Algèbre
(par André Joyal)

Ces notes ont été préparées à l'intention des jeunes stagiaires en mathématiques à l'UQAM en juin-juillet 2003.

Synopsis:

1. Formule de Cardan

Avant de discuter de l'équation du troisième degré, il est bon de faire un bref rappel sur l'équation du second degré:

$$x^2 + ax + b = 0.$$

Cette équation se simplifie grandement si on effectue un changement de variable $x = y + t$ avec un choix convenable de t. En effet, si on remplace x par $y + t$ dans le polynôme $x^2 + ax + b$ on obtient

$$x^2 + ax + b = (y + t)^2 + a(y + t) + b = y^2 + (2t + a)y + t^2 + at + b.$$

Le coefficient de y^2 dans cette dernière expression est $2t + a$. Si on donne à t la valeur $-\frac{a}{2}$ ce coefficient s'annule et on a

$$x^2 + ax + b = y^2 - q$$

avec $q = (a/2)^2 - b$. L'équation initiale devient équivalente à l'équation

$$y^2 = q$$

avec $x = y - a/2$. Par suite,

$$x = -\frac{a}{2} \pm \sqrt{\left(\frac{a}{2}\right)^2 - b}$$

L'observation suivante attribuée à Al-Khwarizmi (circa 840) est importante pour ce qui suit. Si x_1 et x_2 sont les deux solutions de l'équation $x^2 + ax + b = 0$ alors on a

$$x^2 + ax + b = (x - x_1)(x - x_2) = x^2 - (x_1 + x_2)x + x_1x_2$$

Autrement dit,

$$x_1 + x_2 = -a$$
$$x_1x_2 = b.$$

Cela montre que si on connait la somme s et le produit p de deux quantités inconnues x_1 et x_2, on peut obtenir ces quantités en résolvant l'équation du second degré $x^2 - sx + p = 0$. Un résultat semblable est vrai si on connait la différence et le produit de deux quantités inconnues.

L'équation du 3-ième degré apparait naturellement dans certains problèmes de géométrie comme celui de la division d'un angle en trois. Si $q = \sin\theta$ alors $x = \sin(\theta/3)$ satisfait l'équation

$$4x^3 + q = 3x.$$

L'astronome mathématicien Claude Ptolémée (150 après JC) publia les premières tables de trigonométrie. Il obtint la valeur de $\sin(3^o)$ avec des constructions géométrique par règle et compas. Mais ces constructions ne peuvent donner la valeur de $\sin(1^o)$. Il dut se résoudre à utiliser l'approximation

$$\sin(1^o) \simeq \frac{1}{3}\sin(3^o).$$

Le mathématicien Al-Kashi (1429) obtint une valeur plus précise en calculant numériquement une solution de l'équation du troisième degré

$$4x^3 + \sin(3^o) = 3x.$$

Au 16^e siècle plusieurs mathématiciens italiens s'efforcèrent de résoudre des équations du troisième degré en utilisant des racines cubiques. La solution aurait été découverte indépendamment par Scippione del Ferro (1456-1526) et Niccolo Tartaglia (1500-1557). Les découvreurs n'ont pas publié leur solution. Mais Tartaglia confie cette solution à Jérome Cardan, un compatriote médecin et mathématicien. Celui-ci la publie dans son *Ars Magna* en 1545. Nous allons décrire cette solution en utilisant les notations algébriques introduites plus tard par Francois Viète (1540-1603).

On peut commencer par simplifier l'équation

$$x^3 + ax^2 + bx + c = 0$$

en effectuant un changement de variable $x = y + t$ pour un choix convenable de t. En effet,

$$(y+t)^3 + a(y+t)^2 + b(y+t) + c = y^3 + y^2(3t+a) + y(3t^2+2at+b) + (t^3+at^2+bt+c).$$

Le coefficient de y^2 dans cette dernière expression est $3t + a$. Si on donne à t la valeur $-\frac{a}{3}$ ce coefficient s'annule et on obtient que

$$x^3 + ax^2 + bx + c = y^3 + py - q$$

avec

$$p = b - \frac{a^2}{3} \quad \text{et} \quad q = \frac{ba}{3} - \frac{2a^3}{27} - c.$$

L'équation initiale est alors équivalente à l'équation

$$y^3 + py = q.$$

Nous allons voir que cette dernière admet une solution donnée par la *formule de Cardan*:

$$y = \sqrt[3]{\sqrt{D} + \frac{q}{2}} - \sqrt[3]{\sqrt{D} - \frac{q}{2}}.$$

où l'on a posé $D = \left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2$. Pour obtenir cette formule on suppose que l'on a $y = u - v$ où u et v sont des variables auxiliaires dont les valeurs seront à déterminer. Si on remplace y par $u - v$ dans le polynôme $y^3 + py$ on obtient

$$y^3 + py = (u-v)^3 + p(u-v) = u^3 - v^3 + (p - 3uv)(u-v).$$

Cette expression se simplifie si on suppose que $3uv = p$. Faisons une pause pour dire que cette hypothèse n'est pas déraisonnable car les conditions $u - v = y$ et $uv = p/3$ signifient que

$$(U-u)(U+v) = U^2 - yU - \frac{p}{3}.$$

Si y était connu il suffirait de trouver les racines de ce polynôme pour obtenir u et v. Ce point étant éclaircit, reprenons nos calculs en supposant que $y = u-v$ et $3uv = p$. L'équation $y^3+py = q$ devient alors $u^3-v^3 = q$. Comme $3uv = p$, on a aussi $27u^3v^3 = p^3$. Cela donne un système de deux équations à résoudre pour u^3 et v^3:

$$u^3 - v^3 = q \quad \text{et} \quad u^3v^3 = \frac{p^3}{27}$$

Pour résoudre ce système il suffit de caculer les racines du polynôme du second degré

$$(Z - u^3)(Z + v^3) = Z^2 - Zq - \frac{p^3}{27}.$$

On obtient que

$$u^3 = \frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \frac{p^3}{27}} \quad \text{et} \quad -v^3 = \frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \frac{p^3}{27}}.$$

Autrement dit,

$$u^3 = \sqrt{D} + \frac{q}{2} \quad \text{et} \quad v^3 = \sqrt{D} - \frac{q}{2}.$$

Ce qui donne la formule de Cardan:

$$y = u - v = \sqrt[3]{\sqrt{D} + \frac{q}{2}} - \sqrt[3]{\sqrt{D} - \frac{q}{2}}.$$

