.

Programme : Algèbre Générale
Structures & Arithmetique

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 $A = \sum_{k\geqslant 0} a_k X^k$ 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 $\widehat{A}$ le polynôme primitif de $\mathbb{Z}[X]$ défini par $A = \delta(A)\,\widehat{A}$.

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 $w_n = \mathrm{e}^{2i\pi/n}$.

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 $1 \leqslant k \leqslant n$.
   Montrer que le sous-groupe de U_n engendré par z est cyclique d'ordre $\frac{n}{n\wedge k}$.
   En déduire que $R_n = \{w_n^k,\ 1 \leqslant k \leqslant n,\ k \wedge n = 1\}$.
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 $z \mapsto \overline{z}$, et est de cardinal pair si $n \geqslant 3$.
5. Montrer que le produit des éléments de R_n est égal à 1 pour tout $n \geqslant 3$.
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 : $\exists\, m \geqslant 1,\ m \wedge n = 1,\ z = a^m$.

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 $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ 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 : $\forall\, n \geqslant 1,\ n = \sum_{d|n} \varphi(d)$ (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 φ 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 $n \geqslant 2$, 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 $m \geqslant 2$.
   (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 φ, 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 μ 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 Φ_n est le *polynôme cyclotomique* d'indice n.

Φ_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 Φ_n, pour $1 \leqslant n \leqslant 8$.
2. (a) Pour tout n de $\mathbb{N}^*$, montrer que $X^n - 1 = \prod_{d|n} \Phi_d$.
   (b) Montrer que Φ_n est dans $\mathbb{Z}[X]$ pour tout entier $n \geqslant 1$.
3. Dans cette question, on se reportera à (III.3) pour les propriétés de la fonction μ.
   Soit n un entier strictement positif. Soit Ψ_n la fraction rationnelle $\prod_{d|n} (X^d - 1)^{\mu(\frac{n}{d})}$.
   (a) Justifier l'écriture $\Psi_n = \prod_{d|n} \Big(\prod_{k|d} \Phi_k \Big)^{\mu(\frac{n}{d})} = \prod_{k|d|n} \Phi_k^{\mu(\frac{n}{d})} = \prod_{k|n} \Phi_k^{m_k}$, 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 μ.
L'objectif est de dégager des méthodes pratiques de calcul des polynômes Φ_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 Φ_n sous forme de fraction rationnelle non simplifiée.
   Observer ensuite qu'on a l'égalité : $\Phi_{pq}(X) = \dfrac{\Phi_p(X^q)}{\Phi_p(X)}$.

   (b) Même question si n est le produit pqr de trois facteurs premiers distincts.
   Observer ensuite qu'on a l'égalité : $\Phi_{pqr}(X) = \dfrac{\Phi_{pq}(X^r)}{\Phi_{pq}(X)}$.

   (c) En déduire l'expression de Φ_{10} et de Φ_{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 $\Phi_{np}(X) = \dfrac{\Phi_n(X^p)}{\Phi_n(X)}$.
   Ce résultat permet donc de calculer de proche en proche tous les Φ_n
   quand n est un produit d'entiers premiers distincts.

2. Dans cette question, n est un entier strictement positif quelconque.
   On note $n = p_1^{\alpha_1}\, p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ la décomposition de n en produits de facteurs premiers.
   Dans cette écriture, les p_j sont premiers distincts deux à deux, et les α_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 Φ_n à celui de polynômes Φ_m où m est un entier sans carrés, et la question précédente montre comment faire.

   (b) En déduire par exemple l'expression de Φ_{3240}.

3. Montrer que si $n \geqslant 3$ est impair, alors $\Phi_{2n(X)} = \Phi_n(-X)$.
   Donner par exemple Φ_{14} en utilisant cette propriété.

VI. Coefficients des polynômes cyclotomiques

1. (a) On sait que Φ_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 Φ_n appartiennent à $\{-1, 0, 1\}$.
   Montrer qu'il n'en est rien en calculant le coefficient du terme de degré 41 de Φ_{105}.

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

   (b) Montrer que pour $n \geqslant 3$, 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 Φ_n pour $n \geqslant 3$.

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 : $\forall (B,C) \in \mathbb{K}[X]^2,\ A = BC \Rightarrow B \in \mathbb{K}^*$ 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 Φ_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 Φ_p sur $\mathbb{Q}[X]$ en utilisant le *critère d'Eiseinstein.*

   (a) Soit $A = \sum_{k=0}^{n} a_k X^k = a_0 + a_1 X + \cdots + a_{n-1}X^{n-1} + a_n X^n$ un élément de $\mathbb{Z}[X]$.
   On suppose qu'il existe un entier p premier divisant $a_0, \ldots, a_{n-1}$, 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 $\{1, \ldots, p-1\}$.

   (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 Φ_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 barême. 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 Φ_n dans $\mathbb{Q}[X]$, pour $n \geqslant 1$ 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 Φ_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 $\{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$ des classes résiduelles modulo p.

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

Pour tout $A = \sum_{k\geqslant 0} a_k X^k$ de $\mathbb{Z}[X]$, on note $\overline{A} = \sum_{k\geqslant 0} \overline{a_k} X^k$ 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 $\mathbb{Z}$: $m^p \equiv m\ [\,p\,]$.

(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 Φ_n est irréductible dans $\mathbb{Q}[X]$.

Corrigé du problème

I. Polynômes à coefficients entiers

1. Posons $A = \sum_{i\geqslant 0} a_i X^i$, $B = \sum_{j\geqslant 0} b_j X^j$, et $AB = \sum_{k\geqslant 0} c_k X^k$.

   On suppose donc que A et B sont primitifs, et on se donne un entier premier p quelconque.

   Pour conclure, il suffit de prouver que p n'est pas un diviseur commun à tous les c_k.

   Puisque A est primitif, il existe un entier naturel minimum i_0 tel que p ne divise par a_{i_0}.

   De même il existe un entier naturel minimum j_0 tel que p ne divise par b_{j_0}.

   Posons $k_0 = i_0 + j_0$ et vérifions que c_{k_0} n'est pas divisible par p.

   On a en effet $c_{k_0} = \sum_{i=0}^{k_0} a_i b_{k_0-i} = \sum_{i=0}^{i_0-1} a_i b_{k_0-i} + a_{i_0} b_{j_0} + \sum_{i=i_0+1}^{k_0} a_i b_{k_0-i}$.

   Au second membre, les coefficients a_i de la première somme sont divisibles par p (car $i < i_0$), et les coefficients b_{k_0-i} de la seconde sont divisibles par p (car $k_0 - i < j_0$.)

   On en déduit que c_{k_0} est congru à $a_{i_0} b_{j_0}$ modulo p.

