Université Paris Diderot
Université Pierre et Marie Curie

Théorie algébrique des nombres
M2 mathématiques – Année 2012-13

Examen du 18 décembre 2012

Durée : 3h

Soit K un corps décomposition du polynôme X^4-2 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 $K|\mathbf{Q}$.

1. Montrer que le polynôme X^4-2 est irréductible sur $\mathbf{Q}$.

2. Montrer que K contient une racine carrée de -1, notée i et que $K=\mathbf{Q}(\alpha,i)$ où $\alpha\in K$ vérifie $\alpha^4-2=0$.

3. En déduire que $d=8$. Quels sont les nombres de plongements réels et complexes non réels de K ?

4. Notons μ_4 le groupe formé par les racines quatrièmes de l'unité dans $\mathbf{Q}(i)$. Montrer que l'application $\mathrm{Gal}(K/\mathbf{Q}(i))\to\mu_4$ 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 8. Il est engendré par deux éléments τ et ϵ, qui vérifient $\tau^4=1$, $\epsilon\tau\epsilon=\tau^{-1}$ et $\epsilon^2=1$. On pourra caractériser τ et ϵ par $\tau(\alpha)=i\alpha$, $\tau(i)=i$, $\epsilon(i)=-i$ et $\epsilon(\alpha)=\alpha$.

5. Montrer que les extensions $\mathbf{Q}(\alpha)|\mathbf{Q}$ et $\mathbf{Q}(i)|\mathbf{Q}$ sont non ramifiées en dehors de 2. En déduire que l'extension $K|\mathbf{Q}$ est non ramifiée en dehors de 2. Montrer que l'extension $K|\mathbf{Q}$ est totalement ramifiée en 2.

6. Montrer que les classes de conjugaison de G sont $C_1=\{1\}$, $C_2=\{\tau^2\}$, $C_3=\{\tau,\tau^{-1}\}$, $C_5=\{\epsilon,\epsilon\tau^2\}$ et $C_6=\{\epsilon\tau,\epsilon\tau^3\}$.

7.a Montrer que $C(p)=C_1$ si et seulement si on a simultanément que 2 est une puissance 4-ème modulo p et que -1 est un carré modulo p. Ou encore si et seulement si on a $p\equiv 1 \pmod 4$ et $2^{(p-1)/4}\equiv 1 \pmod p$. Indiquer le degré résiduel en p de l'extension $K|\mathbf{Q}$.

7.b Montrer que $C(p)=C_2$ si et seulement si on a simultanément que 2 est un carré mais pas une puissance 4-ème modulo p et que -1 est un carré modulo p. Ou encore si et seulement si on a $p\equiv 1 \pmod 4$ et $2^{(p-1)/4}\equiv -1 \pmod p$. Indiquer le degré résiduel en p de l'extension $K|\mathbf{Q}$.

7.c Montrer que $C(p)=C_3$ si et seulement si on a simultanément que 2 n'est pas un carré modulo p et que -1 est un carré modulo p. Ou encore si et seulement si on a $p\equiv 1 \pmod 4$ et $2^{(p-1)/2}\equiv -1 \pmod p$. Indiquer le degré résiduel en p de l'extension $K|\mathbf{Q}$.

7.d Montrer que $C(p)=C_5$ ou C_6 si et seulement si -1 n'est pas un carré modulo p. Ou encore si et seulement si on a $p\equiv -1 \pmod 4$. Indiquer le degré résiduel en p de l'extension $K|\mathbf{Q}$.

8. Calculer les densités analytiques des ensembles de nombres premiers $\{p/C(p)=C_i\}$, pour $i=1$, 2, 3, 5 ou 6.

9. Déterminer $C(3)$, $C(5)$, $C(7)$. En déduire les coefficients a_n de ζ_K pour $1\leq n\leq 10$.

10. Donner le résidu en $s=1$ de la fonction zêta de $\mathbf{Q}(i)$.

11. Notons K_2 et $\mathbf{Q}_2(i)$ les complétés de K et $\mathbf{Q}(i)$ en leurs uniques idéaux maximaux au dessus de 2. Lesquelles des extensions $K_2|\mathbf{Q}_2$, $K_2|\mathbf{Q}_2(i)$ et $\mathbf{Q}_2(i)|\mathbf{Q}_2$ sont abéliennes ?

12. Quelle est l'image de l'application norme $\mathrm{N}_{\mathbf{Q}_2(i)/\mathbf{Q}_2}:\mathbf{Q}_2(i)^*\to\mathbf{Q}_2^*$?

13. Montrer que $\mathbf{Q}(i)$ est contenu dans le corps de classe de rayon 4∞ de $\mathbf{Q}$.

14. Quelle est l'ordre du conoyau de l'application norme $\mathrm{N}_{K_2/\mathbf{Q}_2(i)}:K_2^*\to\mathbf{Q}_2(i)^*$? Notons n le plus petit entier tel que l'image de $\mathrm{N}_{K_2/\mathbf{Q}_2(i)}$ soit contenue dans $1+(1+i)^n\mathbf{Z}_2[i]$.

15. Montrer que K est contenu dans le corps de classe de rayon $\mathcal{M}=(1+i)^n$ de $\mathbf{Q}(i)$.

16. Montrer qu'on a un homomorphisme de groupes surjectif $C_{\mathbf{Q}(i)}/C^{\mathcal{M}}_{\mathbf{Q}(i)}\to\mathrm{Gal}(K/\mathbf{Q}(i))$, où $C_{\mathbf{Q}(i)}$ (resp. $C^{\mathcal{M}}_{\mathbf{Q}(i)}$) est le groupe des classes d'idèles (resp. sous-groupe de congruence de niveau $\mathcal{M}$) de $\mathbf{Q}(i)$.

17. Montrer que $\zeta_K(s)=\prod_\chi L(\chi,s)$, où χ parcourt certains caractères de $C_{\mathbf{Q}(i)}$.