TD 7 : Correspondance de Galois et corps cyclotomiques

Exercice 1. [Anneau des entiers et discriminant de $\mathbb{Q}(\zeta_n)$]

Pour $n \in \mathbb{N}$, on note $\zeta_n = e^{2i\pi/n}$, $K = \mathbb{Q}(\zeta_n)$ et φ l'indicatrice d'Euler.

(a) Si $n = p^m$ avec p premier, écrire le polynôme minimal de $\zeta_{p^m} - 1$ et en déduire que $N_{K/\mathbb{Q}}(\zeta_{p^m} - 1) = \pm p$.

(b) En déduire que $p\mathcal{O}_K = (\zeta_{p^m} - 1)^{\varphi(p^m)}$ et calculer le discriminant de $\zeta_{p^m} - 1$ au signe près.

(c) En déduire que $p^{p^{m-1}(pm-m-1)}\mathcal{O}_K \subset \mathbb{Z}[\zeta_{p^m}]$.

(d) Que peut-on dire sur la ramification de p dans K ? En conclure que $\mathcal{O}_K = (\zeta_{p^m} - 1)\mathcal{O}_K + \mathbb{Z}[\zeta_{p^m}]$.

(e) En conclure que $\mathcal{O}_K = \mathbb{Z}[\zeta_{p^m}]$ et que $\mathrm{disc}(K)$ est une puissance de p.

(f) Montrer que pour m et n quelconques, $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_d)$ avec d le pgcd de m et n.

(g) (*Plus difficile*) En déduire par récurrence sur le nombre de diviseurs premiers que l'anneau des entiers de $\mathbb{Q}(\zeta_n)$ est $\mathbb{Z}[\zeta_n]$ pour tout n et que son discriminant a les mêmes diviseurs premiers que n.

Exercice 2. [Rappel : décomposition des nombres premiers dans les corps cyclotomiques]

Soit $n \in \mathbb{N}^*$ et p un nombre premier quelconque.

Donner l'indice de ramification, l'inertie et le nombre de facteurs premiers de p dans $\mathbb{Q}(\zeta_n)$ en fonction de p et n.

Exercice 3. [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) Conclure que p est congru à 1 modulo n.

Exercice 4. [Signe des sommes de Gauss]

Dans cet exercice, p est un nombre premier impair, $\zeta = e^{2i\pi/p}$ et

$$G_p = \sum_{k=0}^{p-1} \left(\frac{k}{p}\right) \zeta^k.$$

On rappelle que $G_p^2 = (-1)^{(p-1)/2}p$, donc $G_p = \pm\sqrt{p}$ si $p \equiv 1 \mod 4$, et $G_p = \pm i\sqrt{p}$ si $p \equiv 3 \mod 4$. Le but de cet exercice est de déterminer complètement G_p, pas seulement au signe près.

(a) Montrer que $p = \prod_{r=1}^{p-1}(1-\zeta^r)$.

(b) Montrer que les $\pm 4k-2$ où $k = 1, \cdots, (p-1)/2$ forment un système de représentants de $(\mathbb{Z}/p\mathbb{Z})^*$.

(c) En déduire que $(-1)^{(p-1)/2}p = \prod_{k=1}^{(p-1)/2}(\zeta^{2k-1} - \zeta^{-2k+1})^2$.

(d) Prouver que $\prod_{k=1}^{(p-1)/2}(\zeta^{2k-1} - \zeta^{-2k+1})$ vaut $\sqrt{p}$ si $p \equiv 1 \mod 4$ et $i\sqrt{p}$ si $p \equiv 3 \mod 4$.

On a donc $G_p = \varepsilon \prod_{k=1}^{(p-1)/2}(\zeta^{2k-1} - \zeta^{-2k+1})$ avec $\varepsilon = \pm 1$ qu'il suffit de déterminer.

(e) Soit le polynôme $P(X) = \sum_{k=1}^{(p-1)/2}\left(\frac{k}{p}\right)X^k - \varepsilon\prod_{k=1}^{(p-1)/2}(X^{2k-1} - X^{p-2k+1})$.

Montrer que $X^p - 1$ divise P, soit Q tel que $P(X) = (X^p-1)Q(X)$. On écrit formellement $X = e^z$ d'où une égalité de séries entières $P(e^z) = (e^{pz}-1)Q(e^z)$.

(f) Montrer que le coefficient en $z^{(p-1)/2}$ du terme de gauche est

$$\frac{1}{((p-1)/2)!}\sum_{j=1}^{(p-1)/2}\left(\frac{j}{p}\right)j^{(p-1)/2} - \varepsilon\prod_{k=1}^{(p-1)/2}(4k-p-2).$$

(g) Montrer que le coefficient en $z^{(p-1)/2}$ du terme de droite est de la forme pa/b avec a, b entiers et p ne divisant pas b.

(h) En déduire que

$$\sum_{j=1}^{(p-1)/2}\left(\frac{j}{p}\right)j^{(p-1)/2} \equiv \varepsilon((p-1)/2)!\prod_{k=1}^{(p-1)/2}(4k-2) \mod p$$

(i) En utilisant le théorème de Wilson, en déduire que

$$\sum_{j=1}^{(p-1)/2}\left(\frac{j}{p}\right)j^{(p-1)/2} \equiv -\varepsilon \mod p$$

(j) Conclure que $\varepsilon = 1$.