Université Paris Diderot
ENS Cachan
M1 mathématiques

Arithmétique – Année 2011-12

Examen

Durée : 3h

Soit i une racine carrée de -1 dans $\mathbf{C}$. Soit ζ une racine primitive 2012-ème de l'unité dans $\mathbf{C}$. Soit α une racine carrée de 503 dans $\mathbf{C}$. Rappelons que l'anneau des entiers de $\mathbf{Q}(i)$ est $\mathbf{Z}[i]$, et que ce dernier anneau est principal.

1. Décomposer le nombre 2012 en produit de facteurs premiers.

2. Montrer que les extensions $\mathbf{Q}(\alpha)|\mathbf{Q}$ et $\mathbf{Q}(i)|\mathbf{Q}$ sont galoisiennes. Quels sont les groupes de Galois ?

3. Montrer que l'extension $\mathbf{Q}(\alpha, i)|\mathbf{Q}$ est galoisienne de groupe de Galois G isomorphe au produit de deux groupes cycliques d'ordre 2.

4. Quels sont les nombres premiers ramifiés dans les extensions $\mathbf{Q}(\alpha)|\mathbf{Q}$ et $\mathbf{Q}(i)|\mathbf{Q}$?

5. Soient a, $b \in \mathbf{Q}(i)$. Soit $x = a + b\alpha$ entier sur $\mathbf{Z}[i]$. Montrer que a et b sont dans $\mathbf{Z}[i]$. En déduire que l'anneau des entiers de $\mathbf{Q}(\alpha, i)$ est $\mathbf{Z}[\alpha, i]$.

6. Calculer le discriminant de l'extension $\mathbf{Q}(\alpha, i)|\mathbf{Q}(i)$ (on pourra calculer le discriminant du système $(1, \alpha)$). En déduire les nombres premiers qui sont ramifiés dans l'extension $\mathbf{Q}(\alpha, i)|\mathbf{Q}$.

7. Montrer que l'extension $\mathbf{Q}(\alpha, i)|\mathbf{Q}(i)$ est ramifiée en l'idéal premier principal $(1 + i)$ de $\mathbf{Z}[i]$. Quel est l'indice de ramification en 2 de l'extension $\mathbf{Q}(\alpha, i)|\mathbf{Q}$.

8. Quel est le sous-groupe de décomposition de G en 2 de l'extension $\mathbf{Q}(\alpha, i)|\mathbf{Q}$? Quel est le sous-groupe d'inertie ?

9. Quel est le sous-groupe de décomposition de G en 503 de l'extension $\mathbf{Q}(\alpha, i)|\mathbf{Q}$? Quel est le sous-groupe d'inertie ?

10. Déterminer les ensembles E_1, E_2, E_3 et E_4 formés par les nombres premiers p tel que le groupe de décomposition en p de l'extension $\mathbf{Q}(\alpha, i)|\mathbf{Q}$ soit d'ordre 1, 2, 3 et 4 respectivement ? Quelle est l'ordre de la substitution de Frobenius correpondante dans G dans chacun de ces cas ?

11. Quelles sont les densités des ensembles E_1, E_2, E_3 et E_4 ?

12. Montrer qu'un élément de $(\mathbf{Z}/2012\mathbf{Z})^*$ est un carré si et seulement si c'est un carré modulo 4 et un carré modulo 503.

13. Quelle est la densité de l'ensemble des nombres premiers qui sont des carrrés modulo 2012 ?

14. Admettons que le corps $\mathbf{Q}(\alpha, i)$ est contenu dans $\mathbf{Q}(\zeta)$. Montrer que le groupe G s'identifie au quotient de $(\mathbf{Z}/2012\mathbf{Z})^*$ par le sous-groupe des carrés. Retrouver le résultat de la question 13 en applicant le théorème de Chebotarev à l'extension $\mathbf{Q}(\alpha, i)|\mathbf{Q}$.