   Or l'entier premier p ne divise ni a_{i_0} ni b_{j_0} : il ne divise donc pas leur produit.

   On en déduit que c_{k_0} n'est pas divisible par p.

   Les coefficients du polynôme AB ne sont donc simultanément divisible par aucun facteur premier. En d'autres termes, le polynôme AB est primitif.

2. Si $C = \sum_{k\geqslant 0} c_k X^k$, alors $mC = \sum_{k\geqslant 0} (mc_k) X^k$.

   On sait que $\operatorname{pgcd}\{mc_k, k \geqslant 0\} = m \operatorname{pgcd}\{c_k, k \geqslant 0\}$. Donc $\delta(mC) = m\,\delta(C)$.

   Pour tous A, B de $\mathbb{Z}[X]$, écrivons $A = \delta(A)\widehat{A}$ et $B = \delta(B)\widehat{B}$.

   Alors $AB = mC$ avec $m = \delta(A)\delta(B)$ et $C = \widehat{A}\widehat{B}$.

   Mais $\widehat{A}$ et $\widehat{B}$ sont primitifs. Il en est donc de même de C.

   Il en résulte $\delta(AB) = \delta(mC) = m\delta(C) = m = \delta(A)\delta(B)$.

3. Soit m (resp. n) un dénominateur commun dans $\mathbb{N}^*$ des coefficients de P (resp. de Q).

   Notons $\dot{P}$ et $\dot{Q}$ les polynômes de $\mathbb{Z}[X]$ tels que $\dot{P} = mP$ et $\dot{Q} = nQ$.

   Le coefficient dominant de $\dot{P}$ est m et celui de $\dot{Q}$ est n.

   Il en résulte que $\delta(\dot{P})$ divise m et que $\delta(\dot{Q})$ divise n.

   Observons que PQ est unitaire et dans $\mathbb{Z}[X]$, donc $\delta(PQ) = 1$.

   On a l'égalité $\dot{P}\dot{Q} = mnPQ$ dans $\mathbb{Z}[X]$, donc $\delta(\dot{P}\dot{Q}) = \delta(mnPQ) = mn\,\delta(PQ) = mn$.

   Ainsi $\delta(\dot{P})\delta(\dot{Q}) = mn$, avec $\delta(\dot{P}) \mid m$ et $\delta(\dot{Q}) \mid n$.

   Il en résulte les deux égalités $\delta(\dot{P}) = m$ et $\delta(\dot{Q}) = n$.

   L'entier m divise donc tous les coefficients de $\dot{P}$, et l'entier n divise tous ceux de $\dot{Q}$.

   On en déduit que $P = \frac{1}{m}\dot{P}$ et $Q = \frac{1}{n}\dot{Q}$ sont à coefficients entiers.

4. On raisonne par récurrence sur le degré de A. Posons $n = \deg(A)$ et $m = \deg(B)$.
   Notons que la propriété est évidente si $n < m$ car alors $Q = 0$ et $R = A$.
   On suppose donc que $n \geqslant m$ et que la propriété est vraie « aux rangs précédents ».
   Notons a_n le coefficient dominant de A, et posons $\widehat{A} = A - a_n B X^{n-m}$.
   Le polynôme $\widehat{A}$ est dans $\mathbb{Z}[X]$ et il est de degré strictement inférieur à n.
   Sa division euclidienne par B dans $\mathbb{C}[X]$ s'écrit donc $\widehat{A} = \widehat{Q}B + R$, les polynômes $\widehat{Q}$ et R (avec $\deg R < m$) étant dans $\mathbb{Z}[X]$ (c'est l'hypothèse de récurrence.)
   Ainsi $A = a_n B X^{n-m} + \widehat{A} = QB + R$, où $Q = a_n X^{n-m} + \widehat{Q}$ est dans $\mathbb{Z}[X]$.
   On a ainsi démontré la propriété au rang n, ce qui achève la récurrence.

II. Racines primitives n-ièmes de l'unité

1. Soit z un élément de U_n. Il existe un unique k de $\{1, \dots, n\}$ tel que $z = w_n^k$.
   Posons $d = n \wedge k$, et soient n', k' premiers entre eux, tels que $n = dn'$ et $k = dk'$.
   Pour tout m de $\mathbb{N}^*$: $z^m = 1 \Leftrightarrow w_n^{mk} = 1 \Leftrightarrow n \mid mk \Leftrightarrow n' \mid mk' \Leftrightarrow n' \mid m$ (Gauss).
   Autrement dit, z est un élément d'ordre n' du groupe U_n.
   Cela signifie qu'il engendre un sous-groupe cyclique de U_n, d'ordre $n' = \frac{n}{n \wedge k}$.
   Dire que z est dans R_n, c'est dire que $n' = n$, ce qui équivaut à $n \wedge k = 1$.
   Les éléments de R_n sont donc les $z = w_n^k$, avec $1 \leqslant k \leqslant n$ et $n \wedge k = 1$.

2. Bien sûr $R_1 = \{1\}$ et $R_2 = \{-1\}$.
   Posons $u = w_{12} = \mathrm{e}^{i\pi/6}$, c'est-à-dire $u = \frac{\sqrt{3}}{2} + \frac{1}{2}\,i$. On a $R_6 = \{u, u^5, u^7, u^{11}\}$.
   On a $u_5 = \mathrm{e}^{5i\pi/6} = -\frac{\sqrt{3}}{2} + \frac{1}{2}\,i$; u^5 et u^7 sont conjugués, de même que u et u^{11}.
   Si n est premier, alors $R_n = \{w_n, w_n^2, \dots, w_n^{n-1}\} = U_n \setminus \{1\}$.
   Ainsi, quand n est premier, toutes les racines n-ièmes sont primitives sauf $z = 1$.

3. Soit d un diviseur de n, et soit z un élément de R_d.
   L'égalité $z^d = 1$ implique $z^{md} = 1$ pour tout m de $\mathbb{N}^*$ donc $z^n = 1$. Ainsi $R_d \subset U_n$.
   Réciproquement, soit $z = w_n^k$ dans U_n, avec $1 \leqslant k \leqslant n$. Reprenons les calculs faits en (1).
   On sait que l'entier $m \geqslant 1$ minimum tel que $z^m = 1$ est $m = \frac{n}{n \wedge k}$.
   Autrement dit, z est dans R_m, et $m = \frac{n}{n \wedge k}$ est bien un élément de $\mathcal{D}_n$.
   Conclusion : U_n est la réunion des R_d, où l'entier d parcourt $\mathcal{D}_n$.

