D.M. 14 : φ, cyclotomie, et fonctions multiplicatives

1. Racines primitives de l'unité

Soit $n \in \mathbb{N}^*$, pour tout $k \in [\![0, n-1]\!]$, on note $\omega_k = e^{2ik\pi/n}$.

Définition – Soit $\omega \in \mathbb{U}_n$. On dit que ω est une racine *primitive* n-ième de l'unité si, et seulement si, $< \omega >= \mathbb{U}_n$, autrement dit ω est un générateur du groupe $(\mathbb{U}_n, \times)$.On notera ici $\mathbb{P}_n$ l'ensemble des racines primitives n-ième de l'unité.

Remarque – On sait que $\mathbb{U}_n =< \omega_1 >$ donc $\omega_1 \in \mathbb{P}_n$.

a) Déterminer $\mathbb{P}_n$ si $n = 2, 3, 4, 5, 6$.

b) Justifier que ω_k est une racine primitive n-ième de l'unité si, et seulement si, $\bar{k}$ est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.

c) Montrer que $\omega_k \in \mathbb{P}_n$ ssi $k \wedge n = 1$.

1.2. Ordre et fonction φ

a) Soit $n \in \mathbb{N}^*$ et $\omega_k = e^{2ik\pi/n}$. Soit d un diviseur de n. Montrer que $\omega_k \in \mathbb{P}_d \Leftrightarrow k \wedge n = \frac{n}{d}$. Autrement dit $ord(\omega_k) = n/(k \wedge n)$.
(On pourra commencer à comprendre ce que veut dire cet énoncé sur $\mathbb{U}_6$ ou $\mathbb{U}_{12}$.)

b) En déduire que $\mathbb{U}_n = \coprod_{d|n} \mathbb{P}_d$. Autrement dit, $\mathbb{U}_n$ est l'union disjointe, prise pour tous les d diviseurs de n, des ensembles $\mathbb{P}_d$.

c) En déduire que :

$$\boxed{n = \sum_{d|n} \varphi(d).}$$

2 Polynômes cyclotomiques

Soit $n \in \mathbb{N}^*$ on note $\Phi_n \in \mathbb{C}[X]$ le polynôme défini par :

$$\Phi_n(X) = \prod_{\omega \in \mathbb{P}_n} (X - \omega) = \prod_{k \wedge n = 1} (X - \omega_k)$$

2.1. Premiers exemples

a) Expliciter l'écriture développée de Φ_2, Φ_3, Φ_4 et Φ_6.

b) Expliciter l'écriture développée de Φ_p si p est un nombre premier.

c) Que dire, d'une manière générale, du degré de Φ_n ?

d) Soit q un entier impair différent de 1. Montrer que $\omega \in \mathbb{P}_{2q} \Leftrightarrow -\omega \in \mathbb{P}_q$. En déduire que : $\Phi_{2q}(X) = \Phi_q(-X)$.

2.2. Formule du produit et conséquence : coefficients entiers, valeur de $\Phi_n(1)$

a) Montrer que si $n \in \mathbb{N}^*$, alors $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

b) Si P et Q sont deux polynômes à coefficients entiers (on notera $P \in \mathbb{Z}[X]$ et $Q \in \mathbb{Z}[X]$) et que Q est de coefficient dominant 1, justifier que le quotient de la division euclidienne de P par Q est encore un polynôme à coefficient entiers.

c) Déduire ce qui précède que pour tout n, $\Phi_n \in \mathbb{Z}[X]$.
Remarque : Le fait que ces polynômes soient à coefficients entiers est très important, cela leur confère un statut « universel » mais c'est une autre histoire.

d) Montrer aussi :

$$n = \prod_{d|n,\ d \neq 1} \Phi_d(1).$$

e) Montrer que si $n \in \mathbb{N}$ a au moins deux diviseurs premiers distincts, alors $\Phi_n(1) = 1$.

3 Notion de fonctions multiplicatives en arithmétique

3.1. Définitions

a) **Définition (particulière à l'arithmétique !) :** une fonction $f : \mathbb{N}^* \to \mathbb{N}$ est dite, ici, *multiplicative* si, et seulement si, f *n'est pas la fonction nulle* et :

$$\forall\, (m,n) \in (\mathbb{N}^*)^2,\ m \wedge n = 1 \Rightarrow f(m.n) = f(m).f(n)$$

i) Montrer que si f est une fonction multiplicative, alors $f(1) = 1$.

ii) Montrer que si $m_1, \ldots, m_s$ sont des entiers *deux à deux premiers entre eux* et si f est multiplicative alors $f(\prod_{i=1}^{s} m_i) = \prod_{i=1}^{s} f(m_i)$.

b) **La fonction μ de Möbius.**

Définition : Soit $n = p_1^{r_1} \ldots p_s^{r_s}$ un entier naturel non nul, décomposé ici en facteurs premiers. On définit la fonction μ comme suit : $\mu(1) = 1$, $\mu(n) = 0$ si l'un des exposants r_i est strictement supérieur à 1, et $\mu(n) = (-1)^s$ sinon.

