



Université BORDEAUX 1
UFR Mathématiques et Informatique

année universitaire 2008–2009



Master de Mathématiques approfondies

première année

MHT 831 : DS du lundi 02 mars 2008, *durée 3 heures*, sans document

Théorie Algébrique des Nombres

Avertissement : Il sera attaché la plus grande importance à la précision et la rigueur des raisonnements.

Exercice

Dans ce qui suit, A désigne un anneau de Dedekind de corps des fractions $K = Fr(A)$. L'objet de l'exercice est d'établir la propriété suivante :

(★) Si I est un idéal fractionnaire de A , il existe $(\alpha, \beta) \in K^2$ tels qu'on ait : $I = \alpha A + \beta A$.

On rappelle que tout idéal fractionnaire non nul I de A s'écrit de façon unique comme un produit fini :

$$I = \prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{\nu_{\mathfrak{p}}(I)}$$

où $\mathfrak{p}$ parcourt l'ensemble des idéaux $\mathcal{P}$ premiers non nuls de A et où les entiers relatifs $\nu_{\mathfrak{p}}(I)$ sont presque tous nuls. En particulier, si $I = \alpha A$ est principal (avec $\alpha \in K^\times$), on pose $\nu_{\mathfrak{p}}(\alpha) = \nu_{\mathfrak{p}}(\alpha A)$.

1. Si I et J sont deux idéaux fractionnaires non nuls de A , vérifier qu'on a pour tout $\mathfrak{p} \in \mathcal{P}$:
$$\nu_{\mathfrak{p}}(I + J) = \min \{ \nu_{\mathfrak{p}}(I), \nu_{\mathfrak{p}}(J) \} .$$
2. Soit maintenant I un idéal *entier* non nul (*i.e.* $0 \neq I \subset A$), et α un élément non nul de A .
 - (a) Montrer qu'il existe un entier naturel r et, pour $1 \leq i \leq r$, des idéaux premiers $\mathfrak{p}_i$ ainsi que des entiers $n_i \geq m_i \geq 0$ tels qu'on ait :

$$I = \prod_{i=1}^r \mathfrak{p}_i^{m_i} \quad \text{et} \quad \alpha A = \prod_{i=1}^r \mathfrak{p}_i^{n_i} .$$

- (b) Pour chaque $1 \leq i \leq r$, on fait choix d'un élément $b_i \in \mathfrak{p}_i^{m_i} \setminus \mathfrak{p}_i^{m_i+1}$. Prouver qu'il existe alors un $\beta \in I$ qui vérifie les r congruences :
$$\beta \equiv b_i \pmod{\mathfrak{p}_i^{m_i+1}}, \text{ pour } 1 \leq i \leq r .$$
 - (c) Conclure de ce qui précède à l'égalité $\nu_{\mathfrak{p}}(\alpha A + \beta A) = \nu_{\mathfrak{p}}(I)$ pour tout $\mathfrak{p} \in \mathcal{P}$.
3. Prouver la propriété (★) pour tout idéal entier puis tout idéal fractionnaire de l'anneau A .

Problème

Le but du problème est d'étudier l'anneau des entiers $A = \mathcal{O}_L$ du corps $L = \mathbb{Q}(\sqrt{-1}, \sqrt{3})$.

1. On s'intéresse d'abord aux propriétés galoisiennes de l'extension $L/\mathbb{Q}$.
 - (a) Observer que $K_3 = \mathbb{Q}[\sqrt{3}]$ ne contient pas $i = \sqrt{-1}$; conclure que $[L : \mathbb{Q}]$ vaut 4.
 - (b) Montrer que L est une extension galoisienne de $\mathbb{Q}$. Quel est l'ordre de $G = \text{Gal}(L/\mathbb{Q})$?
 - (c) On note $K_1 = \mathbb{Q}[\sqrt{-1}]$ puis σ l'unique élément non trivial de $G_1 = \text{Gal}(L/K_1)$ et $\tau \in G$ la conjugaison complexe. Quel est le sous-corps de L fixé par τ ?
 - (d) Préciser l'action de τ , σ et $\sigma\tau$ sur $\sqrt{-1}$ et $\sqrt{3}$; conclure que $\sigma\tau$ est d'ordre 2 et en déduire la structure de G .
 - (e) Conclure que L contient un troisième sous-corps non trivial K_2 que l'on précisera.
2. On va maintenant préciser le discriminant $d_L = \text{Disc}(\mathcal{O}_L)$ de L .
 - (a) On note B le $\mathbb{Z}$ -module libre engendré par $(1, i, \sqrt{3}, i\sqrt{3})$. Vérifier que B est un sous-anneau de A et aussi un sous-module d'indice fini.
 - (b) Montrer que pour tout élément $x = \alpha + \beta i + \gamma\sqrt{3} + \delta i\sqrt{3}$ de L , avec $(\alpha, \beta, \gamma, \delta) \in \mathbb{Q}^4$, on a $\text{Tr}_{L/\mathbb{Q}}(x) = 4\alpha$.
 - (c) Calculer le discriminant d_B de B . Quels sont les facteurs premiers possibles de d_L ?
 - (d) Vérifier que 2 et 3 sont bien ramifiés dans l'extension $L/\mathbb{Q}$ (par exemple en considérant une sous-extension quadratique convenable).
 - (e) Conclure que l'indice $(A : B)$ est une puissance de 2.
3. On regarde enfin L comme un corps cyclotomique : on note $j = \frac{1}{2}(-1 + i\sqrt{3})$ et $\zeta = ij$.
 - (a) Vérifier que ζ est une racine 12^e primitive de l'unité et préciser son polynôme minimal Φ_{12} . Exprimer en particulier i et j en fonction de ζ .
 - (b) Conclure que l'on a $L = \mathbb{Q}[\zeta]$ et $G \simeq (\mathbb{Z}/12\mathbb{Z})^\times$.
 - (c) En déduire que tout élément γ de G est de la forme $\sigma_k : P(\zeta) \mapsto P(\zeta^k)$ pour un k étranger à 12. Préciser la valeur de k pour successivement $\gamma = \sigma$, τ et $\sigma\tau$.
 - (d) Déterminer suivant la congruence de p modulo 12 le sous-groupe de décomposition d'un premier $p \nmid 12$ dans l'extension $L/\mathbb{Q}$. Préciser dans chaque cas le sous-corps de décomposition et le degré d'inertie f_p .
 - (e) Existe-t-il des nombres premiers qui soient totalement inertes dans l'extension $L/\mathbb{Q}$? Que pouvez-vous en conclure sur l'irréductibilité du polynôme Φ_{12} modulo p ?