Feuille 2 : Corps cyclotomiques

Exercice 1. Soit $K = \mathbb{Q}(\alpha)$ un corps de nombres, où α est un entier algébrique de degré n et soit $f(x) \in \mathbb{Z}[x]$ son polynôme minimal.

1. Montrer que $\operatorname{disc}(1, \alpha, \dots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} \operatorname{Norm}_{K/\mathbb{Q}}(f'(\alpha))$.
2. Montrer l'égalité $\operatorname{disc}(1, \alpha, \dots, \alpha^{n-1}) = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 \operatorname{disc}(\mathcal{O}_K)$.

Exercice 2. Soient K_1 et K_2 deux corps de nombres. On pose $L = K_1K_2$ l'extension composée. On suppose K_1 et K_2 disjoints, c'est-à-dire que $[L : \mathbb{Q}] = [K_1 : \mathbb{Q}][K_2 : \mathbb{Q}]$. On note A_1, A_2 et B les anneaux d'entiers respectifs de K_1, K_2 et L.

1. Montre que pour tout $x \in K_1$ on a $\operatorname{Tr}_{K_1/\mathbb{Q}}(x) = \operatorname{Tr}_{L/K_2}(x)$.
2. Soit $(e_1, \dots, e_n)$ une base intégrale de A_1, et $(e'_1, \dots, e'_n)$ la base duale relativement à la trace $\operatorname{Tr}_{K_1/\mathbb{Q}}$. Montrer que tout $\alpha \in L$ s'écrit
$$\alpha = \sum_{i=1}^{n} \operatorname{Tr}_{L/K_2}(\alpha e_i) e'_i.$$
3. Monter que $e'_i \in \frac{1}{\operatorname{disc}(A_1)} A_1$.
4. Montre que $\operatorname{disc}(A_1)B \subseteq A_1A_2$.
5. En déduire que si $\operatorname{disc}(A_1)$ et $\operatorname{disc}(A_2)$ sont premier entre eux, on a $B = A_1A_2$ et l'égalité $\operatorname{disc}(B) = \operatorname{disc}(A_1)^{[K_2:\mathbb{Q}]} \operatorname{disc}(A_1)^{[K_1:\mathbb{Q}]}$

Exercice 3. Soit $\ell = p^e$ une puissance d'un nombre premier p et $\zeta \in \mathbb{C}$ une racine primitive ℓ-ème de l'unité. On pose $K = \mathbb{Q}(\zeta)$.

1. Expliciter le polynôme cyclotomique $\Phi_\ell(x)$.
2. Montre que $p = u(1-\zeta)^{\varphi(\ell)}$ pour une unité $u \in \mathbb{Z}[\zeta]^*$.
3. En déduire que p est totalement ramifié dans K et que Φ_ℓ est irréductible sur $\mathbb{Q}$.
4. Montrer que le discriminant de $\mathbb{Z}[\zeta]$ est une puissance de p.
5. Montrer que $\mathbb{Z}[\zeta]$ est p-maximal (voir exercice 12, feuille 1) et en déduire que $\mathcal{O}_K = \mathbb{Z}[\zeta]$.
6. Soit $q \neq p$ un nombre premier. On note f l'ordre de q modulo ℓ et $\varphi(\ell) = fg$. Montrer que l'on a une factorisation
$$q\mathcal{O}_K = \mathfrak{q}_1 \cdots \mathfrak{q}_g$$
où les $\mathfrak{q}_i$ sont des premiers de degré d'inertie f.

Exercice 4. Montrer que $\operatorname{disc}(\mathbb{Z}[\zeta_{p^e}]) = \pm p^{p^{e-1}(pe-e-1)}$.

Exercice 5. Montrer qu'un anneau de Dedekind est principal si et seulement il est factoriel.

Exercice 6. On va montrer que $\mathbb{Z}[\zeta_{23}]$ n'est pas principal. On note dans la suite $\zeta = \exp(2i\pi/23)$ et $K = \mathbb{Q}(\zeta)$.

