Université Bordeaux 1
UFR de Mathématiques et Informatique

Master de Mathématiques approfondies

première année

Examen du mardi 22 avril 2008, *durée 4 heures*, sans documents

Théorie Algébrique des Nombres

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

On rappelle que la constante de Minkowski d'un corps de nombres L de degré n sur $\mathbb{Q}$ admettant c paires de plongements complexes deux à deux conjugués et de discriminant d_L vaut

$$(4/\pi)^c \, n!/n^n \sqrt{|d_L|}.$$

Exercice

Le but de cet exercice est de déterminer le groupe des classes d'idéaux $\mathcal{C}l(K)$ du corps quadratique $K = \mathbb{Q}[\sqrt{-15}]$.

1. Rappeler, sans démonstration, la description de l'anneau des entiers $\mathcal{O}_K$ de K.
2. Montrer que toute classe d'idéaux de K contient un idéal entier de norme inférieure ou égale à 2.
3. Déterminer la décomposition en produit d'idéaux premiers de l'idéal $2\mathcal{O}_K$.
4. Soit $\mathfrak{a} \subset \mathcal{O}_K$ un idéal. Montrer que $\mathfrak{a}$ est principal si et seulement si il existe $x \in \mathfrak{a}$ tel que $\mathrm{N}_{K/\mathbb{Q}}(x) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a})$.
5. Déterminer l'ordre et la structure du groupe des classes de K, et donner un représentant de chaque classe.

Problème

On se propose d'étudier le corps de rupture réel L du polynôme $P(X) = X^5 - X + 1$ de $\mathbb{Z}[X]$. On rappelle que le discriminant Δ_P d'un polynôme de la forme $P(X) = X^n + aX + b$ est donné par la formule

$$\Delta_P = (-1)^{\frac{n(n-1)}{2}}(n^n b^{n-1} + (1-n)^{n-1} a^n).$$

1. On commence par établir que le polynôme $P(X)$ est irréductible dans l'anneau $\mathbb{Z}[X]$.
   (a) On note $P_5(X)$ l'image de P dans $\mathbb{F}_5[X]$ et α l'une des racines de P_5 dans la clôture algébrique $\overline{\mathbb{F}}_5$ de $\mathbb{F}_5$. Justifier l'existence de α et vérifier que pour tout $k \in \mathbb{N}$ on a :
   $$\alpha^{5^k} = \alpha - \bar{k} \quad \text{dans } \overline{\mathbb{F}}_5.$$
   (b) Quel est le plus petit k pour lequel on a : $\alpha^{5^k} = \alpha$? En déduire le degré de α sur $\mathbb{F}_5$.
   (c) En déduire que P_5 est irréductible dans $\mathbb{F}_5[X]$, puis que P est irréductible dans $\mathbb{Z}[X]$.

2. Conclure de ce qui précède que le polynôme P est irréductible dans l'anneau $\mathbb{Q}[X]$. Vérifier directement qu'il possède une unique racine réelle $\theta = \theta_1$ et deux paires de racines complexes conjuguées $\theta_3 = \bar{\theta}_2$ et $\theta_5 = \bar{\theta}_4$.
3. On s'intéresse désormais au corps quintique réel $L = \mathbb{Q}[\theta]$ et on note A son anneau d'entiers.
   (a) Calculer le discriminant Δ_P du polynôme P.
   (b) En déduire que l'on a l'égalité $A = \mathbb{Z}[\theta]$.
   (c) Vérifier enfin que les seuls premiers qui se ramifient dans $L/\mathbb{Q}$ sont 19 et 151.
4. On étudie ensuite la décomposition de l'idéal $2A$ dans l'anneau de Dedekind A
   (a) Soit P_2 la réduction de P modulo 2 (*i.e.* l'image de P dans $\mathbb{F}_2[X]$). Prouver que P_2 est irréductible (par exemple en montrant qu'il n'a pas de racine dans le corps $\mathbb{F}_4$).
   (b) En déduire la décomposition de 2. L'anneau A contient-il des idéaux de norme 2 ou 4 ?
5. On fait de même pour l'idéal $3A$ dans l'anneau de Dedekind A
   (a) Soit P_3 la réduction de P modulo 3 (*i.e.* l'image de P dans $\mathbb{F}_3[X]$). Prouver de même que P_3 est irréductible.
   (b) En déduire la décomposition de 3. L'anneau A contient-il des idéaux de norme 3 ?
6. On va maintenant montrer que l'anneau A est principal.
   (a) Évaluer la constante de Minkowski de L et en déduire que toute classe d'idéaux de l'anneau A contient un idéal entier $\mathfrak{a}$ de norme absolue $N(\mathfrak{a}) < 4$.
   (b) Conclure de qui précède que l'anneau A est principal.
7. Soit enfin P_{19} la réduction de P modulo 19 (*i.e.* l'image de P dans $\mathbb{F}_{19}[X]$).
   (a) Vérifier que le polynôme dérivé de $P_{19}(X)$ est $P'_{19}(X) = \bar{5}(X^4 - \bar{4})$; en déduire que le PGCD $D_{19} = P_{19} \wedge P'_{19}$ de $P_{19}(X)$ et $P'_{19}(X)$ est égal à $X - \bar{6}$.
   (b) Conclure que l'on a la factorisation : $P_{19}(X) = (X - \bar{6})^2 R(X)$, où R est un polynôme séparable de $\mathbb{F}_{19}[X]$ étranger à $X - \bar{6}$ de degré 3 et sans racine dans $\mathbb{F}_{19}$.
   (c) En déduire que la factorisation de l'idéal $19A$ dans l'anneau de Dedekind A s'écrit $19A = \mathfrak{p}^2\mathfrak{q}$, où $\mathfrak{p}$ et $\mathfrak{q}$ sont deux idéaux premiers dont on précisera les degrés d'inertie.