La formule de Cardan a un comportement curieux. Elle peut faire apparaitre des nombres irrationnels dans les calculs bien que la solution soit rationnelle. Par exemple, appliquons la formule à l'équation $x^3+3x = 4$. On obtient une expression irrationelle compliquée:

$$x = \sqrt[3]{\sqrt{5} + 2} - \sqrt[3]{\sqrt{5} - 2}.$$

Mais le calcul numérique donne

$$x = 1.618033989... - .618033989... = 1.000000000...$$

On vérifie que $x = 1$ est effectivement une solution. Mais il y a plus étrange encore. L'équation $x^3 = 15x + 4$ admet $x = 4$ pour solution. La formule de Cardan donne

$$x = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}}.$$

Il est impossible de poursuivre le calcul. Pour cela, il faudrait prendre la racine carré d'un nombre négatif $D = -121$. La formule de Cardan est en difficulté si $D < 0$ l Cardan qualifie ce cas d'*irréductible*. Il tente de poursuivre malgré tout le calcul avec des nombres qu'il qualifie d'*absurdes* et d'*impossibles*. Mais il n'y parvient pas vraiment. Il appartiendra à Bombelli d'introduire les *nombres complexes* $a + bi$ avec $i^2 = -1$. Remarquant que $(2 \pm i)^3 = 2 \pm 11i$, il obtient que

$$x = \sqrt[3]{2 + 11i} + \sqrt[3]{2 - 11i} = (2 + i) + (2 - i) = 4.$$

En effet, on peut montrer que l'équation $x^3 + px = q$ a trois solutions réelles distinctes ssi $D < 0$. Les nombres complexes ont été introduit pour calculer des solutions *réelles*.

Exercices

L'équation du quatrième degré a été résolue par Ferrari, un étudiant de Cardan. La première étape consiste à remplacer l'équation générale

$$x^4 + ax^3 + bx^2 + cx + d = 0$$

par une équation plus simple

$$y^4 + py^2 + qy + r = 0.$$

Pour cela il suffit de poser $y = x - a/4$.

Exercice 1: Vérifier cette dernière affirmation.

Pour la seconde étape nous aurons besoin de l'observation suivante: un polynome du second degré $Ax^2 + Bx + C$ possède une racine double ssi son discriminant $B^2 - 4AC$ est nul; dans ce cas, on a

$$Ax^2 + Bx + C = A(x + B/2A)^2.$$

Retournons maintenant à l'équation $y^4 + py^2 + qy + r = 0$. Si y est solution de cette équation alors on a

$$y^4 = -py^2 - qy - r$$

et par suite

$$(y^2 + t)^2 = y^4 + 2y^2t + t^2 = 2y^2t + t^2 - py^2 - qy - r = (2t - p)y^2 - qy + (t^2 - r)$$

où t est une variable quelconque. L'idée de Ferrari est de donner à t une valeur t_0 pour que le polynôme du second degré

$$(2t - p)y^2 - qy + (t^2 - r) = Ay^2 + By + C$$

ait une racine double. Pour cela il faut que son discriminant

$$B^2 - 4AC = q^2 - 4(2t - p)(t^2 - r)$$

soit nul. Cette expression est un polynôme du troisième degré dans la variable t. On peut lui trouver une racine t_0 par la formule de Cardan. Si $t = t_0$, on obtient que

$$(y^2 + t_0)^2 = (2t_0 - p)y^2 - qy + (t_0^2 - r) = A\big(y + \frac{B}{2A}\big)^2 = (2t_0 - p)\Big(y + \frac{t_0^2 - r}{2(2t_0 - p)}\Big)^2$$

Si on prend ensuite la racine carré de chaque membre de cette égalité, on obtient que

$$y^2 + t_0 = \sqrt{2t_0 - p}\Big(y + \frac{t_0^2 - r}{2(2t_0 - p)}\Big).$$

Cela donne une équation de second degré en y. Il suffit de la résoudre pour obtenir la solution de l'équation initiale.

Exercise 2: Vérifier les calculs de Ferrari.

Exercise 3: Vérifier que si $x = y + t$ alors on a

$$x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_1x + a_0 = y^n + p_1y^{n-1} + p_2y^{n-2} + \cdots + p_1y + p_0$$

avec $p_1 = nt + a_1$. En particulier, on a $p_1 = 0$ si on prend $t = -a_1/n$.

2. Nombres complexes

Les nombres complexes ont été inventés par Rafaë l Bombelli suite aux travaux de Cardan sur l'équation du troisième degré.

Dans ce qui suit nous dénoterons par $\mathbf{R}$ l'ensemble des nombres réels, positifs, négatifs ou nuls. Formellement, un *nombre complexe* $z = a + bi$ est un couple (a, b) de nombres réels; on dit que a est la *partie réelle* de z et que b est sa *partie imaginaire*. On peut voir (a, b) comme les coordonnées d'un point du plan cartésien

ou bien comme les composantes d'un vecteur du plan; on dit que c'est le *plan complexe*. Nous dénoterons par $\mathbf{C}$ l'ensemble des nombres complexes:

$$\mathbf{C} = \{a + bi : a, b \in \mathbf{R}\}.$$

La *somme* $z+w$ de deux nombres complexes $z = a+bi$ et $w = c+di$ est la somme vectorielle: $(a, b)+(c, d) = (a + c, b + d)$. Autrement dit,

$$z + w = (a + c) + (b + d)i.$$

Le *produit* zw est donné par la formule $(a, b)(c, d) = (ac - bd, ac + bd)$. Autrement dit,

$$zw = (ac - bd) + (ad + bc)i.$$

Cette définition implique que $ii = -1$; par suite, $i = \sqrt{-1}$. On dit que le nombre $\bar{z} = a - bi$ est le *conjugué* de $z = a + bi$. On vérifie facilement les identités

$$\overline{z + w} = \bar{z} + \bar{w}$$
$$\overline{zw} = \bar{z}\bar{w}.$$

Si $z = a + bi$ alors $z\bar{z} = a^2 + b^2 =\mid z \mid^2$. Le nombre $\mid z \mid= \sqrt{a^2 + b^2}$ est la longueur de z considéré comme vecteur du plan. On dit que c'est le *module* de z. On montre que $\mid z + w \mid\leq\mid z \mid + \mid w \mid$ et $\mid zw \mid=\mid z \mid \cdot \mid w \mid$. Tout nombre complexe non nul $z = a + bi$ possède un inverse

$$z^{-1} = \frac{\bar{z}}{z\bar{z}} = \frac{a - bi}{a^2 + b^2} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i.$$

