisque $X^4 + 1 = (X + 1)^4$ dans $\mathbf{F}_2[X]$.
d) Le polynôme cyclotomique Φ_8 est irréductible de $\mathbf{Z}[X]$ et pour tout nombre premier p l'image de f dans $\mathbf{F}_p[X]$ est réductible.

2. Soit F le corps

$$F = \mathbf{Q}\left(\sqrt{2},\ \sqrt{7},\ \sqrt{3+\sqrt{2}}\right).$$

a) Posons $\vartheta = \sqrt{3+\sqrt{2}}$. Le nombre ϑ est racine du polynôme

$$f(X) = (X^2 - 3)^2 - 2 = X^4 - 6X^2 + 7.$$

Les racines de ce polynôme sont ϑ, $-\vartheta$, ϑ' et $-\vartheta'$, avec $\vartheta' = \sqrt{3-\sqrt{2}}$. On a $\vartheta\vartheta' = \sqrt{7}$. Le corps F est donc le corps de décomposition sur $\mathbf{Q}$ du polynôme $(X^2 - 2)(X^2 - 7)f(X)$, c'est par conséquent une extension normale de $\mathbf{Q}$.

Comme F est de caractéristique nulle l'extension $F/\mathbf{Q}$ est séparable; elle est donc galoisienne.
b) Montrons d'abord que l'extension $F/\mathbf{Q}$ est de degré 8 sur $\mathbf{Q}$. On sait que le corps $K = \mathbf{Q}(\sqrt{2},\ \sqrt{7})$ est une extension de $\mathbf{Q}$ de degré 4, c'est à dire que 1, $\sqrt{2}$, $\sqrt{7}$, $\sqrt{14}$ sont linéairement indépendants sur $\mathbf{Q}$ (le calcul est facile).

On commence par remarquer que si a, b et c sont des éléments de $\mathbf{Q}(\sqrt{2})$ tels que $(a + b\sqrt{7})^2 = c$, alors $ab = 0$. On applique ceci avec $c = 3 + \sqrt{2}$ et on vérifie ainsi par un petit calcul que c n'est pas un carré dans K. Donc F est une extension quadratique de K et de degré 8 sur $\mathbf{Q}$.

Comme $\sqrt{2} = \vartheta^2 - 3$ on a encore $F = \mathbf{Q}\left(\sqrt{7},\ \sqrt{3+\sqrt{2}}\right)$.

Le corps F est une extension quadratique, donc galoisienne, de K. Soit α l'élément non trivial du groupe de Galois de F sur K. De même soit β l'élément non trivial du groupe de Galois de F sur $\mathbf{Q}(\vartheta)$.

Enfin F est une extension de $\mathbf{Q}(\sqrt{7})$ de degré 4, donc le polynôme $f(X) = X^4 - 6X^2 + 7$ est irréductible dans $\mathbf{Q}(\sqrt{7})[X]$ et les conjuguées de ϑ sur $\mathbf{Q}(\sqrt{7})$ sont ϑ, $-\vartheta$, ϑ' et $-\vartheta'$. Comme ϑ' est conjugué de ϑ sur $\mathbf{Q}(\sqrt{7})$ il existe un élément γ du groupe de Galois de F sur $\mathbf{Q}$ tel que $\gamma(\sqrt{7}) = \sqrt{7}$ et $\gamma(\vartheta) = \vartheta'$. On a alors $\gamma(3+\sqrt{2}) = \gamma(\vartheta^2) = \vartheta'^2 = 3 - \sqrt{2}$, donc $\gamma(\sqrt{2}) = -\sqrt{2}$.

Ainsi les trois automorphismes α, β, γ de F vérifient

$$\begin{array}{lll}
\alpha(\sqrt{2}) = \sqrt{2} & \alpha(\sqrt{7}) = \sqrt{7} & \alpha(\sqrt{3+\sqrt{2}}) = -\sqrt{3+\sqrt{2}} \\
\beta(\sqrt{2}) = \sqrt{2} & \beta(\sqrt{7}) = -\sqrt{7} & \beta(\sqrt{3+\sqrt{2}}) = \sqrt{3+\sqrt{2}} \\
\gamma(\sqrt{2}) = -\sqrt{2} & \gamma(\sqrt{7}) = \sqrt{7} & \gamma(\sqrt{3+\sqrt{2}}) = \sqrt{3-\sqrt{2}}.
\end{array}$$

c) Les relations

$$\alpha^2 = 1, \quad \beta^2 = 1, \quad \gamma^2 = 1, \quad \beta\gamma = \alpha\gamma\beta, \quad \alpha\beta = \beta\alpha, \quad \alpha\gamma = \gamma\alpha.$$

sont faciles à vérifier à partir de ce qui précède (le point essentiel est de calculer l'image de ϑ' par ces automorphismes en utilisant $\vartheta\vartheta' = \sqrt{7}$).

