**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 $\alpha$ est un entier algébrique de degré $n$, et $f(x) \in \mathbb{Z}[x]$ son polynôme minimal.

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

On a la formule $\mathrm{disc}(x_1, \dots x_n) = \det(\sigma_i(x_j))^2$. En notant $\alpha_i$ les conjugués de $\alpha$, on a donc $\mathrm{disc}(x_1, \dots x_n) = \det(\alpha_i^j)^2$. Le déterminant de Vandermonde vaut $\det(\alpha_i^j) = \prod_{i<j}(\alpha_i - \alpha_j)$. Ici on a donc $\mathrm{disc}(Z[\alpha]) = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j}(\alpha_i - \alpha_j)$. On obtient l'égalité avec la norme par un simple calcul.

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

On considère une base adaptée $(x_1, \dots x_n)$ de $\mathbb{Z}_K$ pour laquelle $(d_1 x_1, \dots d_n x_n)$ soit une base de $\mathbb{Z}[\alpha]$, alors $\mathrm{disc}(\mathbb{Z}[\alpha]) = \mathrm{disc}(d_1 x_1, \dots d_n x_n) = (\prod_i d_i)^2 \mathrm{disc}(\mathbb{Z}_K)$, et $\mathbb{Z}_K/\mathbb{Z}[\alpha] = \prod \mathbb{Z}/d_i\mathbb{Z}$.

**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 $x \in K_1$, $Tr_{K_1/\mathbb{Q}}(x) = Tr_{L/K_2}(x)$.

Les extensions étant disjointes, on a une bijection $\mathrm{Hom}_{\mathbb{Q}}(K_1, \mathbb{C}) \simeq \mathrm{Hom}_{K_2}(L, \mathbb{C})$ (chaque plongement $\sigma$ de $K_1$ dans $\mathbb{C}$ s'étend à un plongement de $L$ qui fixe $K_2$), d'où l'égalité des traces.

**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 $\alpha = \sum_i Tr_{L/K_2}(\alpha e_i) e'_i$.

la famille $e'_i$ est une base de $K_1$, et donc une base de $L/K_2$. On a donc $\alpha = \sum_i a_i e'_i$ avec $a_i \in K_2$, et $Tr_{L/K_2}(\alpha e_i) = a_i$.

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

On a donc $e_j = \sum_i Tr_{L/K_2}(e_i e_j) e'_i = \sum_i Tr_{K_1/\mathbb{Q}}(e_i e_j) e'_i$, d'où le résultat en inversant.

**4.** Montrer que $\mathrm{disc}(A_1) B \subset A_1 A_2$.

on applique les deux questions précédentes pour $\alpha \in B$, de sorte que $Tr_{L/K}(\alpha e_i) \in A_2$

**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 $\mathrm{disc}(B) = \mathrm{disc}(A_1)^{[K_2:\mathbb{Q}]}\,\mathrm{disc}(A_2)^{[K_1:\mathbb{Q}]}$.

Sur une base téléscopique $(a_ib_j)$, la matrice des traces sur $B$ $(Tr_{L/\mathbb{Q}}(a_ib_ja_kb_l) = Tr_{K_1/\mathbb{Q}}(Tr_{L/K_1}(a_ia_kb_jb_l)) = Tr_{K_1/\mathbb{Q}}(a_ia_k)Tr_{K_2/\mathbb{Q}}(b_jb_l))$ est le produit de Kronecker des matrices de traces sur $A_1$ et $A_2$, d'où l'égalité de déterminant $\mathrm{disc}(B) = \mathrm{disc}(A_1)^{[K_2:\mathbb{Q}]}\,\mathrm{disc}(A_2)^{[K_1:\mathbb{Q}]}$.

**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.

On localise, un anneau local est principal et les arguments sont les mêmes.

## 2 Corps cyclotomiques

**Exercice 3 : Entiers, ramification**

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

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

C'est $\frac{x^{p^e}-1}{x^{p^{e-1}}-1} = 1 + x^{p^{e-1}} + x^{2p^{e-1}} + \dots x^{\varphi(\ell)}$.

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

On évalue $\Phi_\ell(1) = p = \prod_{(p,k)=1}(1-\zeta^k)$. Or $\frac{1-\zeta^k}{1-\zeta} \in \mathbb{Z}[\zeta]$, de même que son inverse en écrivant $1 = kk' \bmod \ell$, c'est donc une unité et on obtient l'écriture cherchée.