Tout nombre complexe non nul $z = a + bi$ possède deux racines carrées distinctes $w = \pm z^{\frac{1}{2}}$. On peut les obtenir en résolvant l'équation $w^2 = z$ pour un nombre complexe inconnu $w = u + iv$. On a

$$w^2 = (u + iv)(u + iv) = (u^2 - v^2) + 2uvi.$$

L'équation $w^2 = z$ est donc équivalente au système de deux équations

$$u^2 - v^2 = a \quad \text{et} \quad 2uv = b$$

qu'il faut résoudre pour des quantités *réelles* inconnues u et v. L'équation $w^2 = z$ entraîne que $\mid w \mid^2=\mid z \mid$. Par suite, $u^2 + v^2 =\mid z \mid$. Ainsi donc,

$$u^2 = \frac{u^2 + v^2}{2} + \frac{u^2 - v^2}{2} = \frac{\mid z \mid +a}{2}$$
$$v^2 = \frac{u^2 + v^2}{2} - \frac{u^2 - v^2}{2} = \frac{\mid z \mid -a}{2}.$$

La condition $b = 2uv$ montre que u et v sont de même signe si $b > 0$, et de signes opposés si $b < 0$. Si $b \geq 0$ on obtient que

$$u = \pm\sqrt{\frac{\mid z \mid +a}{2}} \quad \text{et} \quad v = \pm\sqrt{\frac{\mid z \mid -a}{2}}$$

et si $b \leq 0$ on obtient que

$$u = \pm\sqrt{\frac{\mid z \mid +a}{2}} \qquad \text{et} \quad v = \mp\sqrt{\frac{\mid z \mid -a}{2}}.$$

Par exemple, on a

$$\sqrt{i} = \pm\Big(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\Big) \quad \text{et} \quad \sqrt{-i} = \pm\Big(\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i\Big).$$

La construction des racines carrées permet de construire des racines quatrièmes $z^{\frac{1}{4}} = (z^{\frac{1}{2}})^{\frac{1}{2}}$, des racines 8-ièmes, etc.

Les nombres $\pm 1, \pm i$ satisfont l'équation $x^4 = 1$. C'est pourquoi on dit que ce sont les *racines quatrièmes de l'unité*. Remarquer la factorisation $x^2 + 1 = (x - i)(x + i)$. On en déduit que

$$x^4 - 1 = (x^2 - 1)(x^2 + 1) = (x - 1)(x + 1)(x - i)(x + i).$$

Tout nombre complexe $z \neq 0$ a deux racines carrés $\pm z^{\frac{1}{2}}$ et quatre racines quatrièmes $\pm z^{\frac{1}{4}}, \pm iz^{\frac{1}{4}}$.

Les *racines cubiques de l'unité* sont les solutions de l'équation $x^3 = 1$. La factorisation $x^3 - 1 = (x - 1)(x^2 + x + 1)$ montre qu'en plus de $x = 1$ ces racines sont obtenues en résolvant l'équation du second degré $x^2 + x + 1 = 0$. Les deux autres racines sont

$$\omega = \frac{-1 + i\sqrt{3}}{2} \quad \text{et} \quad \omega^2 = \frac{-1 - i\sqrt{3}}{2}.$$

On obtient que

$$x^3 - 1 = (x - 1)(x - \omega)(x - \omega^2).$$

Nous verrons que tout nombre complexe $z \neq 0$ a trois racines cubiques $z^{\frac{1}{3}}, \omega z^{\frac{1}{3}}, \omega^2 z^{\frac{1}{3}}$. L'équation du troisième degré $x^3 + px = q$ possède en général trois solutions x_1,x_2 et x_3. Dans la formule de Cardan, les racines cubiques $u = \left(\sqrt{D} + \frac{q}{2}\right)^{\frac{1}{3}}$ et $v = \left(\sqrt{D} - \frac{q}{2}\right)^{\frac{1}{3}}$ doivent satisfaire la condition $3uv = p$ (remarquer que l'on a toujours $u^3v^3 = 27p^3$, ce qui entraîne que la condition $3uv = p$ est automatiquement satisfaite lorsque u et v sont réels). Dans ce cas,

$$x_1 = u - v, \qquad x_2 = \omega u - \omega^2 v \quad \text{et} \quad x_3 = \omega^2 u - \omega v.$$

Si $p \neq 0$, on a $u \neq 0$. Dans ce cas, on peut prendre $v = p/3u$ ce qui nous permet d'écrire

$$x_1 = u - \frac{p}{3u}, \qquad x_2 = \omega u - \frac{p}{3\omega u} \quad \text{et} \quad x_3 = \omega^2 u - \frac{p}{3\omega^2 u}.$$

Pour calculer avec les nombres complexes il est commode d'utiliser les *coordonnées polaires*. Le passage des coordonnées cartésiennes (a, b) aux coordonnées polaires (r, θ) s'obtient des relations $a = r\cos\theta$ et $b = r\sin\theta$. Si $z = a + bi$ alors on a

$$z = r(\cos\theta + i\sin\theta)$$

avec $r = \mid z \mid$. On dit que l'angle θ est l'*argument* de z (il est défini modulo un multiple entier de 2π si $z \neq 0$). On a

$$\cos\theta = \frac{a}{\sqrt{a^2 + b^2}} \quad \text{et} \quad \sin\theta = \frac{b}{\sqrt{a^2 + b^2}}.$$

Pour calculer θ il est commode d'utiliser la formule

$$\frac{\theta}{2} = \arctan\frac{b}{r + a}$$

car elle fournit une valeur non-ambigue de θ comprise dans l'intervalle $(-\pi, \pi)$, à moins que z soit un nombre réel < 0, auquel cas on peut prendre $\theta = \pi$.