1. Remarquer que $2^{23} - 1$ est divisible par 47 mais pas par 47^2, et calculer $\mathrm{Norm}_{K/\mathbb{Q}}(\zeta - 2)$.
2. On note $I = 47\mathcal{O}_K + (\zeta - 2)\mathcal{O}_K$. Montrer que pour tout $\alpha \in I$, on a $47 \mid N_{K/\mathbb{Q}}(\alpha)$.
3. On suppose désormais que $I = (\alpha)$ est principal. Montrer que la norme de α divise 47^{22} et $\mathrm{Norm}_{K/\mathbb{Q}}(\zeta - 2)$. Calculer $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)$.
4. Montrer que K contient un unique corps quadratique F, et qu'il s'agit de $\mathbb{Q}(\sqrt{-23})$. Montrer que F est le seul sous-corps quadratique de K.
5. Montrer que $\mathrm{Norm}_{K/F}(\alpha)$ est un entier algébrique de norme 47 et en déduire que I n'est pas principal.

Exercice 7. On se propose de démontrer le théorème suivant (premier cas du théorème Fermat pour les premiers réguliers) :

Théorème (Kummer). Soit $p \geq 3$ un nombre premier, on note $\mathrm{Cl}(K)$ le groupe des classes d'idéaux du p-ème corps cyclotomique $K = \mathbb{Q}(\zeta_p)$. Si p ne divise pas $|\mathrm{Cl}(K)|$, alors toute solution x, y, z de l'équation $x^p + y^p = z^p$ vérifie $p \mid xyz$.

En raisonnant modulo 9, traiter le cas $p = 3$.

On fixe donc pour la suite $p > 3$ un nombre premier, et sous les hypothèses du théorème, on considère une égalité $x^p + y^p = z^p$ pour $x, y, z \in \mathbb{Z}$. On peut supposer de plus que x, y, z sont premiers entre eux, et que $p \nmid xyz$. En posant $\zeta = \exp(2i\pi/p)$, on a l'égalité

$$z^p = \prod_{i \in \mathbb{Z}/p\mathbb{Z}} (x + \zeta^i y) \tag{1}$$

dans l'anneau des entiers $\mathcal{O}_K = \mathbb{Z}[\zeta]$.

1. Montrer qu'un idéal I de $\mathcal{O}_K$ est principal si et seulement si I^p est principal.
2. Montrer que les idéaux $(x + \zeta^i y)$ sont deux à deux premiers entre eux.
3. Soit $u \in \mathcal{O}_K^*$. Montrer que pour tout k on a $u \neq -\zeta^k \bar{u}$.
4. Monter que l'on peut écrire $x + \zeta^k y = u\alpha^p$ où $u \in \mathcal{O}_K^*$ est une unité et $\alpha \in \mathcal{O}_K$.
5. Montrer qu'un entier algébrique $\alpha \in \overline{\mathbb{Z}}$ diffèrent de 0 et tel que tous ses conjugués sont dans les disque unité de $\mathbb{C}$ est une racine de l'unité.
6. Montrer que tout $u \in \mathcal{O}_K^*$ s'écrit $u = \zeta^k \varepsilon$ où $\varepsilon = \bar{\varepsilon} \in \mathbb{Q}(\zeta + \zeta^{-1})$.
7. Montrer que pour tout $\alpha \in \mathcal{O}_K$ il existe $a \in \mathbb{Z}$ tel que $\alpha^p \equiv a \bmod p\mathcal{O}_K$.
8. Montrer qu'on peut supposer $x \not\equiv y \bmod p$. On fait désormais cette hypothèse.

9. Montrer qu'il existe k tel que $(x + y\zeta) \equiv (x + \zeta^{-1})\zeta^k \bmod p\mathcal{O}_K$.
10. Montrer que $\{1, \zeta, \zeta^{2j}, \zeta^{2j-1}\}$ ne peuvent pas être distincts et conclure.