Université de Paris **30 septembre 2021**
M2 – Théorie des nombres

Feuille 2 : corps cyclotomiques

1 Discriminant

Exercice 1 : Formules utiles

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

1. Montrer que $\mathrm{disc}(1, \alpha, \alpha^2, \dots \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} \mathrm{Norm}_{K/\mathbb{Q}}(f'(\alpha))$.

2. Montrer l'égalité $\mathrm{disc}(1, \alpha, \dots \alpha^{n-1}) = [\mathbb{Z}_K : \mathbb{Z}[\alpha]]^2 \,\mathrm{disc}(\mathbb{Z}_K)$.

Exercice 2 : Extensions composées

Soient K_1, 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. Montrer que pour tout $x \in K_1$, $Tr_{K_1/\mathbb{Q}}(x) = Tr_{L/K_2}(x)$.

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 $Tr_{K_1/\mathbb{Q}}$. Montrer que tout $\alpha \in L$ s'écrit $\alpha = \sum_i Tr_{L/K_2}(\alpha e_i) e'_i$.

3. Montrer que $e'_i \in \frac{1}{\mathrm{disc}(A_1)} A_1$.

4. Montrer que $\mathrm{disc}(A_1)B \subset A_1A_2$.

5. En déduire que si $\mathrm{disc}(A_1)$ et $\mathrm{disc}(A_2)$ sont premiers entre eux, on a $B = A_1A_2$ et l'égalité $\mathrm{disc}(B) = \mathrm{disc}(A_1)^{[K_2:\mathbb{Q}]} \,\mathrm{disc}(A_2)^{[K_1:\mathbb{Q}]}$.

6. Montrer que le résultat reste valable pour des extensions finies séparables K_1/F et K_2/F contenues dans un même corps M, et disjointes.

2 Corps cyclotomiques

Exercice 3 : Entiers, ramification

Soit $\ell = p^e$ une puissance de nombre premier, ζ une racine d'ordre ℓ et $K = \mathbb{Q}(\zeta)$.

1. Expliciter le polynôme cyclotomique $\Phi_\ell(x)$.

2. Montrer que $p = u(1 - \zeta)^{\varphi(\ell)}$ pour une unité $u \in \mathbb{Z}[\zeta]^\times$.

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 11, td 1), en déduire que $\mathbb{Z}_K = \mathbb{Z}[\zeta]$.

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 $q\mathbb{Z}_K = \mathfrak{q}_1 \dots \mathfrak{q}_g$ où les $\mathfrak{q}_i$ sont des premiers de degré résiduel f.

Exercice 4 : Discriminant

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

Exercice 5 : Principalité

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

Exercice 6 : $\mathbb{Z}(\zeta_{23})$ n'est pas principal

On note $\zeta = \exp(2i\pi/23)$ et $K = \mathbb{Q}(\zeta)$.

1. Montrer que $2^{23} - 1$ est divisible par 47 mais pas par 47^2, et calculer $N_{K/\mathbb{Q}}(\zeta - 2)$.

2. On note $\mathfrak{a} = 47\mathbb{Z}_K + (\zeta - 2)\mathbb{Z}_K$. Montrer que pour tout $\alpha \in \mathfrak{a}$, $47 \mid N_{K/\mathbb{Q}}(\alpha)$.

3. On suppose de plus que $\mathfrak{a} = (\alpha)$ est principal, calculer $N_{K/\mathbb{Q}}(\alpha)$.

4. Montrer que K contient un unique corps quadratique F, et qu'il s'agit de $\mathbb{Q}(\sqrt{-23})$.

5. Montrer que $N_{K/F}(\alpha)$ est un entier algébrique de norme 47, en déduire que $\mathfrak{a}$ n'est pas principal.

Exercice 7 : Théorème de Kummer sur l'équation de Fermat

On se propose de démontrer le théorème suivant (premier cas de Fermat pour les premiers réguliers)

Théorème 1 (Kummer)**.** *Soit $p \geqslant 5$ un nombre premier, on note $\mathrm{Cl}(K)$ le groupe des classes d'idéaux du p-ième corps cyclotomique $K = \mathbb{Q}(\zeta_p)K$. Si p ne divise pas $\#\mathrm{Cl}(K)$, alors toute solution x, y, z de l'équation $x^p + y^p = z^p$ vérifie $p \mid xyz$.*

On fixe donc pour la suite $p \geqslant 3$ 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 $\zeta = e^{\frac{2i\pi}{p}}$, on a l'égalité

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

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

1. Montrer qu'un idéal $\mathfrak{a}$ de $\mathbb{Z}_K$ est principal si et seulement si $\mathfrak{a}^p$ est principal.

2. Montrer que les idéaux $(x + \zeta^i y)$ sont deux à deux premiers entre eux.

3. Soit $u \in \mathbb{Z}_K^\times$, montrer que pour tout k, $u \neq -\zeta^k \overline{u}$.

4. Montrer que l'on peut écrire $x + \zeta^i y = u\alpha^p$, où $u \in \mathbb{Z}_K^\times$ est une unité et $\alpha \in \mathbb{Z}_K$.

5. Montrer qu'un entier algébrique $\alpha \in \overline{\mathbb{Q}}$ dont tous les conjugués sont dans le disque unité de $\mathbb{C}$ est une racine de l'unité.

6. Montrer que tout $u \in \mathbb{Z}_K^\times$ s'écrit $u = \zeta^k \epsilon$, où $\epsilon = \overline{\epsilon} \in \mathbb{Q}(\zeta + \zeta^{-1})$.

7. Montrer que pour tout $\alpha \in \mathbb{Z}_K$, il existe $a \in \mathbb{Z}$ tel que $\alpha^p = a \bmod p\mathbb{Z}_K$.

8. Montrer qu'il existe j tel que $(x + y\zeta) \equiv (x + y\zeta^{-1})\zeta^j \bmod p\mathbb{Z}_K$, puis que $x \equiv y \bmod p$.

9. Conclure.