La formule suivante joue un role important en théorie des nombres complexes:

$$(\cos\theta + i\sin\theta)(\cos\psi + i\sin\psi) = \cos(\theta + \psi) + i\sin(\theta + \psi).$$

On dit que c'est la *formule de De Moivre*. Elle est équivalente aux formules d'*addition des angles* pour les fonctions sinus et cosinus:

$$\begin{aligned}\cos(\theta+\psi) &= \cos\theta\cos\psi - \sin\theta\sin\psi \\ \sin(\theta+\psi) &= \cos\theta\sin\psi + \sin\theta\cos\psi\end{aligned}.$$

Si $z = r(\cos\theta + i\sin\theta)$ la formule de De Moivre entraîne que l'on a

$$z^n = r^n(\cos n\theta + i\sin n\theta)$$

pour tout entier $n \in \mathbf{Z}$. Si $z^n = 1$ on dit que z est *racine n-ième de l'unité*. Par exemple, le nombre complexe

$$u = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

est une racine n-ième de l'unité car on a $u^n = \cos 2\pi + i\sin 2\pi = 1$. Il résulte de la formule de De Moivre que les racines de l'unité sont toutes de la forme

$$u^k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$$

pour $0 \geq k < n$. Géométriquement, ces racines sont situées aux sommets d'un polygone régulier inscrit dans le cercle de rayon 1 centré à l'origine.

La formule de De Moivre permet de voir que tout nombre complexe possède une racine n-ième. Si $z = r(\cos\theta + i\sin\theta)$ alors

$$z^{\frac{1}{n}} = r^{\frac{1}{n}}\Big(\cos\frac{\theta}{n} + i\sin\frac{\theta}{n}\Big)$$

est une racine n-ième de z. Cette racine n'est pas unique. Les racines n-ième de z sont

$$u^k z^{\frac{1}{n}} = r^{\frac{1}{n}}\Big(\cos\frac{\theta+2k\pi}{n} + i\sin\frac{\theta+2k\pi}{n}\Big) \quad \text{pour} \quad 0 \leq k < n$$

où $u = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$. Géométriquement, ces racines sont situées aux sommets d'un polygone régulier inscrit dans le cercle de rayon $r^{\frac{1}{n}}$ centré à l'origine. En particulier, tout nombre complexe $z \neq 0$ possède trois racines cubiques $z^{\frac{1}{3}}$, $\omega z^{\frac{1}{3}}$ et $\omega^2 z^{\frac{1}{3}}$.

Les opérations sur les nombres complexes ont un sens géométrique. C'est clair pour la somme, car c'est une somme vectorielle. Pour comprendre la signification de produit il faut utiliser le concept de similitude. Si z est un nombre complexe non nul, et si a, b et c sont des nombres complexes distincts, alors le triangle ayant pour sommets za, zb, zc est semblable au triangle a, b, c. Il faut ajouter que la similitude est directe, ce qui signifie que l'orientation du triangle za, zb, zc est la même que celle du triangle a, b, c. De plus, le rapport entre les côtés du triangle za, zb, zc et les côtés correspondant du triangle a, b, c est égal au module de z. En particulier, si a est un nombre complexe non nul alors le triangle $0, z, za$ est semblable au triangle $0, 1, a$. Cette propriété permet de construire géométriquement le produit za à partir de z et de a. Si z est de module 1 et d'angle θ, l'application $a \mapsto za$ est une rotation d'angle θ autour de l'origine. En particulier, la multiplication par i est une rotation de 90^o autour de l'origine. Le fait que $i^2 = -1$ signifie simplement que le composé de deux rotations de 90^o dans le même sens est une rotation de 180^o.

On peut donner aux nombres complexes une interprétation matricielle. Rappellons la règle de multiplication des matrices carrées 2×2:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}.$$

On peut montrer qu'une rotation d'angle θ autour de l'origine (dans le sens positif) est représentée par la matrice

$$R(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

Comme une rotation d'angle θ suivie d'une rotation d'angle ψ est une rotation d'angle $\theta + \psi$, on obtient l'identité

$$\begin{pmatrix} \cos\psi & -\sin\psi \\ \sin\psi & \cos\psi \end{pmatrix} \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} \cos(\theta+\psi) & -\sin(\theta+\psi) \\ \sin(\theta+\psi) & \cos(\theta+\psi) \end{pmatrix}.$$

L'identité n'est rien d'autre que la formule d'addition des angles pour les fonctions sinus et cosinus. Si $z = a + bi = r(\cos\theta + i\sin\theta)$, posons

$$M(z) = \begin{pmatrix} a & -b \\ b & a, \end{pmatrix} = \begin{pmatrix} r\cos\theta & -r\sin\theta \\ r\sin\theta & r\cos\theta \end{pmatrix}.$$

Alors on a $M(zw) = M(z)M(w)$. Les matrices de la forme $M(z)$ pour $z \neq 0$ représentent les similitudes directes du plan. Noter que l'on a aussi $M(z+w) = M(z) + M(w)$.

Euler (1707-1783) est un calculateur audacieux. Il substitue des nombres complexes dans les séries de Taylor des fonctions exponentielles et trigonométriques. Ces séries avaient déjà été obtenues par Newton:

$$\begin{aligned} e^x &= 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \frac{x^5}{5!} + \cdots \\ \sin x &= x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \frac{x^9}{9!} + \cdots \\ \cos x &= 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \frac{x^8}{8!} + \cdots \end{aligned}$$

Si on met $x = i\theta$ dans le développement de e^x on obtient

$$\begin{aligned} e^{i\theta} &= 1 + i\theta + \frac{(i\theta)^2}{2!} + \frac{(i\theta)^3}{3!} + \frac{(i\theta)^4}{4!} + \frac{(i\theta)^5}{5!} + \frac{(i\theta)^6}{6!} + \frac{(i\theta)^7}{7!} + \frac{(i\theta)^8}{8!} + \cdots \\ &= 1 + i\theta - \frac{\theta^2}{2!} - \frac{i\theta^3}{3!} + \frac{\theta^4}{4!} + \frac{i\theta^5}{5!} - \frac{\theta^6}{6!} - \frac{i\theta^7}{7!} + \frac{\theta^8}{8!} + \frac{i\theta^9}{9!} + \cdots \\ &= \Big(1 - \frac{\theta^2}{2!} + \frac{\theta^4}{4!} - \frac{\theta^6}{6!} + \frac{\theta^8}{8!} + \cdots\Big) + i\Big(\theta - \frac{\theta^3}{3!} + \frac{\theta^5}{5!} - \frac{\theta^7}{7!} + \frac{\theta^9}{9!} + \cdots\Big) \\ &= \cos\theta + i\sin\theta \end{aligned}$$

Nous avons obtenu la *formule d'Euler*:

$$e^{i\theta} = \cos\theta + i\sin\theta$$

En particulier,

$$e^{2\pi i} = 1, \quad e^{\pi i} = -1 \quad \text{et} \quad e^{\frac{\pi}{2}i} = i.$$

La formule

$$e^{i\pi} + 1 = 0$$

semble témoigner d'une harmonie profonde. Il est étonnant de retrouver réunie dans une formule simple, les constantes fondamentales des mathématiques.

