Les polynômes cyclotomiques

On adopte dans ce problème des notations suivantes : $\mathbb{U}$ désigne le cercle unité, et pour tout $n \in \mathbb{N}^*$, $\mathbb{U}_n$ est le groupe des racines n-ièmes de l'unité. De plus, pour tout $n \in \mathbb{N}^*$, un élément $z \in \mathbb{U}_n$ est dit "racine primitive n-ième de l'unité" si et seulement si son ordre dans le groupe multiplicatif $\mathbb{U}_n$ est exactement n. On note $\mathbb{U}'_n$ l'ensemble des racines primitives n-ièmes de l'unité.

De plus, on définit pour tout $n \in \mathbb{N}^*$ le n-ième polynôme cyclotomique :

$$\Phi_n(X) = \prod_{z \in \mathbb{U}'_n} (X - z)$$

Enfin, on introduit la fonction φ, indicatrice d'Euler, définie de la façon suivante : pour tout $n \in \mathbb{N}^*$, $\varphi(n)$ désigne le nombre d'entiers de $[\![1, n]\!]$ qui sont premiers avec n.

1 Relation de récurrence et premières propriétés

1. Démontrer que pour tout $n \in \mathbb{N}^*$, Φ_n est de degré $\varphi(n)$.

2. a) Soit $n \in \mathbb{N}^*$. Démontrer l'égalité :

$$\mathbb{U}_n = \bigcup_{d|n} \mathbb{U}'_d$$

Et vérifier de plus que l'union est disjointe.

b) En déduire pour tout $n \in \mathbb{N}^*$ la relation de récurrence suivante :

$$X^n - 1 = \prod_{d|n} \Phi_d$$

3. a) Soient A, B des polynômes à coefficients entiers, B étant de plus unitaire. On note $A = QB + R$ la division euclidienne de A par B. Montrer que Q et R sont à coefficients entiers.

b) Démontrer que pour tout $n \in \mathbb{N}^*$, Φ_n est un polynôme unitaire à coefficients entiers. On pourra utiliser la relation de récurrence de la question 2. b).

Comme on va le voir, la relation de récurrence de la question 2. b) peut être inversée pour obtenir une expression explicite de Φ_n.
On définit à cet effet la fonction arithmétique de Moebius μ de la façon suivante. Pour tout $n \in \mathbb{N}^*$, on a :

$$\mu(n) = \begin{cases} (-1)^r & \text{si } n = p_1 ... p_r \text{ où } r \in \mathbb{N} \text{ et les } p_i \text{ sont des nombres premiers distincts} \\ 0 & \text{si } n \text{ est divisible par le carré d'un nombre premier.} \end{cases}$$

4. a) Démontrer que pour tout $n \in \mathbb{N}^*$, on a :

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{sinon} \end{cases}$$

b) En utilisant la relation de récurrence pour les polynômes cyclotomiques vue en 2. b), en déduire pour tout $n \in \mathbb{N}^*$ la formule :

$$\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(\frac{n}{d})}$$

5. Calculer Φ_n pour $n = 1, 2, 3, 4, 5, 6$.

2 Irréductibilité dans $\mathbb{Q}[X]$

Dans cette partie, on démontre le résultat arithmétique suivant : pour tout $n \in \mathbb{N}^*$, Φ_n est irréductible sur $\mathbb{Q}[X]$.

6. Pour tout polnyôme $P \in \mathbb{Z}[X]$ non nul, on définit le "contenu" de P, noté $c(P)$, comme le pgcd des coefficients du polynôme P. De plus, P est dit "primitif" si et seulement si $c(P) = 1$.

a) Soient $P, Q \in \mathbb{Z}[X]$ primitifs. Montrer que PQ est primitif.
Indication : Si p est un nombre premier qui divise tous les coefficients de PQ, on pourra réduire le produit PQ dans $\mathbb{F}_p[X]$.

b) Si $P, Q \in \mathbb{Z}[X]$ sont deux polynômes non nuls de $\mathbb{Z}[X]$, montrer l'égalité $c(PQ) = c(P)c(Q)$.

c) On suppose maintenant que P est un polynôme de $\mathbb{Z}[X]$ unitaire, et que $Q, R \in \mathbb{Q}[X]$ sont unitaires et vérifient $P = QR$. Montrer que $Q, R \in \mathbb{Z}[X]$.

On fixe maintenant $n \in \mathbb{N}^*$ et $z \in \mathbb{C}$ racine de Φ_n. On note π_z le polynôme minimal de z sur $\mathbb{Q}$, qui est donc irréductible sur $\mathbb{Q}[X]$, et on va prouver que $P = \Phi_n$.

