

## Les polynômes cyclotomiques

On note  $\mathbb{C}[X]$  (resp.  $\mathbb{R}[X]$ ) l'anneau des polynômes à coefficients dans  $\mathbb{C}$  (resp. dans  $\mathbb{R}$ .)

On note  $\mathbb{Q}[X]$  (resp.  $\mathbb{Z}[X]$ ) l'ensemble des polynômes à coefficients rationnels (resp. entiers.)

Il est clair que  $\mathbb{Q}[X]$  est un sous-anneau de  $\mathbb{R}[X]$  et que  $\mathbb{Z}[X]$  est un sous-anneau de  $\mathbb{Q}[X]$ .

### I. Polynômes à coefficients entiers

Pour tout  $A = \sum_{k \geq 0} a_k X^k$  de  $\mathbb{Z}[X]$ , on note  $\delta(A)$  le pgcd des coefficients  $a_k$ .

On dit que  $A$  est un polynôme *primitif* si  $\delta(A) = 1$ .

Si  $A \neq 0$  (donc  $\delta(A) \neq 0$ ) on note  $\hat{A}$  le polynôme primitif de  $\mathbb{Z}[X]$  défini par  $A = \delta(A) \hat{A}$ .

1. Montrer que si  $A$  et  $B$  sont primitifs, il en est de même du produit  $AB$ .
2. Vérifier que  $\delta(mC) = m\delta(C)$  pour tout  $(m, C)$  de  $\mathbb{Z} \times \mathbb{Z}[X]$ .  
Montrer que dans le cas général, on a  $\delta(AB) = \delta(A)\delta(B)$ .
3. Soient  $P, Q$  deux polynômes unitaires dans  $\mathbb{Q}[X]$ .  
On suppose que  $PQ$  est dans  $\mathbb{Z}[X]$ . Montrer que  $P$  et  $Q$  sont dans  $\mathbb{Z}[X]$ .
4. On se donne deux éléments  $A, B$  de  $\mathbb{Z}[X]$ , le polynôme  $B$  étant unitaire.  
Soit  $A = BQ + R$  la division euclidienne de  $A$  par  $B$  dans  $\mathbb{C}[X]$ .  
Montrer que le quotient  $Q$  et le reste  $R$  sont dans  $\mathbb{Z}[X]$ .

### II. Racines $n$ -ièmes primitives de l'unité

Soit  $n$  dans  $\mathbb{N}^*$  et  $z$  dans  $\mathbb{C}$ .

On dit que  $z$  est une *racine  $n$ -ième primitive de l'unité* si on a  $\begin{cases} z^n = 1 \\ \forall m \in \{1, \dots, n-1\}, z^m \neq 1 \end{cases}$

On désigne par  $U_n$  le groupe des racines  $n$ -ièmes de l'unité.

On note  $R_n$  l'ensemble des racines  $n$ -ièmes primitives de l'unité. On a bien sûr  $R_n \subset U_n$ .

On rappelle que  $U_n$  est un groupe cyclique d'ordre  $n$ , engendré par  $w_n = e^{2i\pi/n}$ .

On note que  $R_n$  est l'ensemble des éléments d'ordre  $n$  du groupe  $(\mathbb{C}^*, \times)$ , donc l'ensemble des générateurs du groupe cyclique  $U_n$ , et que ses éléments sont caractérisés par :  $z^m = 1 \Leftrightarrow n \mid m$ .

On note  $\mathcal{D}_n$  l'ensemble des diviseurs positifs de  $n$ .

1. Soit  $z = \omega_n^k$  un élément de  $U_n$ , avec  $1 \leq k \leq n$ .  
Montrer que le sous-groupe de  $U_n$  engendré par  $z$  est cyclique d'ordre  $\frac{n}{n \wedge k}$ .  
En déduire que  $R_n = \{\omega_n^k, 1 \leq k \leq n, k \wedge n = 1\}$ .
2. Préciser  $R_1$  et  $R_2$ . Donner les éléments de  $R_{12}$ . Que dire de  $R_n$  si  $n$  est premier ?
3. Montrer que  $U_n$  est l'union disjointe des  $R_d$  quand  $d$  parcourt  $\mathcal{D}_n$ .
4. Montrer que  $R_n$  est stable par l'application  $z \mapsto \bar{z}$ , et est de cardinal pair si  $n \geq 3$ .
5. Montrer que le produit des éléments de  $R_n$  est égal à 1 pour tout  $n \geq 3$ .
6. Soient  $m$  et  $n$  deux éléments de  $\mathbb{N}^*$ , premiers entre eux.  
Montrer que l'application  $(a, b) \mapsto ab$  est une bijection de  $R_m \times R_n$  sur  $R_{mn}$ .  
En d'autres termes, on montrera que :  $\forall z \in R_{mn}, \exists ! a \in R_m, \exists ! b \in R_n, z = ab$ .
7. Soit  $a$  un élément particulier de  $R_n$ . Soit  $z$  un nombre complexe.  
Montrer que  $z$  est dans  $R_n$  si et seulement si :  $\exists m \geq 1, m \wedge n = 1, z = a^m$ .

