Université Paris Diderot
ENS Cachan
M1 mathématiques

Arithmétique – Année 2011-12

Feuille d'exercices 5

Étude d'un corps de nombres

Soit j une racine primitive cubique de l'unité dans $\mathbf{C}$. Notons α la racine cubique de 2 dans $\mathbf{R}$. Rappelons que $\mathbf{Z}[j]$ est l'anneau des entiers de $\mathbf{Q}(j)$. On rappelle que c'est un anneau principal. Notons K le corps de décomposition de $X^3 - 2$ dans $\mathbf{C}$. Notons $\mathcal{O}_K$ l'anneau des entiers de K.

1. Montrer que $K = \mathbf{Q}(\alpha, j)$. Quel est le degré de l'extension $K|\mathbf{Q}$?

2. Montrer que le groupe de Galois G de l'extension $K|\mathbf{Q}$ est le troisième groupe symétrique ? Combien a-t-il d'éléments d'ordre 1, d'ordre 2, d'ordre 3 ? Quelles sont ses classes de conjugaison ?

3. Montrer que le discriminant D sur $\mathbf{Z}$ et sur $\mathbf{Z}[j]$ du système $(1, \alpha, \alpha^2)$ est égal à 108. En déduire que le discriminant de $\mathcal{O}_K$ sur $\mathbf{Z}[j]$ est égal à 3 ou 12 ou 27 ou 108. Montrer que 2 est premier dans $\mathbf{Z}[j]$ et qu'il est ramifié dans l'extension $K|\mathbf{Q}(j)$. En déduire que D est égal à 12 ou 108. Montrer que $(1, \alpha, \alpha^2)$ est une base de $\mathcal{O}_K$ sur $\mathbf{Z}[j]$, puis que $\mathcal{O}_K = \mathbf{Z}[\alpha, j]$.

4. Montrer que l'extension $K|\mathbf{Q}$ est non ramifiée en dehors de 2 et 3.

5. Monter que l'idéal $(2 - j)$ de $\mathcal{O}_K$ engendré par $2 - j$ est premier.

6. En déduire que la décomposition de 7 dans $\mathcal{O}_K$ est $7 = (2 - j)(2 - j^2)$.

7. Peut-on parler "du" groupe de décomposition, "du" groupe d'inertie de "la" substitution de Frobenius en 7 ? Comment peut-on les décrire ?

8. Peut-on traiter le nombre premier 31 de la même façon ?

9. Montrer que l'indice de ramification en 2 est égal à 3 et que le degré d'inertie est égal à 2.

10. Montrer que l'indice de ramification en 3 est égal à 6. Quel est le degré d'inertie en 3 ? Quel est le sous-groupe d'inertie en 3?

11. Existe-t-il un nombre premier $p > 3$ tel que le groupe de décomposition en p soit égal à G ? En déduire que le degré résiduel en un nombre premier p de l'extension $K|\mathbf{Q}$ est égal à 1, 2 ou 3.

12. Montrer que si p est un nombre premier impair congru à 2 modulo 3 le degré résiduel en p de l'extension $\mathbf{Q}(j)|\mathbf{Q}$ est 2. En déduire que le degré résiduel de l'extension $K|\mathbf{Q}$ est égal à 2.

13. Si p est nombre premier congru à 1 modulo 3, montrer que 2 est un cube modulo 3 si et seulement si $2^{(p-1)/3}$ est congru à 1 modulo p.

14. Montrer que si p est un nombre premier congru à 1 modulo 3 le degré résiduel en p de l'extension $\mathbf{Q}(j)|\mathbf{Q}$ est 1. Montrer que le degré résiduel de l'extension $\mathbf{Q}(\sqrt[3]{2})|\mathbf{Q}$ est égal à 1 si et seulement si $2^{(p-1)/3}$ est congru à 1 modulo p. En déduire que que le degré résiduel en p de l'extension $\mathbf{Q}(j)|\mathbf{Q}$ est 1 si et seulement si $2^{(p-1)/3}$ est congru à 1 modulo p.

15. Composer un tableau résumant ce que sont les groupes d'inerties, groupes de décomposition, substitution de Frobenius en un nombre premier p suivant les valeurs de p.

16. Montrer que l'ensemble des nombres premiers p congru à 1 modulo 3 et qui vérifie $2^{(p-1)/3}$ congru à 1 modulo p est infini. Quelle est sa densité ?