Avec la formule d'Euler, la formule de De Moivre devient

$$e^{\theta i} e^{\psi i} = e^{(\theta+\psi)i}.$$

Les racines n-ième de l'unité peuvent maintenant s'écrire sous la forme $e^{\frac{2k\pi i}{n}}$ pour $0 \leq k < n$.

Si on rempace θ par $-\theta$ dans la formule d'Euler on trouve

$$e^{-i\theta} = \cos\theta - i\sin\theta.$$

En combinant cette formule avec la formule $e^{i\theta} = \cos\theta + i\sin\theta$ on obtient que

$$\cos\theta = \frac{e^{i\theta} + e^{-i\theta}}{2} \quad \text{et} \quad \sin\theta = \frac{e^{i\theta} - e^{-i\theta}}{2i}.$$

Théorème . *(Théorème Fondamental de l'Algèbre) Tout polynôme à coefficients complexes de degré $n \geq 1$ possède au moins une racine complexe.*

La démonstration de ce théorème est le sujet de la thèse de doctorat de Gauss en 1799. Mais la démonstration de Gauss était lacunaire. C'est sans doute pourquoi il en fournira trois autres durant sa vie. Nous admettrons le théorème sans démonstration.

Le théorème fondamental de l'algèbre est un résultat miraculeux. N'est-il pas surprenant qu'il suffise d'ajouter le nombre i, c'est-à-dire la racine du *seul* polynôme $x^2 + 1$, pour donner une racine à tous les polynômes ?

Exercices

Exercice 1: Montrer que tout nombre complexe est la racine d'un polynôme du second degré à coefficients réels. *Suggestion*: Considerer $(x - z)(x - \bar{z})$.

Exercice 2: Montrer que le conjugué d'une racine d'un polynôme $p(x)$ à coefficients réels, est encore une racine de $p(x)$.

Exercice 3: Montrer qu'un polynôme à coefficients réels possède un nombre pair de racines complexes non réelles.

Exercice 4: Utiliser la relation $e^{\theta i}e^{\psi i} = e^{(\theta+\psi)i}$ pour établir les identités

$$\begin{aligned}\cos(\theta + \psi) &= \cos\theta\cos\psi - \sin\theta\sin\psi,\\ \sin(\theta + \psi) &= \cos\theta\sin\psi + \sin\theta\cos\psi.\end{aligned}$$

En déduire les identités

$$\begin{aligned}\cos(\theta - \psi) &= \cos\theta\cos\psi + \sin\theta\sin\psi\\ \sin(\theta - \psi) &= -\cos\theta\sin\psi + \sin\theta\cos\psi\,.\end{aligned}$$

$$\begin{aligned}\cos\theta\cos\psi &= \frac{1}{2}\big(\cos(\theta + \psi) + \cos(\theta - \psi)\big),\\ \sin\theta\sin\psi &= \frac{1}{2}\big(\cos(\theta - \psi) - \cos(\theta + \psi)\big),\\ \sin\theta\cos\psi &= \frac{1}{2}\big(\sin(\theta + \psi) + \sin(\theta - \psi)\big).\end{aligned}$$

Exercice 5: Démontrer l'identité

$$\tan(\theta + \psi) = \frac{\tan\theta + \tan\psi}{1 - \tan\theta\tan\psi}$$

Exercice 6: Montrer que la relation $e^{i(\theta+\pi)} = e^{i\theta}e^{\pi i}$ équivaut aux relations $\cos(\theta+\pi) = -\cos\theta$ et $\sin(\theta+\pi) = -\sin\theta$. Montrer que la relation $e^{i(\theta+\frac{\pi}{2})} = e^{i\theta}e^{\frac{i\pi}{2}}$ équivaut aux relations $\cos(\theta+\frac{\pi}{2}) = -\sin\theta$ et $\sin(\theta+\frac{\pi}{2}) = \cos\theta$.

Exercice 7: Si $z = a+bi$ alors on a $b+ia = i\bar{z}$. En déduire que $\cos(\frac{\pi}{2}-\theta) = \sin\theta$ et que $\sin(\frac{\pi}{2}-\theta) = \cos\theta$.

Exercice 8: Utiliser les relations $e^{2\theta i} = (e^{\theta i})^2$ et $\cos^2\theta + \sin^2\theta = 1$ pour montrer que

$$\cos 2\theta = \cos^2\theta - \sin^2\theta = 2\cos^2\theta - 1$$
$$\sin 2\theta = 2\cos\theta\sin\theta$$
$$\tan\frac{\theta}{2} = \frac{\sin\theta}{1+\cos\theta} = \frac{1-\cos\theta}{\sin\theta}$$

Exercice 9: Utiliser l'exercice précédent pour montrer que si $t = \tan\frac{\theta}{2}$ alors

$$\cos\theta = \frac{1-t^2}{1+t^2} \quad \text{et} \quad \sin\theta = \frac{2t}{1+t^2}$$

Exercice 10: Montrer que l'argument θ d'un nombre complexe non nul $z = a+bi$ est donné par la formule

$$\theta = 2\arctan\frac{b}{r+a}$$

où $r = \mid z \mid$.

Exercice 11: Utiliser l'identité $\mid z^2 \mid^2 = (\mid z \mid^2)^2$ pour obtenir la relation de Platon

$$(a^2-b^2)^2 + (2ab)^2 = (a^2+b^2)^2.$$

Exercice 12: Utiliser l'identité $\mid zw \mid^2 = \mid z \mid^2 \mid w \mid^2$ pour obtenir la généralisation suivante de la relation de Platon

$$(ac \pm bd)^2 + (ad \mp bc)^2 = (a^2+b^2)(c^2+d^2)$$

Dans son *Arithmetica*, Diophante étudie les représentations d'un entier comme somme de deux carrés. Par exemple, $5 = 1^2+2^2$ et $13 = 2^2+3^2$. Il fait l'observation suivante: *"C'est de la nature de 65 de pouvoir s'exprimer comme somme de deux carrés de deux manières différentes, 16+49 et 64+1; la raison se trouve dans la factorisation* $65 = 5\cdot 13$ *car les facteurs sont eux-mêmes sommes de deux carrés".*

Exercice 13: Utiliser l'exercice précédent pour expliquer l'affirmation de Diophante.

Exercice 14: Montrer que l'on a $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$ et $\sin 3\theta = -4\sin^3\theta + 3\sin\theta$.

