TD 8 : Unités et corps cyclotomiques

Exercice 1. [Autour du théorème des unités de Dirichlet]

(a) Soit $M \in M_n(\mathbb{R})$ une matrice dont tous les coefficients diagonaux sont strictement positifs, tous les autres négatifs, et les lignes de somme nulle. Montrer que chaque sous-partie de $n-1$ de ses colonnes est libre (*astuce : considérer une solution X de $MX = 0$, et son coefficient le plus grand*).

(b) Soit $M \in M_{n-1,n}(\mathbb{R})$ une matrice dont les lignes sont à somme nulle. Montrer que la valeur absolue de tout mineur de taille $n-1$ de M est indépendante du choix du mineur. Qu'en déduire pour le régulateur d'un corps de nombres ?

(c) Décrire tous les anneaux d'entiers de corps de nombres dont le groupe des unités est de rang 1, puis 2.

Exercice 2. [Unités d'un anneau d'entiers quadratique (à la main)]

Soit d un entier sans facteur carré différent de 0 et 1, on note $K = \mathbb{Q}(\sqrt{d})$ et $\mathcal{O}_d$ son anneau des entiers.

(a) Rappeler pourquoi $\mathcal{O}_d^*$ est fini si $d < 0$.

On suppose $d > 0$ congru à 2 ou 3 modulo 4. soit b le plus petit entier positif tel que $db^2 + 1$ ou $db^2 - 1$ est un carré a^2 avec $a > 0$.

(b) Montrer que $a + b\sqrt{d}$ est l'unité fondamentale de $\mathcal{O}_d^*$ (*indice : regarder par récurrence les signes des a_n, b_n tels que $a_n + b_n\sqrt{d} = (a + b\sqrt{d})^n$*).

(c) En déduire les unités fondamentales pour $d = 2, 3, 6, 7, 10, 11$.

(d) Pour $d > 0$ congru à 1 modulo 4, soit b le plus petit entier tel que $db^2 + 4$ ou $db^2 - 4$ est un carré a^2. Montrer que $1/2(a + b\sqrt{d})$ est l'unité fondamentale de $\mathcal{O}_d^*$ par un argument similaire.

(e) En déduire les unités fondamentales pour $d = 5, 13, 17, 21$.

(f) Quel est l'inconvénient majeur de cette méthode ?

Exercice 3. [Recherche d'unité fondamentale par fractions continues]

On rappelle que pour une fraction continue $[a_0; a_1, \cdots a_n] = p_n/q_n$ avec p_n et q_n premiers entre eux, on a

$$p_0 = a_0, \quad q_0 = 1, p_1 = a_0a_1 + 1, q_1 = a_1$$

et la formule de récurrence

$$p_n = a_n p_{n-1} + p_{n-2}, \quad q_n = a_n q_{n-1} + q_{n-2}.$$

(a) Pour $d \equiv\ 2, 3[4]$, rappeler pourquoi l'une des convergentes p_n/q_n du développement en fraction continue de $\sqrt{d}$ vérifie forcément

$$p_n^2 - dq_n^2 = \pm 1.$$

(b) Montrer que pour le premier indice n tel que p_n/q_n vérifie cette formule, $p_n + \sqrt{d}q_n$ est une unité fondamentale de $\mathbb{Z}[\sqrt{d}]$.

(c) Appliquer cet algorithme pour retrouver les unités fondamentales lorsque $d = 2, 3, 6, 7, 10, 11$.

(d) Comment adapter l'algorithme au cas $d \equiv 1[4]$?

Exercice 4. [Quelques résultats sur les corps cyclotomiques]

(a) Pour tout p premier et tout $n \in \mathbb{N}^*$, calculer la ramification, l'inertie et la décomposition de p dans $\mathbb{Z}[\zeta_n]$.

(b) Décrire explicitement les sous-corps quadratiques de $\mathbb{Q}(\zeta_n)$ lorsque n est impair.

(c) Prouver que pour tous $m, n \in \mathbb{N}^*$, $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{(m,n)})$.

(d) (*Gauss-Wantzel*). On admet que les nombres de $\mathbb{C}$ constructibles à la règle et au compas sont ceux qui appartiennent à une tour d'extensions quadratiques, c'est-à-dire à un corps K tel qu'il existe une suite $\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n = K$ où pour tout $i \leq n-1$, $[K_{i+1} : K_i] = 2$. En déduire que les racines de l'unité constructibles à la règle et au compas sont les racines dont l'ordre est de la forme

$$n = 2^k p_1 \cdots p_r$$

où les p_i sont des nombres premiers de Fermat (c'est-à-dire de la forme $2^{2^\ell} + 1$) distincts.

Exercice 5. [TD 5, Théorème de Dirichlet faible]

Le but de cet exercice est de démontrer que pour tout $n \in \mathbb{N}^*$, il existe une infinité de nombres premiers $p \equiv 1 \mod n$.

(a) Montrer qu'il suffit de prouver que pour tout $n \in \mathbb{N}^*$, il existe un nombre premier $p \equiv 1 \mod n$.

(b) Montrer que pour ϕ_n le n-ième polynôme cyclotomique, $|\phi_n(n)| > 1$ pour $n > 2$.

(c) Soit p un diviseur premier de $\phi_n(n)$. Montrer qu'il est premier à n.

(d) Soit t l'ordre de n modulo p, supposons par l'absurde que $t < n$. Montrer que $\phi_n(n)$ divise $(n^n - 1)/(n^t - 1)$ et en déduire une contradiction.

(e) En déduire que p est congru à 1 modulo n, et conclure.