Université Paris Diderot — Arithmétique – Année 2011-12
ENS Cachan
M1 mathématiques

**Feuille d'exercices 2**

**Discriminants et corps cyclotomiques**

## I

Soit $K$ une extension finie de $\mathbf{Q}$. Soit $x$ un élément primitif de $K$, *i.e.* on a $K = \mathbf{Q}(x)$. Soit $P$ un polynôme minimal de $x$ sur $\mathbf{Q}$. Notons $n$ le degré de l'extension $K|\mathbf{Q}$. Notons $x_1$, $x_2$, ..., $x_n$ les racines de $P$ dans $\mathbf{C}$ (ce sont les *conjugués* de $x$ dans $\mathbf{C}$).

1. Montrer que $(1, x, x^2..., x^{n-1})$ est une base de $K$ sur $\mathbf{Q}$.

2. Notons $\sigma_1$, $\sigma_2$, ..., $\sigma_n$ les plongements de $K$ dans $\mathbf{C}$. Sont-ils nécessairement à valeurs dans $K$ ? Sont-ils l'identité sur $\mathbf{Q}$ ? Quelles sont les images de $x$ par ces plongements ?

3. Considérons le discriminant $D(1, x, ..., x^{n-1})$. Montrer que

$$D(1, x, ..., x^{n-1}) = \det(\sigma_i(x^j))^2_{1\leq i,j\leq n} = \det(x_i^j)^2_{1\leq i,j\leq n}.$$

4. Calculer ce dernier discriminant comme un déterminant de Vandermonde. En déduire que

$$D(1, x, ..., x^{n-1}) = \prod_{i=1}^{n} P'(x_i).$$

5. Montrer que $D(1, x, ..., x^{n-1}) = N_{K/\mathbf{Q}}(P'(x))$, où $N_{K/\mathbf{Q}}$ désigne la norme.

6. Supposons que $P(X) = X^n + aX + b$ avec $a$, $b \in \mathbf{Q}$. Montrer que

$$D(1, x, ..., x^{n-1}) = (n^n b^{n-1} + (1-n)^{n-1}a^n)(-1)^{n(n-1)/2}.$$

Donner la formule pour $n = 2$ et $n = 3$.

## II

Soit $n$ un entier $\geq 1$. Le $n$-ème polynôme cyclotomique est le polynôme $\Phi_n$ défini par récurrence sur $n$ par la formule $\Phi_n(X) = (X^n - 1)/\Pi_{d|n, d\neq n, d>0}\Phi_d(X)$. Ainsi, on a $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_3(X) = X^2 + X + 1$, $\Phi_4(X) = X^2 + 1$, $\Phi_5(X) = X^4 + X^3 + X^2 + X + 1$, $\Phi_6(X) = X^2 - X + 1$. On sait que $\Phi_n$ est un polynôme irréductible sur $\mathbf{Q}$, à coefficients entiers, et que ses racines sont les racines primitives $n$-èmes de l'unité.

Un *$n$-ème corps cyclotomique* est un corps de décomposition de $\Phi_n$, ou, ce qui revient au même, un corps de décomposition de $X^n - 1$. Il est commode de plonger un tel corps dans $\mathbf{C}$. Le $n$-ème corps cyclotomique est alors unique : il est égal à $\mathbf{Q}(\zeta)$ où $\zeta$ est une racine primitive $n$-ème de l'unité dans $\mathbf{C}$. Par exemple on peut poser $\zeta = e^{2i\pi/n}$. Posons $B = \mathbf{Z}[\zeta]$ le sous-anneau de $L = \mathbf{Q}(\zeta)$ engendré par $\zeta$.

0. L'extension $\mathbf{Q}(\zeta)|\mathbf{Q}$ est-elle galoisienne ? Est-elle abélienne ? Quel est le groupe de Galois ?

1. Soit $p$ un nombre premier et $k$ un entier $\geq 1$. Donner une formule pour $\Phi_p$, puis pour $\Phi_{p^k}$.

2. Supposons que $n = p$. Montrer que $B = \mathbf{Z}[\zeta]$ a pour base $(1, \zeta, \zeta^2, ..., \zeta^{p-2})$ sur $A = \mathbf{Z}$. Posons $K = \mathbf{Q}$.

3. Supposons que $n = p$. Déterminer $Tr_{L/K}(\zeta)$ et $Tr_{L/K}(1)$. Montrer que $(1-\zeta)(1-\zeta^2)...(1-\zeta^{p-1}) = (-1)^p p$. En déduire $N_{L/K}(1-\zeta)$.

4. Supposons que $n = p$. Montrer que $(1-\zeta)B \cap A = pA$. En déduire que $Tr_{L/K}(y(1-\zeta))$ est dans $pA$ pour tout $y \in B$.

5. Supposons que $n = p$. Soit $x \in L$ et entier sur $A$. Posons $x = a_0 + a_1\zeta + ... + a_{p-2}\zeta^{p-2}$ avec $a_0,,a_{p-2}$ dans $K$. Montrer que la trace de $Tr_{L/K}(x(1-\zeta))$ est $a_0 p$. En déduire que $a_0 \in A$. Calculer $Tr_{L/K}((x-a_0)\zeta^{-1})$. En déduire que $a_1 \in A$, puis que $a_i \in A$ $(i \in \{0, 1..., p-1\})$. Montrer que l'anneau des entiers de $\mathbf{Q}(\zeta)$ est $\mathbf{Z}[\zeta]$.

6. Reprendre les question 2, 3, 4, et 5 en supposant que $n = p^k$. Montrer que l'anneau des entiers de $\mathbf{Q}(\zeta)$ est $\mathbf{Z}[\zeta]$.

7. Reprendre les question 2, 3, 4, et 5 en supposant $n$ quelconque et en posant $n = n_0 p^k$, où $n_0$ est premier à $p$, en remplaçant $A$ par $\mathbf{Z}[\zeta_0]$, où $\zeta_0$ est une racine primitive $n_0$-ème de l'unité et $K$ par $\mathbf{Q}(\zeta_0)$. Montrer par récurrence sur le nombre de diviseurs premiers de $n$ que l'anneau des entiers de $\mathbf{Q}(\zeta)$ est $\mathbf{Z}[\zeta]$.

8. Posons $X^n - 1 = \Phi_n(X)G(X)$. Notons $d$ le degré de l'extension $\mathbf{Q}(\zeta)|\mathbf{Q}$. En utilisant la relation $N_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\Phi_n'(\zeta)) = D(1, \zeta, ...\zeta^{d-1})$, montrer qu'on a $n\zeta^{n-1} = \Phi_n'(\zeta)G(\zeta)$.

9. Montrer que $N_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta) = \pm 1$. En déduire que $D(1, \zeta, ..., \zeta^{d-1})$ divise $\pm n^d$.

10. Soit $(x_1, ..., x_d) \in \mathbf{Z}[\zeta]^d$ qui est une base de $\mathbf{Q}(\zeta)$ sur $\mathbf{Q}$. Montrer que $D(1, \zeta, ..., \zeta^{d-1})$ divise $D(x_1, ..., x_d)$. Montrer qu'on peut choisir $(x_1, ..., x_d)$ de telle sorte que $D(x_1, ..., x_d)$ soit premier aux nombres premiers ne divisant pas $n$.