Pour chaque entier $n \geq 1$, on définit le *polynômes de Chebyshev* $T_n(x)$ comme un polynôme de degré n pour lequel on a identiquement

$$\cos(n\theta) = T_n(\cos\theta)$$

Par exemple, on a $\cos(2\theta) = 2\cos^2\theta - 1$, ce qui signifie que $T_2(x) = 2x^2 - 1$.

Exercice 15 : Montrer que

$$\begin{aligned}
T_1(x) =& x \\
T_2(x) =& 2x^2 - 1 \\
T_3(x) =& 4x^3 - 3x \\
T_4(x) =& 8x^4 - 8x^2 + 1 \\
T_5(x) =& 16x^5 - 20x^3 + 5x \\
T_6(x) =& 32x^6 - 48x^4 + 18x^2 - 1
\end{aligned}$$

Le problème de la division d'un angle θ en trois consiste à trouver une construction géométrique de $\theta/3$ à partir d'un angle θ. Du point de vue algébrique, cela consiste à exprimer $\sin(\theta/3)$ ou $\cos(\theta/3)$ à partir de $\sin\theta$ ou $\cos\theta$.

Exercice 16: Montrer que si $p = \cos\theta$ alors on peut obtenir $x = \cos\frac{\theta}{3}$ en résolvant l'équation du troisième degré

$$4x^3 - 3x = p.$$

Utiliser la formule de Cardan pour exprimer x en fonction de p. Que pensez-vous du résultat?

Les exercices qui suivent ont pour but de calculer explicitement certaines racines de l'unité.

Exercice 17: Si $0 \leq \theta \leq \pi$, montrer que

$$\cos\frac{\theta}{2} = \sqrt{\frac{1+\cos\theta}{2}} \qquad \sin\frac{\theta}{2} = \sqrt{\frac{1-\cos\theta}{2}}.$$

Exercice 18 : Montrer que l'on a

$$\begin{aligned}
e^{\frac{\pi i}{4}} &= \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2} \\
e^{\frac{\pi i}{8}} &= \frac{\sqrt{2+\sqrt{2}}}{2} + i\frac{\sqrt{2-\sqrt{2}}}{2} \\
e^{\frac{\pi i}{16}} &= \frac{\sqrt{2+\sqrt{2+\sqrt{2}}}}{2} + i\frac{\sqrt{2-\sqrt{2+\sqrt{2}}}}{2} \\
e^{\frac{\pi i}{32}} &= \frac{\sqrt{2+\sqrt{2+\sqrt{2+\sqrt{2}}}}}{2} + i\frac{\sqrt{2-\sqrt{2+\sqrt{2+\sqrt{2}}}}}{2} \\
e^{\frac{\pi i}{64}} &= \frac{\sqrt{2+\sqrt{2+\sqrt{2+\sqrt{2+\sqrt{2}}}}}}{2} + i\frac{\sqrt{2-\sqrt{2+\sqrt{2+\sqrt{2+\sqrt{2}}}}}}{2}
\end{aligned}$$

Exercice 19: Montrer que l'on a

$$e^{\frac{\pi i}{4}} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2} \qquad e^{\frac{3\pi i}{4}} = \frac{-\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$$

$$e^{\frac{5\pi i}{4}} = \frac{-\sqrt{2}}{2} - i\frac{\sqrt{2}}{2} \quad \text{et} \quad e^{\frac{7\pi i}{4}} = \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}$$

Exercice 20: Montrer que l'on a

$$\tan\frac{\pi}{8} = \sqrt{2} - 1 \qquad \tan\frac{3\pi}{8} = \sqrt{2} + 1$$

Suggestion: Utiliser l'identité $\tan\frac{\theta}{2} = \frac{\sin\theta}{1+\cos\theta}$.

Exercice 21: Si $0 \leq \psi \leq \pi$, montrer que

$$2\cos\Big(\frac{\pi}{2} \pm \frac{\psi}{2}\Big) = \mp\sqrt{2 - 2\cos\psi}.$$

En déduire que

$$2\cos\Big(\frac{\pi}{2} \pm \frac{1}{2}(\frac{\pi}{2} \pm \frac{\psi}{2})\Big) = \mp\sqrt{2 \pm \sqrt{2 - 2\cos\psi}}.$$

Exercice 22: Montrer que l'on a

$$e^{\frac{\pi i}{8}} = \frac{\sqrt{2+\sqrt{2}}}{2} + i\frac{\sqrt{2-\sqrt{2}}}{2} \qquad e^{\frac{3\pi i}{8}} = \frac{\sqrt{2-\sqrt{2}}}{2} + i\frac{\sqrt{2+\sqrt{2}}}{2}$$

$$e^{\frac{5\pi i}{8}} = \frac{-\sqrt{2-\sqrt{2}}}{2} + i\frac{\sqrt{2+\sqrt{2}}}{2} \qquad e^{\frac{7\pi i}{8}} = \frac{-\sqrt{2+\sqrt{2}}}{2} + i\frac{\sqrt{2-\sqrt{2}}}{2}$$

$$e^{\frac{9\pi i}{8}} = \frac{-\sqrt{2+\sqrt{2}}}{2} - i\frac{\sqrt{2-\sqrt{2}}}{2} \qquad e^{\frac{11\pi}{8}} = \frac{-\sqrt{2-\sqrt{2}}}{2} - i\frac{\sqrt{2+\sqrt{2}}}{2}$$

$$e^{\frac{13\pi i}{8}} = \frac{\sqrt{2-\sqrt{2}}}{2} - i\frac{\sqrt{2+\sqrt{2}}}{2} \qquad e^{\frac{15\pi i}{8}} = \frac{\sqrt{2+\sqrt{2}}}{2} - i\frac{\sqrt{2-\sqrt{2}}}{2}$$

Exercice 23: Si $0 \leq \psi \leq \pi$, montrer que

$$2\cos\left(\frac{\pi}{2} \pm \frac{1}{2}\Big(\frac{\pi}{2} \pm \frac{1}{2}(\frac{\pi}{2} \pm \frac{\psi}{2})\Big)\right) = \mp\sqrt{2 \pm \sqrt{2 \pm \sqrt{2 - 2\cos\psi}}}.$$