4. Soit z un élément de R_n. Autrement dit : $z^n = 1$ et $z^m \neq 1$ si $1 \leqslant m \leqslant n-1$.
   Ces conditions sont évidemment remplies par $\overline{z}$. R_n est donc stable par conjugaison.
   Le réel 1 est dans R_1 uniquement, et -1 est uniquement dans R_2.
   Pour tout $n \geqslant 3$, les éléments de R_n sont donc complexes non réels.
   Comme on peut les grouper en paires de nombres conjugués, $\mathrm{card}(R_n)$ est pair.

5. On a $R_1 = \{1\}$ et $R_2 = \{-1\}$. Le « produit » des éléments de R_1 ou R_2 est donc évident.
   Si $n \geqslant 3$, les éléments de R_n sont non réels et se groupent en paires de nombres conjugués.
   Le produit $z\,\overline{z}$ de chaque paire vaut 1 puisque $|z| = 1$.
   On en déduit que pour tout $n \geqslant 3$ le produit des éléments de R_n est égal à 1.

6. Il existe u, v dans $\mathbb{Z}$ tels que $um + vn = 1$.
   Soit z dans R_{mn}. Alors $z = z^{um+vn} = ab$ avec $a = z^{vn}$ et $b = z^{um}$.
   On constate que : $a^q = 1 \Leftrightarrow z^{vnq} = 1 \Leftrightarrow mn \mid vnq \Leftrightarrow m \mid vq \Leftrightarrow m \mid q$ (car $m \wedge v = 1$.)
   De même : $b^q = 1 \Leftrightarrow z^{umq} = 1 \Leftrightarrow mn \mid umq \Leftrightarrow n \mid uq \Leftrightarrow n \mid q$ (car $n \wedge u = 1$.)
   Autrement dit : a est dans R_m et b est dans R_n.
   Réciproquement, supposons $z = ab = cd$, avec $(a, c) \in R_m^2$ et $(b, d) \in R_n^2$.
   Alors $ab = cd \Rightarrow a^{um}b^{um} = c^{um}d^{um} \Rightarrow b^{um} = d^{um} \Rightarrow b^{1-vn} = d^{1-vn} \Rightarrow b = d$.
   (On a utilisé $a^m = c^m = b^n = d^n = 1$.) L'égalité $ab = cd$ donne alors $a = c$.
   Conclusion : $\forall\, z \in R_{mn},\ \exists !\, a \in R_m,\ \exists !\, b \in R_n,\ z = ab$.

7. Soit z dans R_n : z et a sont donc tous deux des générateurs du groupe cyclique U_n.
   On en déduit qu'il existe m et m' dans $\mathbb{N}^*$ tels que $z = a^m$ et $a = z^{m'}$.
   Ainsi $a = a^{mm'}$ puis $a^{mm'-1} = 1$, et il en découle : $\exists\, k \geqslant 1, mm' - 1 = kn$.
   Cette dernière égalité montre que m et n sont premiers entre eux.
   Réciproquement, on se donne $z = a^m$, avec $m \wedge n = 1$.
   On a alors $z^k = 1 \Leftrightarrow a^{mk} = 1 \Leftrightarrow n \mid mk \Leftrightarrow n \mid k$ (On utilise Gauss car $m \wedge n = 1$.)
   Ainsi z est un élément d'ordre n du groupe $(\mathbb{C}^*, \times)$, c'est-à-dire un élément de R_n.

III. Le retour des fonctions multiplicatives

1. On sait que U_n est l'union disjointe des R_d quand d parcourt $\mathcal{D}_n$.
   Il en découle $\operatorname{card}(U_n) = \sum_{d|n} \operatorname{card}(R_n)$ c'est-à-dire $n = \sum_{d|n} \varphi(n)$.

2. Soient m et n deux éléments de $\mathbb{N}^*$, premiers entre eux.
   On sait que l'application $(a, b) \mapsto ab$ est une bijection de $R_m \times R_n$ sur R_{mn}.
   Il en découle $\operatorname{card}(R_{mn}) = \operatorname{card}(R_m)\operatorname{card}(R_n)$, c'est-à-dire $\varphi(mn) = \varphi(m)\varphi(n)$.

3. (a) On a $R_1 = \{1\}$ donc $\mu(1) = 1$.
   Pour tout $n \geqslant 2$, on sait que la somme des racines n-ièmes de l'unité vaut 0.
   On sait d'autre part que U_n est l'union disjointe des R_d, où d parcourt $\mathcal{D}_n$.
   On en déduit que $\sum_{d|n} \mu(d) = \sum_{d|n} \sum_{z \in R_d} z = \sum_{z \in U_n} z = 0$.

   (b) Si p est premier : $\mathcal{D}_p = \{1, p\} \Rightarrow 0 = \mu(1) + \mu(p) = 1 + \mu(p) \Rightarrow \mu(p) = -1$.
   Pour tout $m \geqslant 2$, on a $\mathcal{D}_{p^m} = \{1, p, p^2, \ldots, p^{m-1}, p^m\}$.
   La question précédente donne $0 = \sum_{k=0}^{m} \mu(p^k) = \sum_{k=2}^{m} \mu(p^k)$ car $\mu(1) + \mu(p) = 0$.
   Ainsi $\mu(p^2) + \mu(p^3) + \cdots + \mu(p^m) = 0$ pour tout entier $m \geqslant 2$.
   En commençant à $m = 2$, une récurrence évidente donne : $\forall\, m \geqslant 2, \mu(p^m) = 0$.

(c) Soient m et n deux éléments de $\mathbb{N}^*$, premiers entre eux.

On sait que pour tout $z \in R_{mn}$: $\exists\,!\, a \in R_m,\ \exists\,!\, b \in R_n,\ z = ab$.

On en déduit $\mu(mn) = \sum_{z \in R_{mn}} z = \sum_{a \in R_m,\, b \in R_n} ab = \sum_{a \in R_m} a \sum_{b \in R_n} b = \mu(m)\,\mu(n)$.

(d) Supposons que $n = p_1 p_2 \dots p_m$, où les p_k sont entiers premiers distincts.

La propriété $\mu(ab) = \mu(a)\,\mu(b)$, vraie quand $a \wedge b = 1$, se généralise au produit d'un nombre quelconque d'entiers premiers entre eux deux à deux.

Ainsi $\mu(n) = \mu(p_1 p_2 \dots p_m) = \prod_{k=1}^{m} \mu(p_k) = (-1)^m$ car $\mu(p_k) = -1$ pour tout k.

Remarque : si $m = 0$, on retrouve la propriété déjà connue $\mu(1) = 1$.

Supposons maintenant que n soit divisible par le carré d'un entier premier p.

Alors il existe un entier $m \geqslant 2$, et un entier q premier avec p, tel que $n = p^m q$.

On a alors $\mu(n) = \mu(p^m q) = \mu(p^m)\,\mu(q) = 0$ car $p^m \wedge q = 1$ et $\mu(p^m) = 0$.