**3.** En déduire que $p$ est totalement ramifié dans $K$, et que $\Phi_\ell$ est irréductible sur $\mathbb{Q}$.

On a $[K:\mathbb{Q}] \leqslant \varphi(\ell)$ d'après la forme de $\Phi_\ell$, or en notant $\mathfrak{p} = (1-\zeta)\mathbb{Z}_K$ on a $p\mathbb{Z}_K = \mathfrak{p}^{\varphi(\ell)}$. Au vu de l'égalité $n = \sum_i f_ie_i$ on en déduit : $\mathfrak{p}$ est un premier d'indice de ramification $e = \varphi(\ell)$, c'est l'unique premier au dessus de $p$, $[K:\mathbb{Q}] = \varphi(\ell)$ et donc $\Phi_\ell$ est irréductible.

**4.** Montrer que le discriminant de $\mathbb{Z}[\zeta]$ est une puissance de $p$.

On écrit $x^\ell - 1 = \Phi_\ell(x)(x^{p^{e-1}}-1)$, alors en dérivant et en évaluant en $\zeta$ on a $\ell\zeta^{-1} = \Phi'_\ell(\zeta)(\zeta^{p^{e-1}}-1)$. En prenant la norme, $|\mathrm{disc}(\mathbb{Z}[\zeta])| = |\mathrm{Norm}(\Phi'(\zeta))| \mid \ell^{\varphi(\ell)}$, le discriminant est une puissance de $p$.

**5.** Montrer que $\mathbb{Z}[\zeta]$ est $p$-maximal (voir exercice 11, td 1), en déduire que $\mathbb{Z}_K = \mathbb{Z}[\zeta]$.

Le minimal $\Phi_\ell(x+1)$ est un polynôme d'Eisenstein en $p$, de sorte que $\mathbb{Z}[\zeta-1] = \mathbb{Z}[\zeta]$ est $p$-maximal.
Or $[\mathbb{Z}_K : \mathbb{Z}[\zeta]]$ divise $\mathrm{disc}(\mathbb{Z}[\zeta])$, la question de maximalité ne se pose qu'en $p$, donc $\mathbb{Z}_K = \mathbb{Z}[\zeta]$.

**6.** Soit $q \neq p$ un nombre premier, on note $f$ l'ordre de $q$ modulo $\ell$ 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 $f$.

On peut appliquer le critère de Dedekind.

**Exercice 4 : Discriminant**

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

On finit le calcul de l'exercice précédent en prenant la norme de l'égalité $\ell\zeta^{-1} = \Phi'_\ell(\zeta)(\zeta^{p^{e-1}} - 1)$. Puisque $\zeta^{p^{e-1}} = \xi$ est une racine $p$-ième de l'unité, on a dans le sous-corps $F = \mathbb{Q}(\xi)$ une norme $\mathrm{Norm}_{F/\mathbb{Q}}(\xi - 1) = \pm p$, et donc $\left|\mathrm{Norm}_{K/\mathbb{Q}}(\xi-1)\right| = p^{\varphi(\ell)/\varphi(p)} = p^{p^{e-1}}$. Ainsi, $\left|\mathrm{Norm}(\Phi'_\ell(\zeta))\right| = \frac{\ell^{\varphi(\ell)}}{p^{p^{e-1}}}$.

**Exercice 5 : Principalité**

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

Il suffit de voir que si l'anneau est factoriel, les idéaux premiers sont principaux. Soit $\mathfrak{p}$ un tel idéal, et $x \in \mathfrak{p}$. On a deux décompositions uniques, la décomposition en idéaux $(x) = \prod_i \mathfrak{p}_i^{e_i}$ et la décomposition en irréductibles $x = u\prod_i \alpha_i^{f_i}$. Puisque $x \in \mathfrak{p}$ premier, il existe $i$ tel que $\mathfrak{p}_i = \mathfrak{p}$ et $\alpha_i \in \mathfrak{p}$. Or si $\alpha_i$ est irréductible, l'idéal $(\alpha_i)$ est premier, donc $\mathfrak{p} = (\alpha_i)$ est principal.

**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 $N_{K/\mathbb{Q}}(\zeta - 2)$.

Simple calcul. Le minimal de $\zeta$ étant $\Phi_{23}(x) = \frac{x^{23}-1}{x-1}$, la norme de $\zeta - 2$ est $\Phi_{23}(2) = 2^{23} - 1$.

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

On écrit $\alpha = 47u + (\zeta - 2)t$, on prend le produit des conjugués en faisant sortir 47, on obtient $N(\alpha) \in 47\mathbb{Z} + N(\zeta - 2)\mathbb{Z}$.

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

On sait que la valeur absolue vaut 47, il reste à montrer qu'elle est positive. Or $N(\alpha)$ est le produit des conjugués de $\alpha$, en appariant les conjugués complexes c'est un produit de nombres positifs.