Exercice 24: Montrer que l'on a

$$e^{\frac{\pi i}{16}} = \frac{\sqrt{2+\sqrt{2+\sqrt{2}}}}{2} + i\frac{\sqrt{2-\sqrt{2+\sqrt{2}}}}{2}$$

$$e^{\frac{3\pi i}{16}} = \frac{\sqrt{2+\sqrt{2-\sqrt{2}}}}{2} + i\frac{\sqrt{2-\sqrt{2-\sqrt{2}}}}{2}$$

$$e^{\frac{5\pi i}{16}} = \frac{\sqrt{2-\sqrt{2-\sqrt{2}}}}{2} + i\frac{\sqrt{2+\sqrt{2-\sqrt{2}}}}{2}$$

$$e^{\frac{7\pi i}{16}} = \frac{\sqrt{2-\sqrt{2+\sqrt{2}}}}{2} + i\frac{\sqrt{2+\sqrt{2+\sqrt{2}}}}{2}$$

Exercice 25: Montrer que tout nombre impair $0 < a < 2^n$ peut s'exprimer comme une somme

$$\frac{a}{2^n} = \frac{1}{2} \pm \frac{1}{4} \pm \frac{1}{8} \pm \cdots \pm \frac{1}{2^{n-1}} \pm \frac{1}{2^n}$$

pour une suite bien déterminée de signes $\pm$. En déduire que l'on a

$$\frac{a}{2^n} = \frac{1}{2} \pm \left(\frac{1}{4} \pm \left(\frac{1}{8} \pm \left(\cdots \pm \left(\frac{1}{2^{n-1}} \pm \frac{1}{2^n}\right)\right)\cdots\right)\right)$$

pour une autre suite bien déterminée de signes $\pm$.

Exercice 26: Montrer que si on a

$$\frac{a}{2^n} = \frac{1}{2} \pm \left(\frac{1}{4} \pm \left(\frac{1}{8} \pm \left(\cdots \pm \left(\frac{1}{2^{n-1}} \pm \frac{1}{2^n}\right)\right)\cdots\right)\right)$$

pour une suite déterminée de signes $\pm$, alors on a

$$2\cos\theta = \quad \mp\sqrt{2 \pm \sqrt{2 \pm \sqrt{\cdots \pm \sqrt{2 \pm \sqrt{2}}}}}$$

pour la même suite de signes sauf pour le premier.

Exercice 27: Utiliser la factorisation $x^3 - 1 = (x-1)(x^2+x+1)$ pour montrer que l'on a

$$e^{\frac{2\pi i}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2} \quad \text{et} \quad e^{\frac{4\pi i}{3}} = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$$

Exercice 28: Montrer que

$$e^{\frac{\pi i}{3}} = -e^{\frac{4\pi i}{3}} = \frac{1}{2} + \frac{\sqrt{3}}{2}i, \qquad \text{et} \quad e^{\frac{\pi i}{6}} = -ie^{\frac{2\pi i}{3}} = \frac{\sqrt{3}}{2} + \frac{1}{2}i.$$

Exercice 29: Montrer que

$$\tan\frac{\pi}{3} = \sqrt{3}, \qquad \tan\frac{\pi}{6} = \frac{1}{\sqrt{3}}, \qquad \tan\frac{\pi}{12} = 2-\sqrt{3} \quad \text{et} \quad \tan\frac{5\pi}{12} = 2+\sqrt{3}.$$

L'exercice suivant a pour but de calculer les racines 5-ièmes de l'unité en utilisant la factorisation

$$x^5 - 1 = (x-1)(x^4+x^3+x^2+x+1)$$

Le *nombre d'or* $\beta = \frac{1+\sqrt{5}}{2}$ est par définition la solution positive de l'équation $\beta^2 - \beta - 1 = 0$, l'autre racine étant $\beta' = 1 - \beta$.

Exercice 30: Vérifier que l'on a

$$x^4 + x^3 + x^2 + x + 1 = (x^2 + \beta x + 1)(x^2 + \beta' x + 1).$$

Montrer que le polynome $x^2 + \beta' x + 1$ a pour racines

$$e^{\frac{2\pi i}{5}} = \frac{\sqrt{5}-1}{4} + i\sqrt{\frac{5+\sqrt{5}}{8}} \quad \text{et} \quad e^{\frac{8\pi i}{5}} = \frac{\sqrt{5}-1}{4} - i\sqrt{\frac{5+\sqrt{5}}{8}},$$

et que le polynôme $x^2 + \beta x + 1$ a pour racines

$$e^{\frac{4\pi i}{5}} = \frac{-\sqrt{5}-1}{4} + i\sqrt{\frac{5-\sqrt{5}}{8}} \quad \text{et} \quad e^{\frac{6\pi i}{5}} = \frac{-\sqrt{5}-1}{4} - i\sqrt{\frac{5-\sqrt{5}}{8}}.$$

Exercice 31: Montrer que

$$e^{\frac{\pi i}{5}} = -e^{\frac{-4\pi i}{5}} = \frac{\sqrt{5}+1}{4} + i\sqrt{\frac{5-\sqrt{5}}{8}} \quad \text{et} \qquad e^{\frac{\pi i}{10}} = ie^{\frac{-2\pi i}{5}} = \sqrt{\frac{5+\sqrt{5}}{8}} + i\frac{\sqrt{5}-1}{4}$$

L'exercice 31 montre que $\beta = 2\cos(\pi/5)$.

Les exercices qui suivent ont pour but de montrer que si un entier n a une décomposition en facteurs premiers de la forme $2^k \cdot 3 \cdot 5$, alors on peut exprimer les racine n-ième de l'unité au moyen de racines carrés. Gauss a montré plus généralement que c'est le cas pour les entiers n pour lesques $\phi(n)$ est une puissance de 2.

Exercice 32: Soit u une racine n-ième de l'unité. Montrer si $a \equiv b \bmod n$ alors $u^a = u^b$.

Exercice 33 : Soit u une racine n-ième de l'unité. Montrer si $a \equiv b \bmod n$ alors $u^a = u^b$. Soient m et n des entiers > 0 relativement premiers. Montrer qu'il existe des entiers a et b tels que l'on ait

$$\frac{a}{m} + \frac{b}{n} = \frac{1}{mn}$$

Si $u = e^{\frac{2\pi i}{m}}$ et $v = e^{\frac{2\pi i}{n}}$ montrer que $u^a v^b = e^{\frac{2\pi i}{mn}}$.

