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 $\operatorname{disc}(1, \alpha, \dots, \alpha^{n-1}) = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 \operatorname{disc}(\mathcal{O}_K)$.

Indications 1.

1. On a la formule $\operatorname{disc}(x_1, \dots, x_n) = \det(\sigma_i(x_j))^2$. En notant α_i les conjugués de α, on a donc
$$\operatorname{disc}(x_1, \dots, x_n) = \det(\alpha_j^i)^2.$$
Le déterminant de Vandermonde vaut $\det(\alpha_j^i) = \prod_{i<j}(\sigma_i(\alpha) - \sigma_j(\alpha))$. Ici, on a donc $\operatorname{disc}(1, \alpha, \dots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j}(\sigma_i(\alpha) - \sigma_j(\alpha))$. On obtient l'égalité avec la norme par un simple calcul.
2. On considère une base adaptée $(x_1, \dots, x_n)$ de $\mathcal{O}_K$ pour laquelle la famille $(d_1 x_1, \dots, d_n x_n)$ soit une base de $\mathbb{Z}[\alpha]$. Alors
$$\operatorname{disc}(\mathbb{Z}[\alpha]) = \operatorname{disc}(d_1 x_1, \dots, d_n x_n) = \prod_i d_i^2 \operatorname{disc}(\mathcal{O}_K),$$
et $\mathcal{O}_K/\mathbb{Z}[\alpha] \cong \prod \mathbb{Z}/d_i\mathbb{Z}$.

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 $\operatorname{disc}(B) = \operatorname{disc}(A_1)^{[K_2:\mathbb{Q}]} \operatorname{disc}(A_1)^{[K_1:\mathbb{Q}]}$

Indications 2.

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

2. 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 $\mathrm{Tr}_{L/K_2}(\alpha e_i) = a_i$.
3. On a donc $e_j = \sum_i \mathrm{Tr}_{L/K_2}(e_i e_j) e'_i = \sum_i \mathrm{Tr}_{K_1/\mathbb{Q}}(e_i e_j) e'_i$, d'où le résultat en inversant.
4. On applique les deux questions précédentes.

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.

Indications 3.

1. C'est

$$\Phi_\ell(x) = \frac{x^{p^e} - 1}{x^{p^{e-1}} - 1} = 1 + x^{p^{e-1}} + x^{2p^{e-1}} + \cdots + x^{\varphi(\ell)}.$$

2. 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 $1 = kk' \mod \ell$, c'est donc une unité et on obtient l'écriture cherchée.
3. On a $[K : \mathbb{Q}] \leq \varphi(\ell)$ d'après la forme de Φ_ℓ, or en notant $\mathfrak{p} = (1-\zeta)\mathcal{O}_K$, on a $p\mathcal{O}_K = \mathfrak{p}^{\varphi(\ell)}$. Au vu de l'égalité $n = \sum_i f_i e_i$, 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 Φ_ℓ est irréductible.
4. On écrit $x^\ell - 1 = \Phi_\ell(x)(x^{p^{e-1}} - 1)$, alors en dérivant et en évaluant en ζ, on a $\ell\zeta^{\ell-1} = \Phi'_\ell(\zeta)(\zeta^{p^{e-1}} - 1)$. En prenant la norme, $|\mathrm{disc}(\mathbb{Z}[\zeta])| = \left|\mathrm{Norm}_{K/\mathbb{Q}}(\Phi'_\ell(\zeta))\right| p^{\varphi(\ell)}$, le discriminant est une puissance de p.
5. 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 $[\mathcal{O}_K : \mathbb{Z}[\theta]]$ divise $\mathrm{disc}(\mathbb{Z}[\zeta])$, la question de maximalité ne se pose qu'en p, donc $\mathcal{O}_K = \mathbb{Z}[\zeta]$.
6. Comme $K/\mathbb{Q}$ est une extension ramifiée seulement en p, on sait que

$$q\mathcal{O}_K = \mathfrak{q}_1 \cdots \mathfrak{q}_r$$

où les $\mathfrak{q}_i$ sont des premiers distincts. Il faut donc calculer f_i, le degré d'inertie de $\mathfrak{q}_i$. Soit $\Phi_\ell(x) \equiv P_1(x)\cdots P_m(x) \bmod q$ la factorisation en irréductibles de Φ_ℓ modulo q. On sait que $\mathbb{F}_q[x]/P_i(x) \cong \mathbb{F}_{q^{f_i}}$ pour tout i. La décomposition de Φ_ℓ modulo q est connue : chaque P_i est de degré égal à f l'ordre de q modulo ℓ et donc $f_i = f$ pour tout i (et il y en a forcement g).

