Algèbre Générale : Arithmétique

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 $A = \sum_{k\geqslant 0} a_k X^k$ 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.

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