IV. Polynômes cyclotomiques

1. (a) On sait que $R_p = U_p \setminus \{1\}$ (cf II.2).

On peut donc écrire $X^p - 1 = \prod_{z \in U_p} (X - z) = (X - 1) \prod_{z \in R_p} (X - z) = (X - 1)\Phi_p$.

La factorisation classique de $X^p - 1$ donne $\Phi_p = X^{p-1} + X^{p-2} + \dots + X + 1$.

(b) On a $R_1 = \{1\}$ donc $\Phi_1 = X - 1$. On a $R_2 = \{-1\}$ donc $\Phi_2 = X + 1$.

On a $R_3 = \{j, j^2\}$ donc $\Phi_3 = (X - j)(X - j^2) = X^2 + X + 1$.

On a $R_4 = \{i, -i\}$ donc $\Phi_4 = (X - i)(X + i) = X^2 + 1$.

Puisque 5 est premier, on a $\Phi_5 = X^4 + X^3 + X^2 + X + 1$.

On a $R_6 = \{-j^2, -j\}$ donc $\Phi_6 = (X + j^2)(X + j) = X^2 - X + 1$.

Puisque 7 est premier, on a $\Phi_7 = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$.

On a $R_8 = \{\mathrm{e}^{i\pi/4}, \mathrm{e}^{3i\pi/4}, -\mathrm{e}^{i\pi/4}, -\mathrm{e}^{3i\pi/4}\}$. On en déduit :

$\Phi_8 = (X - \mathrm{e}^{i\pi/4})(X - \mathrm{e}^{3i\pi/4})(X + \mathrm{e}^{i\pi/4})(X + \mathrm{e}^{3i\pi/4}) = (X^2 - i)(X^2 + i) = X^4 + 1$.

2. (a) On sait que U_n est l'union disjointe des R_d quand d parcourt $\mathcal{D}_n$ (cf II.3)

Il en résulte que $X^n - 1 = \prod_{z \in U_n} (X - z) = \prod_{d|n} \prod_{z \in R_d} (X - z) = \prod_{d|n} \Phi_d$

(b) La propriété est vraie si $n = 1$ car $\Phi_n = X - 1$.

On se donne $n \geqslant 2$, et on suppose que Φ_d est dans $\mathbb{Z}[X]$ pour tout $d < n$.

On a $X^n - 1 = \prod_{d|n} \Phi_d = Q\Phi_n$, avec $Q = \prod_{d|n,\, d<n} \Phi_d$.

Dans le produit égal à Q, les Φ_d sont unitaires et dans $\mathbb{Z}[X]$ (car $d < n$.)

Il en résulte que le polynôme Q lui-même est unitaire et dans $\mathbb{Z}[X]$.

L'égalité $X^n - 1 = Q\Phi_n$ exprime une division euclidienne dans $\mathbb{R}[X]$.

On est dans les conditions d'application du résultat vu en (I.4).

On en déduit que Φ_n est à coefficients dans $\mathbb{Z}$, ce qui achève la récurrence.

3. (a) Pour tout $d \geqslant 1$, on a $X^d - 1 = \prod_{k|d} \Phi_k$. Ainsi $\Psi_n = \prod_{d|n} (X^d - 1)^{\mu(\frac{n}{d})} = \prod_{d|n} \Big(\prod_{k|d} \Phi_k \Big)^{\mu(\frac{n}{d})}$.

On obtient $\Psi_n = \prod_{k|d|n} \Phi_k^{\mu(\frac{n}{d})}$ en groupant tous les facteurs dans un produit double étendu aux différents couples (k, d) tels que $k \mid d \mid n$.

On peut alors réorganiser le produit suivant k, qui parcourt les diviseurs de n.

Pour chaque k de $\mathcal{D}_n$, on obtient un produit étendu aux entiers d tels que $k \mid d \mid n$, c'est-à-dire aux multiples de k qui sont en même temps des diviseurs de n.

Ainsi $\Psi_n = \prod_{k|n} \Big(\prod_{k|d|n} \Phi_k^{\mu(\frac{n}{d})} \Big) = \prod_{k|n} \Phi_k^{m_k}$, en notant $m_k = \sum_{k|d|n} \mu(\frac{n}{d})$.

On notera bien que la mention $k \mid d \mid n$ désigne un produit ou une somme relatives à l'entier d uniquement, l'entier k étant fixé dans ce produit ou cette somme.

(b) Soit k dans $\mathcal{D}_n$. Il existe $m \geqslant 1$ tel que $n = mk$. On a alors les équivalences :

$$k \mid d \mid n \Leftrightarrow \begin{cases} \exists\, \delta \geqslant 1,\ n = \delta d \\ \exists\, r \geqslant 1,\ d = rk \end{cases} \Leftrightarrow \begin{cases} \exists\, \delta \geqslant 1,\ n = \delta d \\ \exists\, r \geqslant 1,\ n = \delta r k \end{cases} \Leftrightarrow \begin{cases} \exists\, \delta \geqslant 1,\ n = \delta d \\ \exists\, r \geqslant 1,\ \delta r = m \end{cases}$$
$$\Leftrightarrow \begin{cases} \exists\, \delta \geqslant 1,\ n = \delta d \\ \delta \mid m \end{cases} \Leftrightarrow \begin{cases} \exists\, \delta \geqslant 1,\ n = \delta d \\ \delta \mid (n/k) \end{cases}$$

Ainsi quand d parcourt la condition $k \mid d \mid n$, l'entier $\frac{n}{d}$ décrit les diviseurs de $\frac{n}{k}$.

Avec les notations de (3a), on a donc $m_k = \sum_{k|d|n} \mu(\frac{n}{d}) = \sum_{\delta|(n/k)} \mu(\delta)$.

(c) On sait que $\mu(1) = 1$ et $\sum_{k|m} \mu(k) = 0$ si $m \geqslant 2$ (cf III.3.a)

On en déduit $m_k = \sum_{\delta|(n/k)} \mu(\delta) = \begin{cases} 1 \text{ si } k = n \\ 0 \text{ si } k < n \end{cases}$ donc $\Psi_n = \prod_{k|n} \Phi_k^{m_k} = \Phi_n$.

V. Relations entre polynômes cyclotomiques

1. (a) On a $\mathcal{D}_n = \{1, p, q, pq\}$. D'autre part $\begin{cases} \mu(1) = \mu(pq) = 1 \\ \mu(p) = \mu(q) = -1 \end{cases}$. On en déduit :

$$\Phi_{pq} = (X^{pq} - 1)^{\mu(1)} (X^p - 1)^{\mu(q)} (X^q - 1)^{\mu(p)} (X - 1)^{\mu(pq)} = \frac{(X^{pq} - 1)(X - 1)}{(X^p - 1)(X^q - 1)}.$$

On a bien $\Phi_{pq}(X) = \dfrac{\Phi_p(X^q)}{\Phi_p(X)}$ car $\Phi_p(X) = \dfrac{X^p - 1}{X - 1}$.