### III. Fonctions multiplicatives

Pour tout  $n$  de  $\mathbb{N}^*$  on note  $\varphi(n)$  le nombre d'entiers de  $\{1, \dots, n\}$  qui sont premiers avec  $n$ .

L'application  $\varphi : \mathbb{N}^* \rightarrow \mathbb{N}^*$  est appelée *indicateur d'Euler*.

La question (II.1) a permis d'établir que  $\text{card}(R_n) = \varphi(n)$ , pour tout  $n$  de  $\mathbb{N}^*$ .

1. Utiliser la partie II pour établir :  $\forall n \geq 1, n = \sum_{d|n} \varphi(d)$  (somme étendue aux  $d$  de  $\mathcal{D}_n$ .)
2. Utiliser II.6 pour montrer que :  $\forall m \in \mathbb{N}^*, \forall n \in \mathbb{N}^*, m \wedge n = 1 \Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$ .

On exprime ce résultat en disant que  $\varphi$  est une application *multiplicative*.

3. Dans cette question, on se propose de calculer la somme notée  $\mu(n)$  des éléments de  $R_n$ .

(a) Vérifier que  $\mu(1) = 1$ . En utilisant (II.3), et pour  $n \geq 2$ , montrer que  $\sum_{d|n} \mu(d) = 0$ .

(b) Si  $p$  est premier, montrer que  $\mu(p) = -1$ , et que  $\mu(p^m) = 0$  si  $m \geq 2$ .

(c) Montrer que :  $\forall m \in \mathbb{N}^*, \forall n \in \mathbb{N}^*, m \wedge n = 1 \Rightarrow \mu(mn) = \mu(m)\mu(n)$ .

Tout comme  $\varphi$ , l'application  $n \mapsto \mu(n)$  est donc *multiplicative*.

(d) Etablir finalement que, pour tout  $n$  de  $\mathbb{N}^*$  :

— Si  $n$  est divisible par le carré d'un entier premier, alors  $\mu(n) = 0$ .

— Si  $n$  est le produit de  $m$  facteurs premiers distincts, alors  $\mu(n) = (-1)^m$ .

On dit que l'application  $\mu$  ainsi définie est la *fonction de Moebius*.

### IV. Polynômes cyclotomiques

Pour tout  $n$  de  $\mathbb{N}^*$ , on pose  $\Phi_n = \prod_{z \in R_n} (X - z)$ , où le produit est étendu aux éléments  $z$  de  $R_n$ .

On dit que  $\Phi_n$  est le *polynôme cyclotomique* d'indice  $n$ .

$\Phi_n$  est donc un polynôme unitaire de degré  $\varphi(n)$  (et a priori à coefficients complexes...)

1. (a) Montrer que si  $p$  est un entier premier, alors  $\Phi_p = \sum_{k=0}^{p-1} X^k$ .

(b) Écrire les polynômes  $\Phi_n$ , pour  $1 \leq n \leq 8$ .

2. (a) Pour tout  $n$  de  $\mathbb{N}^*$ , montrer que  $X^n - 1 = \prod_{d|n} \Phi_d$ .

(b) Montrer que  $\Phi_n$  est dans  $\mathbb{Z}[X]$  pour tout entier  $n \geq 1$ .

3. Dans cette question, on se reportera à (III.3) pour les propriétés de la fonction  $\mu$ .

Soit  $n$  un entier strictement positif. Soit  $\Psi_n$  la fraction rationnelle  $\prod_{d|n} (X^d - 1)^{\mu(\frac{n}{d})}$ .

