Université Paris Diderot
Université Pierre et Marie Curie

Théorie algébrique des nombres
M2 mathématiques – Année 2013-14

Examen du 20 décembre 2013

Durée : 3h

Soit K un corps décomposition du polynôme $X^3 - 3$ sur $\mathbf{Q}$. Posons $G = \mathrm{Gal}(K/\mathbf{Q})$. Pour p premier non ramifié dans K, notons $C(p)$ la classe de conjugaison dans G d'une substitution de Frobenius en p. Notons ζ_K la fonction ζ de K et posons $\zeta_K(s) = \sum_{n=1}^{\infty} a_n n^{-s}$. Notons d le degré de l'extension $K|\mathbf{Q}$.

I

1. Montrer que le polynôme $X^3 - 3$ est irréductible sur $\mathbf{Q}$.

2. Montrer que K contient une racine cubique primitive de 1, notée j, et que $K = \mathbf{Q}(\alpha, j)$ où $\alpha \in K$ vérifie $\alpha^3 - 3 = 0$.

3. En déduire que $d = 6$. Quels sont les nombres de plongements réels et complexes non réels de K ?

4. Notons μ_3 le groupe formé par les racines cubiques de l'unité dans $\mathbf{Q}(j)$. Montrer que l'application $\mathrm{Gal}(K/\mathbf{Q}(j)) \to \mu_3$ qui à σ associe $\sigma(\alpha)/\alpha$ est un isomorphisme de groupes. En déduire que $\mathrm{Gal}(K/\mathbf{Q})$ est un groupe diédral d'ordre 6. Il est engendré par deux éléments τ et ϵ, qui vérifient $\tau^3 = 1$, $\epsilon\tau\epsilon = \tau^{-1}$ et $\epsilon^2 = 1$. On pourra caractériser τ et ϵ par $\tau(\alpha) = j\alpha$, $\tau(j) = j$, $\epsilon(j) = j^{-1}$ et $\epsilon(\alpha) = \alpha$.

5. Montrer que les extensions $\mathbf{Q}(\alpha)|\mathbf{Q}$ et $\mathbf{Q}(j)|\mathbf{Q}$ sont non ramifiées en dehors de 3. En déduire que l'extension $K|\mathbf{Q}$ est non ramifiée en dehors de 3. Montrer que l'extension $K|\mathbf{Q}$ est totalement ramifiée en 3.

6. Montrer que les classes de conjugaison de G sont $C_1 = \{1\}$, $C_2 = \{\tau, \tau^{-1}\}$, $C_3 = \{\epsilon, \epsilon\tau, \epsilon\tau^2\}$.

7. Soit p un nombre premier > 3.

7.a Montrer que $C(p) = C_1$ si et seulement si on a simultanément que 3 est un cube modulo p et que -3 est un carré modulo p. Ou encore si et seulement si on a $p \equiv 1 \pmod 3$ et $3^{(p-1)/3} \equiv 1 \pmod p$.

7.b Montrer que $C(p) = C_2$ si et seulement si on a simultanément que -3 est un carré et 3 n'est pas un cube modulo p. Ou encore si et seulement si on a $p \equiv 1 \pmod 3$ et on n'a pas $3^{(p-1)/3} \equiv 1 \pmod p$.

7.c Montrer que $C(p) = C_3$ si et seulement si on a simultanément que -3 n'est pas un carré modulo p et que 3 est un cube modulo p. Ou encore si et seulement si on a $p \equiv -1 \pmod 3$.

8. Calculer les densités analytiques des ensembles de nombres premiers $\{p/C(p) = C_i\}$, pour $i = 1, 2, 3$. Dans chaque cas, indiquer le degré résiduel en p de l'extension $K|\mathbf{Q}$.

9. Quel est le degré de l'extension $\mathbf{Q}(\alpha)|\mathbf{Q}$? Quelle est la densité analytique de l'ensemble des nombres premiers p qui ont un diviseur premier de degré 1 dans le corps $\mathbf{Q}(\alpha)$?