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

Le groupe de Galois est cyclique et possède un unique sous-groupe d'indice 2.
Dans ce corps $F = \mathbb{Q}(\sqrt{d})$, 23 est le seul premier ramifié donc $d = \pm 23$. Or $\mathbb{Q}(\sqrt{23})$ a pour discriminant $4 \times 23$ donc 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.

Par transitivité de la norme, $\omega = N_{K/F}(\alpha)$ est un entier de $\mathbb{Z}_F = \mathbb{Z}[\frac{1+\sqrt{-23}}{2}]$ de norme 47. En écrivant $\omega = x + y\frac{1+\sqrt{-23}}{2}$ cela donnerait une solution entière à l'équation $x^2 + xy + 6y^2 = 47$, on voit vite que c'est impossible.

**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.

Par hypothèse du théorème, l'ordre dans le groupe des classes est premier à $p$.

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

Soit $\mathfrak{p}$ un idéal premier qui divise $(x+\zeta^i y)+(x+\zeta^j y)$, alors $\mathfrak{p} \mid (\zeta^i-\zeta^j)y\mathbb{Z}_K = (1-\zeta)y\mathbb{Z}_K$. De même, $\mathfrak{p} \mid (1-\zeta)x\mathbb{Z}_K$.
On a donc $\mathfrak{p} = (1-\zeta)$, puisque $x$ et $y$ sont premiers entre eux.
Mais alors $x+\zeta^i y \equiv x+y \bmod \mathfrak{p}$, d'où $p \mid x+y$ dans $\mathbb{Z}$. On a alors $z^p = x^p+y^p \equiv x+y \equiv 0 \bmod p$, donc $p \mid z$, absurde.

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

On écrit $u = \sum a_i\zeta^i$, en réduisant modulo $1-\zeta$ on obtient $u \equiv \sum a_i = -\sum a_i \equiv -\overline{u} \bmod 1-\zeta$, or $u \neq 0 \bmod 1-\zeta$ puisque $u$ est une unité, donc $1-\zeta \mid (2)$, impossible ($p$ est le seul premier au dessus de $1-\zeta$).

**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 $\alpha \in \mathbb{Z}_K$.

Si on écrit une décomposition unique en idéaux premiers de (1), on a à droite une puissance $p$-ième qui est principale, donc les générateurs diffèrent d'une unité.

**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.

C'est le lemme de Kronecker : l'hypothèse reste vraie pour toutes les puissances de $\alpha$, de sorte qu'il n'y a qu'un nombre fini de polynômes annulateurs possibles (leurs coefficients sont des entiers bornés), donc deux puissances sont égales.

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

$\frac{u}{\overline{u}}$ est un entier algébrique dont tous les conjugués sont de module $\leqslant 1$, c'est donc une racine de l'unité de $K$. En notant $d$ son ordre, on a $\mathbb{Q}(\zeta_d) \subset \mathbb{Q}(\zeta)$ donc $\varphi(d) \mid \varphi(p)$, soit $d \mid 2p$ et cette racine s'écrit $\pm\zeta^r$. La question précédente détermine le signe et on écrit $r = 2k \bmod p$, de sorte que $\epsilon = \zeta^{-k}u$ vérifie les conditions.

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

On décompose sur la base d'entiers, les racines de l'unité disparaissent à la puissance $p$.

**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 $x \equiv y \bmod p$.

$(x+y\zeta) \equiv \zeta^k\epsilon a \bmod p$, donc $(x+y\zeta^{-1}) \equiv \zeta^{-k}\epsilon a \bmod p$, d'où $j = 2k$. Or en décomposant sur la base d'entiers, cette égalité impose $j = 1$, puis $x \equiv y \bmod p$.

**9.** Conclure.

En refactorisant $x^p + (-z)^p = (-y)^p$ on a de même $x \equiv -z \bmod p$, donc $p \mid 3x$, donc $p \mid x$, absurde.

Remarque sur un raisonnement alternatif proposé en TD : de $2x = z \bmod p$ on tire $2x^p \equiv (2x)^p \bmod p^2$ d'où $2^p \equiv 2 \bmod p^2$, c'est-à-dire que 2 est d'ordre divisant $p-1$ modulo $p^2$ (ie qu'il est dans le sous-groupe des puissances $p$-ièmes). Ce n'est pas le cas pour $p = 3$, d'où une démonstration de ce cas qui n'était pas prévue dans l'énoncé. En général on s'attend à ce que l'égalité $2^p = 2 \bmod p^2$ soit vérifiée avec probabilité $\frac{1}{p}$, l'ordinateur nous sort immédiatement les cas $p = 1093$ et $p = 3511$. Le second est de toutes façons un premier irrégulier pour lequel l'exercice ne s'applique pas.