(a) Justifier l'écriture  $\Psi_n = \prod_{d|n} \left( \prod_{k|d} \Phi_k \right)^{\mu(\frac{n}{d})} = \prod_{k|d|n} \Phi_k^{\mu(\frac{n}{d})} = \prod_{k|n} \Phi_k^{m_k}$ , où  $m_k = \sum_{k|d|n} \mu(\frac{n}{d})$ .

(b) Pour tout  $k$  de  $\mathcal{D}_n$ , montrer que l'exposant  $m_k$  peut s'écrire  $\sum_{\delta|(n/k)} \mu(\delta)$ .

(c) En déduire  $\Psi_n = \Phi_n$ . Ainsi  $\Phi_n = \prod_{d|n} (X^d - 1)^{\mu(\frac{n}{d})}$ .

## V. Relations entre polynômes cyclotomiques

On utilisera ici les résultats précédents (notamment IV.3.c) et les propriétés de la fonction  $\mu$ . L'objectif est de dégager des méthodes pratiques de calcul des polynômes  $\Phi_n$ .

1. Dans cette question, on considère le cas où  $n$  est un produit d'entiers premiers distincts.

(a) On suppose qu'il existe deux entiers premiers distincts  $p, q$  tels que  $n = pq$ .

Exprimer  $\Phi_n$  sous forme de fraction rationnelle non simplifiée.

Observer ensuite qu'on a l'égalité :  $\Phi_{pq}(X) = \frac{\Phi_p(X^q)}{\Phi_p(X)}$ .

(b) Même question si  $n$  est le produit  $pqr$  de trois facteurs premiers distincts.

Observer ensuite qu'on a l'égalité :  $\Phi_{pqr}(X) = \frac{\Phi_{pq}(X^r)}{\Phi_{pq}(X)}$ .

(c) En déduire l'expression de  $\Phi_{10}$  et de  $\Phi_{30}$  sous forme de polynômes.

(d) Plus généralement, soit  $n$  un entier strictement positif quelconque.

Montrer que pour tout entier premier  $p$  ne divisant pas  $n$ , on a  $\Phi_{np}(X) = \frac{\Phi_n(X^p)}{\Phi_n(X)}$ .

Ce résultat permet donc de calculer de proche en proche tous les  $\Phi_n$  quand  $n$  est un produit d'entiers premiers distincts.

2. Dans cette question,  $n$  est un entier strictement positif quelconque.

On note  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$  la décomposition de  $n$  en produits de facteurs premiers.

Dans cette écriture, les  $p_j$  sont premiers distincts deux à deux, et les  $\alpha_j$  sont dans  $\mathbb{N}^*$ .

On note alors  $m = p_1 p_2 \dots p_k$  le produit des facteurs premiers distincts de  $n$ .

(a) Montrer que  $\Phi_n(X) = \Phi_m(X^{n/m})$ .

Cette égalité ramène donc le calcul de tout polynôme  $\Phi_n$  à celui de polynômes  $\Phi_m$  où  $m$  est un entier sans carrés, et la question précédente montre comment faire.

(b) En déduire par exemple l'expression de  $\Phi_{3240}$ .

3. Montrer que si  $n \geq 3$  est impair, alors  $\Phi_{2n}(X) = \Phi_n(-X)$ .

Donner par exemple  $\Phi_{14}$  en utilisant cette propriété.

## VI. Coefficients des polynômes cyclotomiques

1. (a) On sait que  $\Phi_n$  est un polynôme unitaire de degré  $\varphi(n)$ .

Quel est son coefficient de degré  $\varphi(n) - 1$ ? (cf partie III)

Quel est son coefficient constant? (cf partie II)

(b) A ce stade du problème, les calculs explicites de polynômes cyclotomiques pourraient laisser croire que les coefficients de tous les  $\Phi_n$  appartiennent à  $\{-1, 0, 1\}$ .

Montrer qu'il n'en est rien en calculant le coefficient du terme de degré 41 de  $\Phi_{105}$ .

2. (a) Soit un polynôme  $P_m(X) = a_m X^m + a_{m-1} X^{m-1} + \dots + a_1 X + a_0$ , avec  $a_0 a_m \neq 0$ .

Montrer que  $X^m P(1/X) = a_0 X^m + a_1 X^{m-1} + \dots + a_{m-1} X + a_m$ .

(b) Montrer que pour  $n \geq 3$ , on a  $\Phi_n(X) = X^m \Phi_n(1/X)$  avec  $m = \varphi(n)$ .

Indication : on considérera les racines de ces deux polynômes.