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

Indications 4. On finit le calcul de l'exercice précédent en prenant la norme de l'égalité $\ell\zeta^{\ell-1} = \Phi'_\ell(\zeta)(\zeta^{p^{e-1}} - 1)$. Puisque $\zeta^{p^{e-1}} = \xi$ est une racine primitive p-ème de l'unité, on a, dans le sous-corps $F = \mathbb{Q}(\xi)$, l'égalité $\mathrm{Norm}_{F/\mathbb{Q}}(\xi - 1) = \pm p$ (qui est, par exemple, une conséquence de $p = u(\xi-1)^{p-1}$), et donc

$$\left|\mathrm{Norm}_{K/\mathbb{Q}}(\xi - 1)\right| = p^{\varphi(\ell)/\varphi(p)} = p^{p^e-1}.$$

Ainsi,

$$\left|\mathrm{Norm}_{K/\mathbb{Q}}(\Phi'_\ell(\zeta))\right| = \ell^{\varphi(\ell)} p^{p^e-1}.$$

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

Indications 5. Il suffit de voir que si l'anneau est factoriel, les idéaux premiers sont principaux. Soit p un tel idéal, et $x \in p$. On a deux décompositions uniques, la décomposition en idéaux $(x) = \prod_i p_i^{e_i}$ et la décomposition en irréductibles $x = u\prod_i \alpha_i^{f_i}$. Puisque $x \in p$ premier, il existe i tel que $p_i = p$ et $\alpha_i \in p$. Or si α_i est irréductible, l'idéal (α_i) est premier, donc $p = (\alpha_i)$ est principal.

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 $47 \mid \mathrm{Norm}_{K/\mathbb{Q}}(\alpha)$.
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.

Indications 6.

1. Simple calcul. Le minimal de ζ étant $\Phi_{23}(x) = \frac{x^{23}-1}{x-1}$, la norme de $\zeta - 2$ est $\Phi_{23}(2) = 2^{23} - 1$.
2. On écrit $\alpha = 47u + (\zeta - 2)t$. La norme de α est un produit de conjugués de α : un tel conjugué s'écrit $47u' + (\zeta' - 2)t'$ où les u', ζ' et t' sont des conjugués de u, ζ et t. En développant le produit et en rassemblant tous

les termes où 47 apparaît, on trouve $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = 47A + \mathrm{Norm}_{K/\mathbb{Q}}(\zeta - 2)\,\mathrm{Norm}_{K/\mathbb{Q}}(t)$. Comme $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)$, $\mathrm{Norm}_{K/\mathbb{Q}}(\zeta-2)$ et $\mathrm{Norm}_{K/\mathbb{Q}}(t)$ sont rationnels, il en est de même de A. D'autre part, A est une somme de produits d'entiers algébriques, c'est donc un entier algébrique. En fin de compte, A est un entier rationnel, et $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) \in 47\mathbb{Z} + \mathrm{Norm}_{K/\mathbb{Q}}(\zeta - 2)\mathbb{Z}$.

