Université Paris Diderot
Université Pierre et Marie Curie

L. Merel
Théorie algébrique des nombres
M2 mathématiques – Année 2014-15

Examen du 31 octobre 2014

Durée : 3h. Document autorisé : une feuille manuscrite.

Considérons le polynôme (irréductible sur $\mathbf{Q}$) $P(X) = X^3 - X + 1$. Soit $K = \mathbf{Q}(\alpha)$ un corps de rupture de P sur $\mathbf{Q}$, avec α racine de P. Soit L un corps de décomposition de P contenant K. On notera G le groupe de Galois de $L|\mathbf{Q}$. Notons $\mathcal{O}_K$ l'anneau des entiers de K. Posons $\zeta_K(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ (fonction zêta de Dedekind de K).

1. Donner le degré d de l'extension $K|\mathbf{Q}$. Cette extension est-elle galoisienne ?
2. Quels sont les nombres r_1 et r_2 (de plongements réels et de plongements complexes non-réels respectivement) de K ?
3. Montrer que le discriminant absolu du système $(1, \alpha, \alpha^2)$ est -23.
4. Soit $(x_1, x_2, x_3) \in \mathcal{O}_K^3$. Montrer que si le discriminant absolu du système (x_1, x_2, x_3) est un entier non nul sans facteur carré, (x_1, x_2, x_3) est une base du $\mathbf{Z}$-module $\mathcal{O}_K$.
5. En déduire que $\mathcal{O}_K = \mathbf{Z}[\alpha]$.
6. Quel est le discriminant $\mathcal{D}_K$ de l'extension $K|\mathbf{Q}$? Quels sont les nombres premiers ramifiés dans K ?
7. Montrer l'inégalité : $|\mathcal{D}_K|^{1/2}(\frac{4}{\pi})^{r_2} d!/d^d < 2$.
8. Montrer que le nombre de classes de K est égal à 1. L'anneau $\mathcal{O}_K$ est-il principal ?
9. Quel est le rang du groupe $\mathcal{O}_K^*$ des unités de K ? Donner une unité de $\mathcal{O}_K$ qui n'est pas dans $\mathbf{Z}$. En déduire un générateur d'un sous-groupe d'indice fini de $\mathcal{O}_K^*$.
10. Pour p nombre premier < 10 non ramifié dans K, déterminer le degré résiduel en les idéaux premiers au-dessus de p de K.
11. Donner la décomposition de l'idéal $23\mathcal{O}_K$ dans le groupe des idéaux de $\mathcal{O}_K$. On précisera les indices de ramification.
12. Pour n entier ≤ 10, déterminer a_n.
13. Déterminer le résidu de ζ_K en $s = 1$ à multiplication par un entier près.
14. Quel est le groupe de Galois de l'extension $L|\mathbf{Q}$?
15. Montrer que $L = K(\sqrt{-23})$.
16. Montrer que si p est nombre premier différent de 23, l'extension $L|\mathbf{Q}$ est non ramifiée en p
17. Quelle est la densité analytique de l'ensemble des nombres premiers p qui sont inertes dans L ? (Rappel : p est inerte dans L si le degré résiduel en p est égal au degré $[L : \mathbf{Q}]$.)
18. Quel est le lien entre le nombres de racines dans $\mathbf{F}_p$ de P et l'ordre dans G d'une substitution de Frobenius en un idéal de L au-dessus de p ?
19. Quelle est la densité analytique de l'ensemble des nombres premiers p tels que la réduction modulo p de P admette une (resp. deux, resp. trois, resp. aucune) racines dans un corps à p éléments ?
20. Montrer que l'extension $L|\mathbf{Q}(\sqrt{-23})$ est partout non ramifiée.