En déduire une propriété de symétrie des coefficients de  $\Phi_n$  pour  $n \geq 3$ .

## VII. Irréductibilité des polynômes cyclotomiques d'indice premier

On rappelle que si  $\mathbb{K}$  est un corps et  $A$  un polynôme non constant de  $\mathbb{K}[X]$ , on dit que  $A$  est *irréductible* sur  $\mathbb{K}[X]$  si :  $\forall (B, C) \in \mathbb{K}[X]^2, A = BC \Rightarrow B \in \mathbb{K}^* \text{ ou } C \in \mathbb{K}^*$ .

Pour un élément  $A$  de  $\mathbb{Z}[X]$ , on définit de la même manière l'irréductibilité de  $A$  dans  $\mathbb{Z}[X]$ .

Dans cette partie, on va démontrer l'irréductibilité de  $\Phi_p$  sur  $\mathbb{Q}[X]$ , avec  $p$  premier.

1. Soit  $A$  un polynôme à coefficients entiers (donc un élément de  $\mathbb{Z}[X]$ .)

Montrer que  $A$  est irréductible dans  $\mathbb{Q}[X]$  si et seulement s'il l'est dans  $\mathbb{Z}[X]$ .

Cette propriété signifie que pour prouver l'irréductibilité dans  $\mathbb{Q}[X]$  d'un polynôme à coefficients entiers, il suffit de la vérifier dans  $\mathbb{Z}[X]$  (ce qui a l'avantage d'être plus «ciblé» et de tout limiter à des calculs sur des entiers.)

Pour cette démonstration technique, on s'inspirera des méthodes de la partie I.

2. Dans cette question,  $p$  désigne un entier premier.

On va prouver l'irréductibilité de  $\Phi_p$  sur  $\mathbb{Q}[X]$  en utilisant le *critère d'Eisenstein*.

- (a) Soit  $A = \sum_{k=0}^n a_k X^k = a_0 + a_1 X + \dots + a_{n-1} X^{n-1} + a_n X^n$  un élément de  $\mathbb{Z}[X]$ .

On suppose qu'il existe un entier  $p$  premier divisant  $a_0, \dots, a_{n-1}$ , mais pas  $a_n$ .

On suppose enfin que l'entier  $p^2$  ne divise pas  $a_0$ .

Montrer que  $A$  est irréductible dans  $\mathbb{Z}[X]$ , donc dans  $\mathbb{Q}[X]$ .

- (b) Montrer que si  $p$  est premier, il divise  $\binom{p}{k}$  pour tout  $k$  de  $\{1, \dots, p-1\}$ .

- (c) Si  $p$  est premier, montrer que  $\Phi_p(X+1) = \sum_{k=0}^{p-1} \binom{p}{k+1} X^k$ .

- (d) En déduire que si  $p$  est premier, alors  $\Phi_p$  est irréductible dans  $\mathbb{Q}[X]$ .

## VIII. Irréductibilité des polynômes cyclotomiques d'indice quelconque

Compte tenu de sa difficulté, et parce qu'elle utilise des notions en marge du programme MPSI, cette partie est hors barème. Elle ne figure donc dans ce problème que pour lui donner un peu plus de profondeur.

On utilisera ici les notions introduites dans la partie VII, et les résultats de la question (VII.1).

On se propose de prouver l'irréductibilité de  $\Phi_n$  dans  $\mathbb{Q}[X]$ , pour  $n \geq 1$  quelconque.

La démonstration suit les étapes suivantes :

- On se donne un élément  $a$  de  $R_n$ . On considère dans  $\mathbb{Q}[X]$  le polynôme unitaire de degré minimum  $M_a$  qui s'annule au point  $a$  (l'existence d'un tel polynôme et le fait qu'il est dans  $\mathbb{Z}[X]$  et irréductible sont discutés dans la question 1.).
- L'objectif est de prouver que  $M_a$  s'annule sur tous les éléments de  $R_n$  (ce qui implique l'égalité  $M_a = \Phi_n$  donc l'irréductibilité de  $\Phi_n$ .)
- Dans un premier temps, on se donne un entier premier  $p$  ne divisant pas  $n$ , et on montre que  $M_a$  s'annule en  $a^p$  (qui est bien un élément de  $R_n$ .) Une application répétée de ce principe permet alors d'atteindre tout élément  $b$  de  $R_n$  à partir de  $a$ , et d'en déduire que  $M_a$  s'annule sur tous les éléments de  $R_n$ . La conclusion en résulte.