(b) On a $\mathcal{D}_n = \{1, p, q, r, pq, pr, qr, pqr\}$, et $\begin{cases} \mu(1) = \mu(pq) = \mu(pr) = \mu(qr) = 1 \\ \mu(p) = \mu(q) = \mu(r) = \mu(pqr) = -1 \end{cases}$

On en déduit : $\Phi_{pqr} = \dfrac{(X^{pqr} - 1)(X^p - 1)(X^q - 1)(X^r - 1)}{(X^{pq} - 1)(X^{pr} - 1)(X^{qr} - 1)(X - 1)}$.

On a bien $\Phi_{pqr}(X) = \dfrac{\Phi_{pq}(X^r)}{\Phi_{pq}(X)}$ car $\Phi_{pq}(X) = \dfrac{(X^{pq} - 1)(X - 1)}{(X^p - 1)(X^q - 1)}$.

(c) On a $\Phi_{10} = \dfrac{(X^{10} - 1)(X - 1)}{(X^2 - 1)(X^5 - 1)} = \dfrac{X^5 + 1}{X + 1} = X^4 - X^3 + X^2 - X + 1$.

$$\Phi_{30}(X) = \frac{\Phi_{10}(X^3)}{\Phi_{10}(X)} = \frac{X^{12} - X^9 + X^6 - X^3 + 1}{X^4 - X^3 + X^2 - X + 1} = X^8 + X^7 - X^5 - X^4 - X^3 + X + 1.$$

(d) Un diviseur de l'entier np est ou bien un diviseur de n ou bien le produit de p par un diviseur de n. Autrement dit : $\mathcal{D}_{np} = \mathcal{D}_n \cup \{\delta p, \delta \in \mathcal{D}_n\}$ (union disjointe.)

En utilisant cette séparation en deux camps des diviseurs de np, on trouve :

$\Phi_{np} = \prod_{d|(np)} (X^d-1)^{\mu(\frac{np}{d})} = \prod_{d|n}(X^d-1)^{\mu(\frac{np}{d})} \prod_{\delta|n}(X^{\delta p}-1)^{\mu(\frac{n}{\delta})}$.

– Pour tout diviseur d de n, on a $\mu(\frac{n}{d}\, p) = -\mu(\frac{n}{d})$ (d'après la définition de μ.)

Le produit $\prod_{d|n}(X^d-1)^{\mu(\frac{np}{d})}$ est donc l'inverse du polynôme $\Phi_n(X)$.

– Dans le produit $\prod_{\delta|n}((X^p)^\delta-1)^{\mu(\frac{n}{\delta})}$ on reconnait $\Phi_n(X^p)$.

En regroupant ces observations, on constate bien que $\Phi_{np}(X) = \dfrac{\Phi_n(X^p)}{\Phi_n(X)}$.

Cette formule permet donc de calculer de proche en proche les polynômes Φ_n, pour tous les entiers n « sans facteurs carrés ».

2. (a) On sait que $\Phi_n = \prod_{d|n}(X^d-1)^{\mu(\frac{n}{d})}$.

Les diviseurs de n sont les $d = p_1^{\beta_1}\, p_2^{\beta_2} \cdots p_k^{\beta_k}$, avec $0 \leqslant \beta_j \leqslant \alpha_j$ pour tout j.

Pour un tel d, on a $\frac{n}{d} = \prod_{j=1}^{k} p_j^{\alpha_j-\beta_j}$.

On en déduit que si l'un au moins des β_j vérifie $\alpha_j - \beta_j > 1$ alors $\mu\left(\frac{n}{d}\right) = 0$.

Dans le produit donnant Φ_n, on peut donc se limiter aux seuls diviseurs d de n pour lesquels on a $\alpha_j - 1 \leqslant \beta_j \leqslant \alpha_j$ pour tout j.

Mais ces diviseurs d de n sont les $d = \delta\frac{n}{m}$, où δ est un diviseur quelconque de m.

Ainsi $\Phi_n = \prod_{d|n}(X^d-1)^{\mu(\frac{n}{d})}$ se réduit à $\Phi_n = \prod_{\delta|m}(X^{\delta n/m}-1)^{\mu(m/\delta)}$.

Puisque Φ_m est égal à $\prod_{\delta|m}(X^\delta-1)^{\mu(\frac{m}{\delta})}$, on constate que $\Phi_n(X) = \Phi_m(X^{\frac{n}{m}})$.

(b) On a $3240 = 2^3 3^4 5$. Avec les notations précédentes, $m = 2\cdot 3\cdot 5 = 30$, et $\frac{n}{m} = 108$.

D'autre part, on sait que $\Phi_{30}(X) = X^8 + X^7 - X^5 - X^4 - X^3 + X + 1$.

Ainsi $\Phi_{3240}(X) = \Phi_{30}(X^{108}) = X^{864} + X^{756} - X^{540} - X^{432} - X^{324} + X^{108} + 1$.

3. Puisque l'entier premier 2 ne divise pas n, la question V.1.d fournit $\Phi_{2n}(X) = \dfrac{\Phi_n(X^2)}{\Phi_n(X)}$.

La question posée revient donc à prouver que $\Phi_n(X^2) = \Phi_n(X)\Phi_n(-X)$.

Or $\Phi_n(-X) = \prod_{z\in R_n}(-X-z) = \prod_{z\in R_n}(X+z)$ car le degré $\varphi(n)$ de Φ_n est pair (cf II.4)

Ainsi le produit $\Phi_n(X)\Phi_n(-X)$ est égal à $\prod_{z\in R_n}(X^2-z^2)$.

Il suffit donc de vérifier que l'application $z \mapsto z^2$ est une bijection de R_n.

Si z est dans R_n alors $-z$ n'y est pas car $(-z)^n = (-1)^n z^n = -1$ (n est impair.)

Si $z \in R_n$ alors $z^2 \in R_n$ car : $z^{2m} = 1 \Leftrightarrow n \mid 2m \Leftrightarrow n \mid m$ (parce que n est impair.)

Ainsi l'application $z \mapsto z^2$, restreinte à R_n, est injective et à valeurs dans R_n. Il en résulte qu'elle réalise une bijection de R_n sur lui-même, ce qu'il fallait démontrer.

Exemple : $\Phi_{14}(X) = \Phi_7(-X) = X^6 - X^5 + X^4 - X^3 + X^2 - X + 1$.

VI. Coefficients des polynômes cyclotomiques

1. (a) Posons $m = \varphi(n)$ et $\Phi_n = \prod_{z \in R_n} (X - z) = X^{\varphi(n)} + aX^{\varphi(n)-1} + \cdots + b$.