7. Montrer que $\pi_z \in \mathbb{Z}[X]$, et qu'il existe $Q \in \mathbb{Z}[X]$ unitaire tel que $\Phi_n = Q\pi_z$.

8. Soit p un nombre premier avec n. On suppose par l'absurde que z^p n'est pas racine de π_z.

a) Montrer que π_z divise $Q(X^p)$.

b) Pour tout $R \in \mathbb{Z}[X]$, on note $\overline{R}$ la réduction de R dans $\mathbb{F}_p[X]$. Montrer que $\overline{\pi_z}$ divise $\overline{Q}(X)^p$.

c) On note $\theta \in \mathbb{F}_p[X]$ un facteur irréductible non constant de $\overline{\pi}_z$. Montrer que θ^2 divise $\overline{X^n - 1}$. En déduire une absurdité.

Ainsi, on a prouvé que pour tout $p \in \mathbb{N}^*$ premier ne divisant pas n, z^p est racine de π_z.

9. Montrer que $\pi_z = \Phi_n$ et conclure quant à l'irréductibilité de Φ_n.

3 Le théorème de Wedderburn

On donne dans cette partie une première application des polynômes cyclotomiques, le théorème de Wedderburn. Ce théorème énonce que tout corps fini est commutatif. Bien entendu, si la définition d'un corps inclus la commutativité, comme c'est le cas chez certains auteurs, cette affirmation est tautologique. Ainsi, dans cette partie uniquement, on ne demande pas la commutativité dans la définition d'un corps : un corps n'est ici rien d'autre qu'une algèbre à division, non nécessairement commutative.

Dans toute cette partie, on fixe un corps fini $\mathbb{K}$, dont on note q le cardinal. On note également le centre k du corps $\mathbb{K}$, définit comme l'ensemble des éléments de $\mathbb{K}$ qui commutent avec tout élément de $\mathbb{K}$. On note p le cardinal de k.

10. a) Montrer que k est un corps commutatif.

b) Montrer qu'on peut munir $\mathbb{K}$ d'une structure de k-espace vetoriel. En déduire qu'on peut écrire $q = p^n$ où q et p sont respectivement les cardinaux de $\mathbb{K}$ et k, et où n est un entier naturel.

11. Soit $z \in \mathbb{K}^*$. On note $\Omega(z)$ la classe de conjugaison de z dans le groupe multiplicatif $\mathbb{K}^*$, et $C(z)$

l'ensemble des éléments de $\mathbb{K}$ qui commutent avec z.

a) Montrer que : $|C(z)| \times |\Omega(z)| = q - 1$

b) Vérifier que $C(z)$ peut être muni d'une structure de k espace vectoriel.

c) Montrer l'existence de $d \in [\![1, n]\!]$ tel que $|\Omega(z)| = \frac{p^n-1}{p^d-1}$.

d) En munissant $\mathbb{K}$ d'une structure de $C(z)$-espace vectoriel à gauche, vérifier de plus que d divise n.

12. a) En séparant les éléments de $\mathbb{K}^*$ en classes de conjugaisons, et en isolant les éléments du centre k^*, montrer l'existence de $r \in \mathbb{N}$ et de $d_1, ..., d_r \in [\![1, n-1]\!]$ divisant n tels que :

$$p^n - 1 = p - 1 + \sum_{i=1}^{r} \frac{p^n - 1}{p^{d_i} - 1}$$

b) En déduire que $\Phi_n(p)$ divise $p - 1$.

13. a) En raisonnant sur les facteurs linéaires de Φ_n, montrer que si $n > 1$, on a : $|\Phi_n(p)| > (p-1)^{\varphi(n)} \geq p-1$.

b) En déduire que $n = 1$ et conclure.

4 Un cas particulier du théorème de la progression arithmétique

Dans cette partie, on donne une seconde application, arithmétique, des polynômes cyclotomiques. On y démontre le cas particulier suivant du théorème de la progression arithmétique de Dirichlet : pour tout entier $n > 1$, il existe une infinité de nombre premiers congrus à 1 modulo n.

On fixe donc un entier $n > 1$, et on raisonne par l'absurde en supposant qu'il existe seulement un nombre fini de nombres premiers congrus à 1 modulo n. On les note $p_1, ..., p_r$ et on pose $N = np_1...p_r$.

14. Soit $a \in \mathbb{N}^*$ et p un diviseur premier de $\Phi_N(a)$ qui ne divise aucun des $\Phi_d(a)$ où d parcourt les diviseurs stricts de N.

a) Quel est l'ordre de a modulo p ?

b) En déduire que p est congru à 1 modulo n et est différent de $p_1, ..., p_r$.

15. On note Q le produit des Φ_d où d parcourt l'ensemble des diviseurs stricts de N.

a) Montrer l'existence d'un entier $a > 2$ tel que $\Phi_N(a) \notin \{0, -1, 1\}$ et de $A, B \in \mathbb{Z}[X]$ tels que $A\Phi_N + BQ = a$.

b) On prend p un diviseur premier de $\Phi_N(a)$. Montrer que p ne divise pas a, puis que pour tout diviseur strict d de N, p ne divise pas $\Phi_N(a)$.

16. Conclure.