Autrement dit, pour n différent de 1, $\mu(n)$ est nul dès que n a un de ses facteurs premiers avec une puissance différente de 1, et vaut 1 si n est le produit d'un nombre pair de nombres premiers (tous à la puissance 1) et -1 si n est le produit d'un nombre impair de nombres premiers (chacun à la puissance 1).

Montrer que μ est une fonction multiplicative.

3.2. Fonction « somme » d'une fonction multiplicative

a) **Lemme clef :** Soit $f : \mathbb{N}^* \to \mathbb{N}$ une fonction multiplicative. Pour tout $n \in \mathbb{N}^*$, on pose $F(n) = \sum_{d|n} f(d)$. Montrer F est une fonction multiplicative.

b) Si $f = \varphi$ la fonction d'Euler introduite en cours.
Soit F la fonction associée $F(n) = \sum_{d|n} \varphi(d)$. On veut retrouver avec le résultat du a) la propriété déjà prouvée au § 1) , c'est-à-dire que $F = \mathrm{id}_{\mathbb{N}^*}$. Pour cela :

i) A partir de la valeur de $\varphi(p^r)$ pour p premier, calculer la valeur de $F(p^r)$.

ii) En déduire que pour tout $n \in \mathbb{N}^*$, $F(n) = n$.

c) Si $f = \mu$ la fonction de Möbius. On veut calculer la fonction F définie par $F(n) = \sum_{d|n} \mu(d)$.

i) Calculer $F(p^r)$ pour $p \in \mathbb{P}$.

ii) En déduire que F est la fonction qui est nulle sur $[2, +\infty[$ et vaut 1 en 1 Autrement dit, on a montré que :

$$\boxed{\forall\, n \in \mathbb{N}_{\geq 2},\ \sum_{d|n} \mu(d) = 0.}$$

iii) Justifier qu'on peut calculer toutes les valeurs de la fonction μ sans utiliser la D.F.P. en utilisant seulement que $\mu(1) = 1$ et que pour tout $n \in \mathbb{N}_{\geq 2}$, $\sum_{d|n} \mu(d) = 0$.

3.3.Le rôle clef de la fonction de Möbius pour l'inversion d'une somme

La définition qu'on a donnée de la fonction de Möbius semble tomber du ciel. Pour comprendre dans quel contexte apparaît la fonction de Möbius, considérons une suite $(b_n)_{n\in\mathbb{N}^*}$ d'entiers naturels (ce qui est une autre façon de dire qu'on considère une fonction $b : \mathbb{N}^* \to \mathbb{N}$, $n \mapsto b(n) = b_n$) et la suite $(a_n)_{n\in\ \mathbb{N}^*}$ définie par :

$$a_n = \sum_{d|n} b_d, \quad (\dagger)$$

alors la suite $b = (b_n)_{n\geq 1}$ permet de calculer la suite $a = (a_n)_{n\geq 1}$, mais on peut aussi inverser la relation (†) pour exprimer la suite b à partir de a. Cela se fait de proche en proche, en utilisant le fait que :

$$b_n = a_n - \sum_{d|n, d\neq n} b_d.$$

On obtient ainsi :

$$b_1 = a_1,\ b_2 = a_2 - b_1 = a_2 - a_1,\ b_3 = a_3 - a_1,$$
$$b_4 = a_4 - a_2, \text{ etc}$$

Prenons comme suite a particulière la suite dite à *impulsion initiale* telle que $a_1 = 1$ et $\forall\, i \geq 2,\ a_i = 0$.

a) Quelle est la suite b associée à la suite a à impulsion initiale ?

b) Le rôle crucial de la fonction de Möbius vient alors du :
Théorème (à démontrer !) Si f est une fonction de $\mathbb{N}^*$ dans $\mathbb{N}$ et si $F(n) = \sum_{d|n} f(d)$ pour tout $n \in \mathbb{N}^*$ alors :

$$\forall\, n \in \mathbb{N}^*,\ f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d}).$$

3.4. La convolution arithmétique

Soit $E = \mathcal{F}(\mathbb{N}^*, \mathbb{C})$ i.e. l'ensemble des suites complexes indexées par $\mathbb{N}^*$.
Pour tout entier n naturel, on note D_n l'ensemble des diviseurs de n dans $\mathbb{N}$.
On définit une loi de composition interne $*$ sur E comme suit :
si f et g sont deux élément de E, on définit pour tout $n \in \mathbb{N}^*$, $(f * g)(n) = \sum_{d\in D_n} f(d) g(\frac{n}{d})$.

a) Etudier les propriétés de la loi $*$: commutativité, associativité,

b) En notant δ la suite définie par $\delta_0 = 1$ et $\forall\, n \geq 1,\ \delta_n = 0$, justifier que δ est le neutre pour $*$.

c) Montrer que $(E, +, *)$ est un anneau commutatif.

d) Montrer que μ est l'inverse pour $*$ de la fonction constante égale à 1 ce qu'on écrira $\mu * 1 = \delta$.

e) En remarquant qu'avec les notations du 3.3. $F = f * 1$, retrouver alors le théorème du 3.3. b).

f)Justifier qu'on a montré ci-dessus que $\varphi * 1 = \text{id}$ où 1 est la fonction constante égale à 1 et en déduire alors aussi une expression de φ. en fonction de μ .