3. Comme I contient 47 et $\zeta - 2$, sa norme divise celle de chacun d'eux, donc $\mathrm{Norm}_{K/\mathbb{Q}}(I)$ divise 47^{22} et aussi $2^{23} - 1$. En particulier elle divise $47 = \mathrm{pgcd}(47^{22}, 2^{23} - 1)$. D'autre part, la question précédente implique que $I \neq \mathcal{O}_K$ et donc $\mathrm{Norm}_{K/\mathbb{Q}}(I) \neq 1$ et donc $\mathrm{Norm}_{K/\mathbb{Q}}(I) = 47$. Cela implique que $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = \pm 47$, il reste à montrer qu'elle est positive. Or $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)$ est le produit des conjugués de α, en appariant les conjugués complexes, c'est un produit de nombres positifs.
4. Le groupe de Galois est cyclique et possède un unique sous-groupe d'indice 2 qui correspond à un sous-corps quadratique $F = \mathbb{Q}(\sqrt{d})$. Dans F, 23 est le seul premier ramifié, donc $d = \pm 23$. Or $\mathbb{Q}(\sqrt{23})$ a pour discriminant 4×23, donc il s'agit de $\mathbb{Q}(\sqrt{-23})$.
5. Par transitivité de la norme, $\omega = \mathrm{Norm}_{K/F}(\alpha)$ est un entier de $\mathcal{O}_F = \mathbb{Z}[\frac{1+\sqrt{-23}}{2}]$ 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. 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 $\alpha \in \overline{\mathbb{Z}}$ différent 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.

Indications 7.
1. Par hypothèse du théorème, l'ordre dans le groupe des classes est premier à p.
2. Soit p un idéal premier qui divise $(x + \zeta^i y) + (x + \zeta^j y)$, alors $p \mid (\zeta^i - \zeta^j)y\mathcal{O}_K = (1-\zeta)y\mathcal{O}_K$. De même, $p \mid (1-\zeta)x\mathcal{O}_K$. On a donc $p = (1-\zeta)$, puisque x et y sont premiers entre eux. Mais alors $x + \zeta^i y \equiv x + y \bmod p$, 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. On écrit $u = \sum a_i \zeta^i$, en réduisant modulo $1 - \zeta$, on obtient $u \equiv \sum a_i = -\sum a_i \equiv -u \bmod 1 - \zeta$. 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. Si on écrit une décomposition unique en idéaux premiers de (1), on a à droite une puissance p-ème qui est principale, donc les générateurs diffèrent d'une unité.
5. C'est le lemme de Kronecker : l'hypothèse reste vraie pour toutes les puissances de α, 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. $\frac{u}{\bar{u}}$ est un entier algébrique dont tous les conjugués sont de module ≤ 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 $\varepsilon = \zeta^{-k}u$ vérifie les conditions.
7. On décompose sur la $\mathbb{Z}$-base ζ^k, les racines de l'unité disparaissent à la puissance p.
8. Supposons de savoir faire le cas $x \not\equiv y \bmod p$ et supposons $x \equiv y \bmod p$. Si $x \equiv -z \bmod p$ alors $-2z^p \equiv z^p \bmod p$ ce qui est impossible car $p \nmid 3z$, donc $x \not\equiv -z \bmod p$. À partir de $x^p + y^p = z^p$ on déduit $x^p + (-z)^p = (-y)^p$ et on conclut.
9. $(x + y\zeta) \equiv \zeta^k \varepsilon a \bmod p$, donc $(x + y\zeta^{-1}) \equiv \zeta^{-k}\varepsilon a \bmod p$, d'où $j = 2k$ convient.
10. On a
$$x + \zeta y - \zeta^{2k}x - \zeta^{2k-1}y \equiv 0 \bmod p.$$
Si $\{1, \zeta, \zeta^{2j}, \zeta^{2j-1}\}$ sont distincts ils forment une famille libre (parce que $p \geq 5$) sur $\mathbb{Z}$ et donc $p \mid x$ ce qui est absurde. Vu que $\zeta \neq 1$ et $\zeta^{2k-1} \neq \zeta^{2k}$ il reste trois cas à considérer.

— Si $\zeta^{2k} = 1$ on a $x + \zeta y - x - \zeta^{-1} y \equiv 0 \bmod p$ et donc $p \mid y$, absurde.
— Si $\zeta^{2k-1} = 1$ on a $(x-y) - (x-y)\zeta \equiv 0 \bmod p$ donc $p \mid x-y$ absurde.
— Si $\zeta^{2k-1} = \zeta$ on a $z - \zeta^2 x \equiv 0 \bmod p$ e donc $p \mid x$ absurde.