1. Dans cette question,  $z$  désigne un élément quelconque de  $U_n$ .

Soit  $\mathcal{A}_z$  l'ensemble des polynômes  $A$  de  $\mathbb{Q}[X]$  tels que  $A(z) = 0$ .

- (a) Montrer qu'il existe dans  $\mathcal{A}_z$  un unique polynôme unitaire  $M_z$  de degré minimum.

On dira que  $M_z$  est le *polynôme minimal* de  $z$  sur  $\mathbb{Q}$ .

(b) Montrer que  $\mathcal{A}_z = \{QM_z, Q \in \mathbb{Q}[X]\}$ .

(c) Montrer que  $M_z$  est dans  $\mathbb{Z}[X]$ , et qu'il existe  $N_z$  dans  $\mathbb{Z}[X]$  tel que  $X^n - 1 = M_z N_z$  (indication : utiliser la question I.3)

(d) Montrer que le polynôme  $M_z$  est irréductible dans  $\mathbb{Q}[X]$ .

2. Dans cette question  $p$  désigne un entier premier fixé.

Pour tout  $m$  de  $\mathbb{Z}$ , on note  $\overline{m}$  le reste dans la division de  $m$  par  $p$ .

On désigne par  $F_p$  le corps  $\{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$  des classes résiduelles modulo  $p$ .

On note  $F_p[X]$  l'anneau des polynômes à coefficients dans le corps  $F_p$ .

Pour tout  $A = \sum_{k \geq 0} a_k X^k$  de  $\mathbb{Z}[X]$ , on note  $\overline{A} = \sum_{k \geq 0} \overline{a_k} X^k$  dans  $F_p[X]$ .

(a) Vérifier rapidement que  $\overline{A+B} = \overline{A} + \overline{B}$  et  $\overline{AB} = \overline{A} \overline{B}$  pour tous  $A, B$  de  $\mathbb{Z}[X]$ .

(b) Montrer que :  $\forall (A, B) \in \mathbb{Z}[X]^2, \overline{(A+B)^p} = \overline{A^p} + \overline{B^p}$  (utiliser VII.2.b).

(c) Vérifier que pour tout  $m$  de  $\mathbb{Z}$  :  $m^p \equiv m \pmod{p}$ .

(d) En déduire que pour tout  $A$  de  $\mathbb{Z}[X]$ , on a :  $\overline{A(X)^p} = \overline{A}(X^p)$ .

3. Soit  $a$  un élément fixé de  $R_n$ , et soit  $p$  un entier premier qui ne divise pas  $n$ .

On pose  $b = a^p$ . On sait depuis la question (II.7) que  $b$  est également dans  $R_n$ .

On note  $M_a, M_b$  les polynômes minimaux de  $a, b$  dans  $\mathbb{Q}[X]$  (cf VIII.1)

L'objectif de cette question est de prouver l'égalité  $M_a = M_b$ .

Pour cela on raisonne par l'absurde et on suppose  $M_a \neq M_b$ .

(a) Montrer qu'il existe  $Q \in \mathbb{Z}[X]$  unitaire, tel que  $X^n - 1 = M_a(X)M_b(X)Q(X)$ .

(b) Montrer qu'il existe  $R$  unitaire dans  $\mathbb{Z}[X]$  tel que  $M_b(X^p) = M_a(X)R(X)$ .

En déduire l'égalité  $\overline{M_b(X)^p} = \overline{M_a(X)} \overline{R(X)}$  dans  $F_p[X]$ .

(c) Soit  $S(X)$  un diviseur irréductible unitaire de  $M_a(X)$  dans  $F_p[X]$ .

Montrer que  $S^2(X)$  est un diviseur de  $X^n - 1$  dans  $F_p[X]$ .

(d) En utilisant une dérivation, montrer que  $S(X) = X$  et conclure.

4. Soit  $a$  un élément fixé de  $R_n$ , et  $M_a$  son polynôme minimal dans  $\mathbb{Q}[X]$ .

(a) Soit  $b$  un élément quelconque de  $R_n$ . En utilisant les questions II.7 et VIII.3, montrer que le polynôme  $M_a$  s'annule au point  $b$ .

(b) En déduire que  $M_a = \Phi_n$ , et donc que le polynôme  $\Phi_n$  est irréductible dans  $\mathbb{Q}[X]$ .