TD 3 : Décomposition en idéaux premiers et résidus quadratiques

Exercice 1. [Cas quadratique] On suppose ici que $d \neq 1$ est un entier sans facteur carré congru à 1 modulo 4, et $K = \mathbb{Q}(\sqrt{d})$.

(a) Rappeler quel est le discriminant de K.

(b) En déduire quels sont les nombres premiers ramifiés dans $\mathcal{O}_K$.

(c) Trouver quels sont les nombres premiers inertes dans $\mathcal{O}_K$.

(d) Pour ceux qui ne sont pas inertes, dire comment on expliciterait leur décomposition.

(e) Quels nombres premiers peuvent s'écrire sous la forme $p = a^2 + ab + b^2$ avec $a, b \in \mathbb{Z}$?

Exercice 2. [Symbole de Jacobi]

Pour $a \in \mathbb{Z}$ et $b = \prod_i p_i^{r_i}$ impair premiers entre eux, on définit le symbole de Jacobi de a modulo b par

$$\left(\frac{a}{b}\right) := \prod_i \left(\frac{a}{p_i}\right)^{r_i}.$$

(a) Montrer que $\left(\frac{a}{b}\right)$ peut être égal à 1 sans que a ne soit un carré modulo b.

(b) Montrer que $\left(\frac{a}{b}\right)$ ne dépend que de a modulo b, et est multiplicatif en a et en b.

(c) Calculer $\left(\frac{-1}{b}\right)$ et $\left(\frac{2}{b}\right)$ en fonction des congruences de b modulo 4 et 8.

(d) Démontrer que pour tous a, b premiers entre eux, impairs et avec $a > 0$, $\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right)$ si a ou b est congru à 1 modulo 4, et $-\left(\frac{b}{a}\right)$ sinon.

(e) En déduire un algorithme de calcul du symbole de Legendre.

(f) Calculer les symboles de Jacobi $\left(\frac{7}{15}\right), \left(\frac{12}{43}\right), \left(\frac{13}{53}\right), \left(\frac{10}{99}\right)$.

Exercice 3. [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 4. [Réciprocité quadratique pour 2]

On pose $G = e^{i\pi/4} + e^{-i\pi/4}$.

(a) Montrer que $G = \sqrt{2}$, et en déduire que $G \cdot 2^{(p-1)/2} = e^{i\pi p/4} + e^{-i\pi p/4} \mod p$.

(b) Suivant les congruences de p modulo p, en déduire la valeur de $2^{(p-1)/2} \mod p$.

(c) Conclure.

Exercice 5. [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 $\varepsilon = 1$.