10. Déterminer $C(2)$, $C(5)$, $C(7)$. En déduire les coefficients a_n de ζ_K pour $1 \leq n \leq 10$.

11. Donner le résidu en $s = 1$ de la fonction zêta de $\mathbf{Q}(j)$ grâce à la formule du nombre de classes. En déduire la valeur en $s = 1$ de la fonction $L(\chi, s)$ où χ est le caractère de Dirichlet non trivial modulo 3.

12. Notons K_3 et $\mathbf{Q}_3(j)$ les complétés de K et $\mathbf{Q}(j)$ en leurs uniques idéaux maximaux au dessus de 3. Lesquelles des extensions $K_3|\mathbf{Q}_3$, $K_3|\mathbf{Q}_3(j)$ et $\mathbf{Q}_3(j)|\mathbf{Q}_3$ sont abéliennes ?

13. Quelle est l'image de l'application norme $\mathrm{N}_{\mathbf{Q}_3(j)/\mathbf{Q}_3} : \mathbf{Q}_3(j)^* \to \mathbf{Q}_3^*$?

II

Soit V un $\mathbf{C}$-espace vectoriel de dimension finie d. Soit $\rho : G \to \mathrm{GL}(V)$ un homomorphisme de groupes. On dit alors que ρ est une *représentation de dimension d*. Soit p un nombre premier. Soient I_p un sous-groupe d'inertie en p de G et $\phi_p \in G/I_p$ une substitution de Frobenius. Posons $W = V^{I_p} = \{v \in V / \rho(g)(v) = v (g \in I_p)\}$. Posons, pour $s \in \mathbf{C}$, $L_p(\rho, s) = 1/\det(I_W - \rho(\phi_p)p^{-s})$, où I_W est l'endomorphisme identité de W.

14. Montrer que $L_p(\rho, s)$ ne dépend que de p (et pas du choix de ϕ_p) et qu'il s'écrit $\prod_\alpha (1 - \alpha p^{-s})^{-1}$ où α parcourt un nombre d_p de nombres complexes de module 1. Montrer qu'on a $d_p \leq d$ pour tout p, et $d_p = d$ pour presque tout p.

15. Montrer que le produit $L(\rho, s) = \prod_p L_p(\rho, s)$ converge vers une fonction holomorphe sur le demi-plan $\{s \in \mathbf{C} / \Re(s) > 1\}$.

16. Soit V_0 le $\mathbf{C}$-espace vectoriel de base $(e_\sigma)_{\sigma \in G}$. Notons $\rho_0 : G \to \mathrm{GL}(V_0)$ la représentation telle que $\rho_0(\sigma)(e_\eta) = e_{\sigma\eta}$. Suivant la valeur de i, quel est le polynôme caractéristique de $\rho_0(\sigma)$ si $\sigma \in C_i$?

17. Calculer $L_3(\rho_0, s)$. Calculer $L_p(\rho_0, s)$ suivant la valeur de $C(p)$ pour $p \neq 3$.

18. Montrer qu'on a $\zeta_K(s) = L(\rho_0, s)$.

19. Soient ρ_1 et ρ_2 deux représentations de G de dimensions finies. Montrer qu'on a $L(\rho_1 \times \rho_2, s) = L(\rho_1, s)L(\rho_2, s)$ (où $(\rho_1 \times \rho_2)(g) = \rho_1(g) \times \rho_2(g)$ opérant sur l'espace vectoriel produit).

20. Montrer qu'on peut écrire $V_0 = V_1 \oplus V_2 \oplus V_3$, où V_1, V_2 et V_3 donnent lieu à des représentations ρ_1, ρ_2 et ρ_3 de G dimensions 1, 1 et 4 respectivement, avec ρ_1 constante égale à l'identité I_{V_1}. Montrer que $L(\rho_2, s)$ et $L(\rho_3, s)$ admettent des prolongements holomorphes au voisinage de $s = 1$, et même à $\mathbf{C}$.