   Le polynôme Φ_n possède $\varphi(n)$ racines distinctes, qui sont les éléments de R_n.

   Les relations coefficients-racines donnent $a = -\sum_{z \in R_n} z = -\mu(n)$ (cf partie III).

   On en déduit que a est nul si n est divisible par le produit d'un carré et que a est égal à $(-1)^{m-1}$ si n est le produit de m entiers premiers distincts.

   Toujours en vertu des relations coefficients-racines, $b = (-1)^{\varphi(n)} \prod_{z \in R_n} z$.

   On sait que $\Phi_1 = X - 1$ et $\Phi_2 = X + 1$, et dans ces cas la valeur de b est évidente.

   On sait que $\varphi(n)$ est pair si $n \geqslant 3$ (voir II.4)

   En utilisant II.5, on en déduit, pour tout $n \geqslant 3$: $b = \prod_{z \in R_n} z = 1$.

   On peut résumer ce résultat en écrivant : $\Phi_1(0) = -1$ et $\Phi_n(0) = 1$ si $n \geqslant 2$.

   (b) On a $105 = 3 \cdot 5 \cdot 7$. Connaissant Φ_3, on va calculer Φ_{15} puis Φ_{105}.

   On trouve $\Phi_{15}(X) = \dfrac{\Phi_3(X^5)}{\Phi_3(X)} = \dfrac{X^{10} + X^5 + 1}{X^2 + X + 1} = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1$.

   Ensuite $\Phi_{105}(X) = \dfrac{\Phi_{15}(X^7)}{\Phi_{15}(X)} = \dfrac{X^{56} - X^{49} + X^{35} - X^{28} + X^{21} - X^7 + 1}{X^8 - X^7 + X^5 - X^4 + X^3 - X + 1}$.

   On trouve alors : $\Phi_{105}(X) = X^{48} + X^{47} + X^{46} - X^{43} - X^{42} - 2X^{41} + \cdots$

2. (a) On pose $P_m(X) = a_m X^m + a_{m-1} X^{m-1} + \cdots + a_k X^k + \cdots + a_1 X + a_0 = \sum_{k=0}^{m} a_k X^k$.

   On trouve $X^m P_m(1/X) = X^m \sum_{k=0}^{m} a_k X^{-k} = \sum_{k=0}^{m} a_k X^{m-k} = \sum_{k=0}^{m} a_{m-k} X^k$.

   Ainsi $X^m P_m(1/X) = a_0 X^m + a_1 X^{m-1} + \cdots + a_{m-k} X^k + \cdots + a_{m-1} X + a_m$.

   (b) On sait Φ_n est unitaire, et que son coefficient constant vaut 1 si $n \geqslant 3$.

   Avec les notations précédentes, et $m = \varphi(n)$, le polynôme $\Psi_n(X) = X^m \Phi_m(1/X)$ est donc lui aussi unitaire et de degré m, et son coefficient constant vaut 1.

   Les racines de Ψ_n sont nécessairement non nulles, puisque $\Psi_n(0) = 1$.

   On en déduit $\Psi_n(z) = 0 \Leftrightarrow z^m \Phi_n(1/z) = 0 \Leftrightarrow \Phi_n(1/z) = 0 \Leftrightarrow 1/z \in R_n \Leftrightarrow \overline{z} \in R_n$.

   Mais on sait que l'application $z \mapsto \overline{z}$ laisse invariant l'ensemble R_n.

   On en déduit que les racines de Ψ_n sont, tout comme Φ_n, les éléments de R_n.

   Du fait que Ψ_n et Φ_n sont unitaires de même degré, il en résulte $\Psi_n = \Phi_n$.

   Mais on sait que la liste des coefficients de Ψ_n est la liste inversée de ceux de Φ_n.

   Si on pose $\Phi_n = \sum_{k=0}^{m} a_k X^k$ (avec $m = \varphi(n)$) on a donc $a_k = a_{m-k}$ pour tout k.

   La liste des coefficients de Φ_n (pour $n \geqslant 3$) est donc la même qu'on la lise dans l'ordre des degrés croissants ou dans l'ordre des degrés décroissants.

VII. Irréductibilité des polynômes cyclotomiques

1. Soit A un élément de $\mathbb{Z}[X]$. Bien sûr, si A est irréductible dans $\mathbb{Q}[X]$, il l'est dans $\mathbb{Z}[X]$.

   Réciproquement, on suppose que A est irréductible dans $\mathbb{Z}[X]$.

   Donnons-nous deux polynômes B, C de $\mathbb{Q}[X]$ tels que $A = BC$.

   On réduit les coefficients de B au même dénominateur, et on factorise le pgcd des numérateurs obtenus. On peut alors écrire $B = \frac{b}{\beta}\widehat{B}$, où β et b sont deux entiers premiers entre eux, et où $\widehat{B}$ est un élément primitif de $\mathbb{Z}[X]$ (cf partie I.)

   De même, on peut écrire $C = \frac{c}{\gamma}\widehat{C}$, où $\gamma \wedge c = 1$ et où $\widehat{C}$ est primitif dans $\mathbb{Z}[X]$.

   $A = BC$ devient $\beta\gamma A = bc\widehat{B}\widehat{C}$. On en déduit $\beta\gamma\delta(A) = bc\delta(\widehat{B}\widehat{C}) = bc$ (voir partie I.)

   Puisque $\beta \wedge b = 1$ et $\gamma \wedge c = 1$, on voit que $\beta \mid c$ et $\gamma \mid b$ (théorème de Gauss.)

   Ainsi $A = BC$ devient $A = \Big(\frac{b}{\gamma}\,\widehat{B}\Big)\Big(\frac{c}{\beta}\,\widehat{C}\Big) = \Big(\frac{\beta}{\gamma}\,B\Big)\Big(\frac{\gamma}{\beta}\,C\Big)$.

   Cette dernière expression exprime A comme un produit de deux éléments de $\mathbb{Z}[X]$.

   L'irréductibilité de A sur $\mathbb{Z}[X]$ implique que $\frac{\beta}{\gamma}\,B$ ou $\frac{\gamma}{\beta}\,C$ est une constante de $\mathbb{Z}^*$.

   Ainsi l'un des deux polynômes B ou C est une constante de $\mathbb{Q}^*$.

   On a ainsi prouvé l'irréductibilité de A dans $\mathbb{Q}[X]$, ce qui achève la démonstration.

2. (a) On suppose par l'absurde qu'il existe $B = \sum_{k=0}^{r} b_k X^k$ et $C = \sum_{k=0}^{s} c_k X^k$ dans $\mathbb{Z}[X]$, non constants, et tels que $A = BC$.

