VIII.— Polynômes cyclotomiques

Exercice 1 *a) Calculer $\Phi_p(X)$ pour tout nombre premier p.*

b) Soient t un entier impair > 2 et $p_1 < p_2 < ... < p_t$ des nombres premiers distincts. On pose $n := p_1 ... p_t$ et $p := p_t$. On suppose que $p_1 + p_2 > p_t$.

Montrer que $\Phi_n(X) = (1 + X + ... + X^p)(1 - X^{p_1} - ... - X^{p_t}) \bmod X^{p+1}$.

En déduire les coefficients de $\Phi_n(X)$ de degrés p et $p - 2$.

c) Quel est le coefficient de degré 7 de $\Phi_{105}(X)$?

d) Montrer que, pour tout entier impair m, $\Phi_{2m}(X) = \Phi_m(-X)$.

Quel est le coefficient de degré 7 de $\Phi_{210}(X)$?

Exercice 2 (théorème de Kronecker) *Soit $P(X) = X^n + a_1 X^{n-1} + ... + a_n \in \mathbb{Z}[X]$ un polynôme unitaire irréductible dont toutes les racines sont de module 1.*

Soit $A \in M_n(\mathbb{Z})$ la matrice compagnon de $P(X)$.

a) Montrer qu'il existe $U \in \mathrm{GL}_n(\mathbb{C})$ telle que $A = UDU^{-1}$ où D est la matrice diagonale des racines de P.

b) Si B est une matrice, on note $|B|$ la matrice obtenue en remplaçant les coefficients de B par leurs modules.

Montrer que $|UD^t| = |U|$ pour tout t entier. En déduire que l'ensemble des coefficients des matrices A^t, $t \in \mathbb{Z}$, est borné.

c) En déduire qu'il existe $s, t > 0$ tels que $A^{s+t} = A^t$.

d) Montrer que les racines de $P(X)$ sont des racines de l'unité.

e) Démontrer le théorème de Kronecker :

Soit $P(X) \in \mathbb{Z}[X]$ un polynôme unitaire irréductible dont toutes les racines complexes sont de modules ≤ 1. Alors $P(X) = X$ ou $P(X)$ est un polynôme cyclotomique.

Exercice 3 *Calculer $\Phi_8(X)$ et montrer que $\Phi_8(X)$ est réductible modulo p pour tout p premier (indication : vérifier que dans $\mathbb{Z}/p\mathbb{Z}$, $-1, 2$ ou -2 est un carré).*

Exercice 4 *Soient $p, q \neq 0$ deux entiers premiers entre eux. On pose $t := \pi p/q$.*

a) Montrer que e^{it} est de degré ≤ 2 sur $\mathbb{Q}$. En déduire que $\varphi(q) \leq 2$.

b) Montrer que si t est un multiple rationnel de π, alors :

— $\cos t \in \mathbb{Q} \Rightarrow \cos t = 0, \pm 1/2$ *ou* ± 1 *;*

— $\sin t \in \mathbb{Q} \Rightarrow \sin t = 0, \pm 1/2$ *ou* ± 1 *;*

— $\tan t \in \mathbb{Q} \Rightarrow \tan t = 0$ *ou* ± 1.

Exercice 5 *Soit p un nombre premier. Soient $\zeta := e^{2i\pi/p}$ et H_f l'unique sous-groupe d'ordre f de $(\mathbb{Z}/p\mathbb{Z})^*$. Pour tout l premier à p, on définit une $l-$période comme la somme :*

$$\sum_{a \in lH_f} \zeta^a \ .$$

a) Soient e, f des entiers positifs tels que $ef = p-1$. Soient $(f, l_1), ..., (f, l_e)$ les différentes $f-$périodes. Montrer que

$$(X - (f, l_1))...(X - (f, l_e))$$

est le polynôme minimal de toute $f-$période sur $\mathbb{Q}$ et que toute $f-$période est un élément générique de $\mathbb{Q}(\zeta)^{H_f}$ sur $\mathbb{Q}$.

b) Si $(f, l), (f, m)$ sont des $f-$périodes avec p premier à l, m alors vérifier que :

$$(f, l)(f, m) = \sum_{l' \in lH_f} (f, l' + m) \ .$$

c) On suppose que $p = 17$. Montrer que 3 est un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$ pour la multiplication.

d) Exprimer $(8, 1)$ et $(8, 3)$ en fonction de ζ et montrer que :

$$(8, 1) + (8, 3) = -1 \text{ et } (8, 1)(8, 3) = -4 \ .$$

En déduire $(8, 1)$ et $(8, 3)$.

e) De même, montrer que les $4-$périodes sont les racines des polynômes :

$$X^2 - (8, 1)X - 1 \text{ et } X^2 - (8, 3)X - 1$$

et en particulier que :

$$(4, 1) = 1/4 \left(-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} \right) \ ;$$

$$(4, 2) = 1/4 \left(-1 + \sqrt{17} - \sqrt{34 - 2\sqrt{17}} \right) \ ;$$

$$(4, 3) = 1/4 \left(-1 - \sqrt{17} + \sqrt{34 + 2\sqrt{17}} \right) \ .$$

f) Montrer que $(2, 1)$ et $(2, 4)$ sont racines de l'équation :

$$X^2 - (4, 1)X + (4, 3) = 0 \ .$$

En déduire que :

$$\cos(2\pi/17) =$$

$$-\frac{1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34 - 2\sqrt{17}} + \frac{1}{8}\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}.$$