d) Le groupe de Galois G de F sur $\mathbf{Q}$ a 8 éléments; on vérifie que ce sont

$$\{1, \ \alpha, \ \beta, \ \gamma, \ \alpha\beta, \ \alpha\gamma, \ \beta\gamma, \ \alpha\beta\gamma\}.$$

Le centre de G est $\{1, \alpha\}$, le quotient de G par son centre est isomorphe à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ (des générateurs sont les classes de β et γ)

3. Soit $\mathbf{Z}_k$ l'anneau des entiers du corps quadratique imaginaire $k = \mathbf{Q}(\sqrt{-23})$.

a) Le discriminant de $\mathbf{Z}_k$ est -23

b) Une base de $\mathbf{Z}_k$ comme $\mathbf{Z}$-module est 1, $(1+\sqrt{-23})/2$.

c) Les unités de $\mathbf{Z}_k$ sont ± 1.

d) L'idéal (2) de $\mathbf{Z}_k$ est décomposé dans k en $(2) = \mathfrak{p}\mathfrak{p}'$ avec $\mathfrak{p} = (2, (1+\sqrt{-23})/2)$ et $\mathfrak{p}' = (2, (1-\sqrt{-23})/2)$.

e) La norme de $\mathfrak{p}$ ainsi que celle de $\mathfrak{p}'$ est 2.

Le corps résiduel de $\mathfrak{p}$ est le corps $\mathbf{F}_2$ à 2 éléments.

Une uniformisante pour la valuation ultramétrique $v_{\mathfrak{p}}$ est 2.

On a $v_{\mathfrak{p}}(\sqrt{-23}) = 0$.

f) L'idéal $\mathfrak{p}$ n'est pas principal (il n'y a pas d'entier dans k de norme 2), on a $\mathfrak{p}^2 = (4, (-3+\sqrt{-23})/2)$ tandis que $\mathfrak{p}^3$ est principal engendré par $(-3+\sqrt{-23})/2$. Donc la classe de $\mathfrak{p}$ est d'ordre 3 dans le groupe des classes d'idéaux de k. D'un autre côté le théorème de Minkowski montre que toute classe d'idéaux contient un idéal entier de norme au plus 3, le groupe des classes a donc au plus 5 éléments; comme ce nombre est multiple de 3 on conclut que le nombre de classes de k est 3.

4.

a) Soit t un nombre réel. L'abscisse de convergence de la série de Dirichlet

$$\sum_{n \geq 1} \frac{(-1)^n + n^t}{n^s}$$

est

$$\sigma_c = \max\{0, 1+t\} = \begin{cases} 0 & \text{si } t \leq -1 \\ 1+t & \text{si } t \geq -1 \end{cases}$$

et son abscisse de convergence absolue

$$\sigma_a = \max\{1, 1+t\} = \begin{cases} 1 & \text{si } t \leq 0 \\ 1+t & \text{si } t \geq 0. \end{cases}$$

b) Soit

$$\sum_{n\geq 1} \frac{a_n}{n^s}$$

une série de Dirichlet. On note σ_c son abscisse de convergence et σ_a son abscisse de convergence absolue. La majoration $\sigma_c \leq \sigma_a$ résulte des définitions et du fait qu'une série absolument convergente est convergente. Pour démontrer l'inégalité $\sigma_a \leq \sigma_c + 1$, on se ramène (en remplaçant a_n par $a_n n^{-\sigma_c}$) au cas où $\sigma_c = 0$. Soit $\epsilon > 0$. La série de terme général a_n/n^ϵ converge, donc son terme général tend vers 0, par conséquent la série de terme général $|a_n|/n^{1+2\epsilon}$ converge, d'où on déduit $\sigma_a \leq 1$.

L'exemple a) montre que les inégalités

$$\sigma_c \leq \sigma_a \leq \sigma_c + 1$$

sont optimales.