   Pour être précis, on suppose $\deg B = r \geqslant 1$ ($b_r \neq 0$) et $\deg C = s \geqslant 1$ ($c_s \neq 0$.)

   En identifiant les termes constants, $a_0 = b_0 c_0$. Mais p est premier et divise a_0.
   On en déduit $p \mid b_0$ ou $p \mid c_0$. Supposons par exemple que p divise b_0.

   Il en résulte que p ne divise pas c_0 (sinon p^2 diviserait a_0) donc que $p \wedge c_0 = 1$.

   Pour tout entier k de $\{1, \dots, r\}$, on peut écrire $a_k = b_0 c_k + b_1 c_{k-1} + \cdots + b_{k-1} c_1 + b_k c_0$.

   Supposons qu'on ait prouvé que p divise $b_0, b_1, \dots, b_{k-1}$ (c'est vrai si $k = 1$.)

   Puisque $k \leqslant r < n$, l'entier p divise a_k et $b_0 c_k + b_1 c_{k-1} + \cdots + b_{k-1} c_1$.

   Il en résulte qu'il divise la différence $b_k c_0$, donc b_k car $p \wedge c_0 = 1$.

   Ainsi, par récurrence finie, p divise tous les coefficients $b_0, b_1, \dots, b_r$ de B.

   On en déduit que p divise le coefficient dominant $a_n = b_r c_s$ de A, ce qui est absurde.

   Conclusion : le polynôme A est irréductible sur $\mathbb{Q}[X]$.

   (b) Pour tout k de $\{1, \dots, p-1\}$, p divise $p! = k!(n-k)!\binom{p}{k}$.

   Mais p est premier avec $1, 2, \dots, k-1$ donc avec $k!(n-k)!$

   En utilisant le théorème de Gauss, il en résulte que p divise $\binom{p}{k}$.

   (c) On sait depuis IV.1.a que $\Phi_p = \dfrac{X^p - 1}{X - 1}$.

   On en déduit $\Phi_p(X+1) = \dfrac{1}{X}\Big(\sum_{k=0}^{p}\binom{p}{k}X^k - 1\Big) = \sum_{k=1}^{p}\binom{p}{k}X^{k-1} = \sum_{k=0}^{p-1}\binom{p}{k+1}X^k$.

   (d) On a obtenu $\Phi_p(X+1) = \binom{p}{1} + \binom{p}{2}X + \cdots + \binom{p}{k+1}X^k + \cdots + \binom{p}{p-1}X^{p-2} + X^{p-1}$.

   On voit que p divise tous les coefficients de $\Phi_p(X+1)$, sauf son coefficient dominant.

   D'autre part p^2 ne divise pas le coefficient constant $\binom{p}{1} = p$ de $\Phi_p(X+1)$.

   On est donc exactement dans les conditions d'application du critère d'Eiseinstein.

   On peut donc affirmer que le polynôme $\Phi_p(X+1)$ est irréductible sur $\mathbb{Q}[X]$.

VIII. Irréductibilité des polynômes cyclotomiques d'indice quelconque

1. (a) Dans $\mathcal{A}_z$, il y a des polynômes non constants, comme par exemple $X^n - 1$.

   L'ensemble $\{\deg(A) \geqslant 1,\ A \in \mathcal{A}_z\}$ est donc une famille finie non vide de $\mathbb{N}^*$.

   Cette famille contient nécessairement un plus petit élément m.

   Donnons-nous dans $\mathcal{A}_z$ un polynôme A de degré m. Quitte à diviser A par son coefficient dominant (ce qui ne change pas le fait que A est dans $\mathbb{Q}[X]$ et s'annule en z), on peut supposer que A est unitaire.

   Soit B un « autre » polynôme unitaire, de même degré que A, et s'annulant en z.

   Alors le polynôme $A - B$ s'annule en z et est de degré strictement inférieur à m.

   Par définition de m, le polynôme $A - B$ est nécessairement constant, donc nul.

   Ainsi, il existe dans $\mathcal{A}_z$ un unique polynôme M_z unitaire de degré minimum.

   (b) Si Q est un polynôme quelconque de $\mathbb{Q}[X]$, alors le polynôme $A = QM_z$ est élément de $\mathbb{Q}[X]$ et il s'annule en z : il est donc élément de $\mathcal{A}_z$.

   Réciproquement, soit A un élément de $\mathcal{A}_z$ (donc dans $\mathbb{Q}[X]$ et s'annulant en z.)

   La division euclidienne de A par M_z s'écrit $A = QM_z + R$, avec $\deg(R) < \deg(M_z)$.

   Le quotient et le reste dans cette division sont encore dans $\mathbb{Q}[X]$.

   On a $R(z) = A(z) - Q(z)M_z(z) = 0$, alors que $\deg(R) < \deg(M_z)$.

   La seule solution est que R soit constant, donc nul. Ainsi $A = QM_z$.

   Les polynômes de $\mathbb{Q}[X]$ s'annulant en z sont donc les QM_z, avec $Q \in \mathbb{Q}[X]$.

   (c) $X^n - 1$ est dans A_z. Il existe donc N_z dans $\mathbb{Q}[X]$ tel que $X^n - 1 = N_z M_z$.

   Puisque $X^n - 1$ et M_z sont unitaires, il en est de même de N_z.

   Ainsi N_z et M_z sont dans $\mathbb{Q}[X]$, unitaires, et leur produit est dans $\mathbb{Z}[X]$.

   La question I.3 montre que les polynômes M_z et N_z sont dans $\mathbb{Z}[X]$.

   (d) Supposons que M_z s'écrive sous la forme d'un produit AB, avec A, B dans $\mathbb{Q}[X]$.

   Si A, B étaient non constants, on aurait $\deg(A) < \deg(M_z)$ et $\deg(B) < \deg(M_z)$.

   Mais $0 = M_z(z) = A(z)B(z)$ impliquerait $A(z) = 0$ ou $B(z) = 0$ ce qui est absurde car par définition M_z est de degré minimum parmi les polynômes non constants de $\mathbb{Q}[X]$ qui s'annulent au point z.

   Ainsi l'égalité $M_z = AB$ dans $\mathbb{Q}[X]$ implique que A ou B est constant. En d'autres termes, le polynôme M_z est irréductible dans $\mathbb{Q}[X]$.

2. (a) Posons $A = \sum_{k\geqslant 0} a_k X^k$, $B = \sum_{k\geqslant 0} b_k X^k$.

   On a $\overline{A+B} = \sum_{k\geqslant 0} (\overline{a_k + b_k}) X^k = \sum_{k\geqslant 0} (\overline{a_k} + \overline{b_k}) X^k = \sum_{k\geqslant 0} \overline{a_k} X^k + \sum_{k\geqslant 0} \overline{b_k} X^k = \overline{A} + \overline{B}$.

   De même $\overline{AB} = \sum_{k\geqslant 0} \Big(\overline{\sum_{i+j=k} a_i b_j} \Big) X^k = \sum_{k\geqslant 0} \Big(\sum_{i+j=k} \overline{a_i}\,\overline{b_j} \Big) X^k = \overline{A}\,\overline{B}$.

   (b) On a $(A+B)^p = \sum_{k=0}^{p} \binom{p}{k} A^k B^{p-k} = A^p + B^p + \sum_{k=1}^{p-1} \binom{p}{k} A^k B^{p-k}$.

   D'après VII.2.b, on sait que p divise $\binom{p}{k}$ pour tout k de $\{1, \ldots, p-1\}$.

   On en déduit que $\sum_{k=1}^{p-1} \overline{\binom{p}{k} A^k B^{p-k}} = 0$ dans $F_p[X]$. Ainsi $\overline{(A+B)^p} = \overline{A^p} + \overline{B^p}$.

(c) Pour tous a, b de $\mathbb{Z}$, on a $(a+b)^p \equiv a^p + b^p$ (cas particulier de ce qui précède.)

On peut généraliser à m entiers : $(a_1 + a_2 + \cdots + a_m)^p \equiv a_1^p + a_2^p + \cdots + a_m^p \ [p]$.

Si on choisit $a_k = 1$ pour tout k, on trouve $m^p \equiv m \ [p]$ pour tout m de $\mathbb{N}^*$.

L'égalité $m^p \equiv m \ [p]$ est par ailleurs évidente si $m = 0$.

Si p est impair, un simple changement de signe donne $m^p \equiv m \ [p]$ pour $m \in \mathbb{Z}^{-*}$.

Enfin, si $p = 2$ et $m \in \mathbb{Z}^{-*}$, on a $m^p = (-m)^p \equiv -m \ [p] \equiv m \ [p]$.

Finalement, l'égalité de congruence $m^p \equiv m \ [p]$ est vraie pour tout m de $\mathbb{Z}$.

(d) Si $A = \sum_{k \geqslant 0} a_k X^k$, alors $\overline{A^p(X)} = \overline{(\sum_{k \geqslant 0} a_k X^k)^p} = \sum_{k \geqslant 0} \overline{(a_k X^k)^p}$ (généralisation de (b).)

On en déduit $\overline{A^p(X)} = \sum_{k \geqslant 0} \overline{a_k^p} X^{pk}$ donc $\overline{A^p(X)} = \sum_{k \geqslant 0} \overline{a_k} (X^p)^k$ d'après (c).

On a bien obtenu $\overline{A^p(X)} = \overline{A}(X^p)$.

3. (a) Les polynômes M_a et M_b sont unitaires et irréductibles dans $\mathbb{Q}[X]$.

Si on suppose $M_a \neq M_b$, alors ces deux polynômes sont premiers entre eux.

$X^n - 1$, qui est divisible par M_a et M_b, est donc divisible par $M_a M_b$ dans $\mathbb{Q}[X]$.

Autrement dit, il existe Q dans $\mathbb{Q}[X]$ tel que $X^n - 1 = M_a(X) M_b(X) Q(X)$.

Puisque $X^n - 1, M_a, M_b$ sont unitaires, Q est unitaire.

La question I.3 montre alors que Q est un élément de $\mathbb{Z}[X]$.

(b) On sait que M_b s'annule en $b = a^p$ (c'est même le polynôme minimal de b.)

Ainsi $M_b(X^p)$ (élément de $\mathbb{Q}[X]$) s'annule en a : c'est un élément de A_a.

La question VIII.1.b donne alors : $\exists\, R \in \mathbb{Q}[X],\ M_b(X^p) = M_a(X) R(X)$.

La question I.3 montre à nouveau que $R(X)$ est unitaire et dans $\mathbb{Z}[X]$.

On transforme cette égalité dans $\mathbb{Z}[X]$ en une égalité dans $F_p[X]$.

On trouve $\overline{M_b(X^p)} = \overline{M_a(X) R(X)} = \overline{M_a(X)}\ \overline{R(X)}$.

La question (2d) donne alors $\overline{M_b(X)}^p = \overline{M_a(X)}\ \overline{R(X)}$.

(c) Par hypothèse $S(X)$ divise $M_a(X)$ donc divise $\overline{M_b(X)}^p$ dans $F_p[X]$.

Mais $S(X)$ est irréductible dans $F_p[X]$. Il divise donc $\overline{M_b(X)}$ dans $F_p[X]$.

$X^n - 1 = M_a(X) M_b(X) Q(X)$ implique que $S^2(X)$ divise $X^n - 1$ dans $F_p[X]$.

(d) Il existe donc $T(X)$ tel que $X^n - \overline{1} = S^2(X) T(X)$ (égalité dans $F_p[X]$.)

Par dérivation : $nX^{n-1} = S(X)(2S'(X)T(X) + S(X)T'(X))$.

Ainsi $S(X)$, irréductible et unitaire dans $F_p(X)$, divise nX^{n-1} dans $F_p(X)$.

Puisque $n \neq 0$ dans F_p (en effet $p \nmid n$) il en découle $S(X) \mid X$ donc $S(X) = X$.

Mais ceci est absurde car X ne divise pas $X^n - 1$.

On a donc abouti à une contradiction en partant de l'hypothèse que les polynômes minimaux de a et de $b = a^p$ étaient distincts.

On peut donc affirmer que le polynôme minimal M_a de a s'annule sur tous les $b = a^p$, pour p entier premier ne divisant pas n.

4. (a) La question II.7 montre qu'il existe un entier m tel que $b = a^m$, avec $m \wedge n = 1$.

   L'entier m s'écrit donc comme le produit d'entiers premiers qui ne divisent pas n.

   Ainsi on peut passer de a à b par une succession finie d'exponentiations $z \mapsto z^p$, où les entiers p sont premiers et ne divisent pas n. Mais on sait que dans une telle exponentiation $z \mapsto z^p$, le polynôme minimal ne change pas.

   On en déduit que M_a est aussi le polynôme minimal de b.

   (b) Ainsi le polynôme M_a admet tous les b de R_n pour racines, ce qui assure qu'il est divisible par Φ_n. Mais comme Φ_n (en tant qu'élément particulier de A_a) est divisible par M_a (cf VIII.1.b), on en déduit l'égalité $M_a = \Phi_n$.

   Or on sait que le polynôme M_a est irréductible sur $\mathbb{Q}[X]$ (cf VIII.1.d)

   On en déduit finalement que Φ_n est irréductible sur $\mathbb{Q}[X]$, pour tout n de $\mathbb{N}^*$.