Exercice 34: Montrer que

$$e^{\frac{\pi i}{12}} = \frac{\sqrt{2}}{4}(\sqrt{3}+1) + i\frac{\sqrt{2}}{4}(\sqrt{3}-1).$$

Exercice 35: Montrer que

$$e^{\frac{\pi i}{20}} = \left(\frac{\sqrt{5}+1}{4\sqrt{2}} + \frac{\sqrt{5-\sqrt{5}}}{4}\right) + i\left(\frac{\sqrt{5}+1}{4\sqrt{2}} - \frac{\sqrt{5-\sqrt{5}}}{4}\right)$$

Exercice 36: L'astronome grec Claude Ptolémée (150 après JC) calcula le côté d'un polygône régulier de 120 côtés. Pourriez-vous répéter son exploit? *Suggestion:* On a $120 = 8 \cdot 5 \cdot 3$. Utiliser le fait que

$$\frac{1}{3} - \frac{1}{8} - \frac{1}{5} = \frac{1}{120}.$$

2. Arithmétique des polynômes

Dans cette partie, K désigne un corps commutatif quelconque. Les pricipaux exemples sont le corps $\mathbf{Q}$ des nombres rationnels, le corps $\mathbf{R}$ des nombres réels et le corps $\mathbf{C}$ des nombres complexes. Nous considérerons aussi les corps finis $\mathbf{Z}_p$ pour p un nombre premier.

Un polynôme

$$p = p(X) = \sum_{i=0}^{n} a_i X^i = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$$

est connu si on connait la suite $(a_0, a_1, \ldots, a_n)$ de ses coefficients. C'est la conception originale des mathématiciens arabes. Si $a_i \in K$ nous dirons que p est un polynôme à coefficients dans K. Il sera plus commode de définir un polynôme de degré $\leq n$ comme une suite infinie d'éléments de K, $a_0, a_1, a_2, \ldots$ avec la condition que $a_i = 0$ si $i > n$. On peut alors écrire

$$p = \sum_{i \geq 0} a_i X^i$$

Le polynôme est *nul* si $a_i = 0$ pour tout $i \geq 0$. Sinon, le plus grand entier i pour lequel $a_i \neq 0$ est le *degré* n de p, $n = \deg(p)$. Bien que le degré du polynôme nul ne soit pas défini nous inclurons le polynôme nul parmi les polynômes de degré est $\leq n$ queque soit $n \geq 0$. Les polynômes de degré ≤ 0 sont les *polynômes constants*. On définit la somme et le produit de deux polynômes

$$p = \sum_{i \geq 0} a_i X^i \quad \text{et} \quad q = \sum_{i \geq 0} b_i X^i$$

en posant

$$p + q = \sum_{i \geq 0} (a_i + b_i) X^i$$

et

$$pq = \sum_{k \geq 0} \Big(\sum_{i+j=k} a_i b_j \Big) X^k .$$

Si p est (non-nul) de degré m et q (non-nul) de degré n, le terme $a_j b_j$ de la somme

$$\sum_{i+j=k} a_i b_j = a_0 b_k + a_1 b_{k-1} + \cdots + a_{k-1} b_1 + a_k b_0$$

est nul pour $i > m$ ou $j > n$. En particulier, on a $c_{m+n} = a_m b_n$ et $c_k = 0$ pour $k > m + n$. On voit que pq est (non-nul) de degré $m + n$. De plus, le coefficient dominant de pq est le produit des coefficients dominants de p et de q.

Nous dénoterons par $K[X]$ l'ensemble des polynômes à coefficients dans K. On vérifie facilement que $K[X]$ est un anneau. La *valeur* d'un polynôme $p(X) = a_0 + a_1 X + \cdots + a_n X^n$ en $z \in K$ s'obtient en posant

$$p(z) = a_0 + a_1 z + \cdots + a_n z^n.$$

On voit facilement que si $p(X) = a(X)b(X)$ alors $p(z) = a(z)b(z)$ et que si $p(X) = a(X) + b(X)$, alors $p(z) = a(z) + b(z)$. Si $p(z) = 0$ on dit que z est une *racine* de $p(X)$.

Definition 1: Nous dirons qu'un polynôme $a \in K[X]$ *divise* un polynôme $b \in K[X]$ s'il existe un polynôme $q \in K[X]$ tel que $b = aq$. Nous écrirons $a \mid b$ pour indiquer que a divise b.

Exercice : Montrer que si $0 \mid a$ alors $a = 0$.

Proposition 2.
(i) On a $p \mid pq$. En particulier, $p \mid 0$, $1 \mid p$ et $p \mid p$;
(ii) si $p \mid q$ et $q \mid r$ alors $p \mid r$.
(iii) si $p \mid a$ et $p \mid b$ alors $p \mid (a \pm b)$.

Si deux polynômes non nuls $p(X)$ et $q(X)$ se divisent mutuellement, alors on a $p(X) = c \cdot q(X)$ pour une constante non-nulle $c \in K$.

Définition : Nous dirons que des polynômes non nuls $p, q \in K[X]$ sont *associés* s'ils se divisent mutuellement. Nous écrirons $p \sim q$ pour indiquer que p et q sont associés.

Tout polynome non nul est associé à un polynome unitaire et un seul.

Théorème . *(Division euclidienne) Soit $p \in K[X]$ un polynôme non nul de degré $n > 0$. Alors pour tout polynôme $a \in K[X]$ il existe des polynômes q et $r \in K[X]$ tels que l'on ait $a = pq + r$ avec r un polynôme de degré $< n$. De plus, les polynômes q et r sont déterminés uniquement.*

Preuve: Démontrons d'abord l'existence de $q(X)$ et $r(X)$. Le résultat est trivial si $a = a(X)$ est de degré $< n$ car dans ce cas on peut prendre $q(X) = 0$ et $r(X) = a(X)$. Pour le reste nous allons supposer que $a(X)$ est non-nul de degré $m \geq n$. Nous allons raisonner par induction sur m. Soit a_m le coefficient dominant de $a(X)$ et b_n le coeficient dominant de $p(X)$. Le degré du polynôme $b_n^{-1}p(X)a_mX^{m-n}$ est m et son coefficient dominant est a_m. Le polynôme

$$f(X) = a(X) - b_n^{-1}p(X)a_mX^{m-n}.$$

est de degré $< m$. On peut supposer par l'hypothèse d'induction que l'on a $f(X) = p(X)g(X) + r(X)$ avec $r(X)$ un polynôme de degré $< n$. Si on pose $q(X) = g(X) + b_n^{-1}a_mX^{m-n}$ on obtient que

$$a(X) = p(X)q(X) + r(X).$$

L'existence de $q(X)$ et de $r(X)$ est démontré. Démontrons l'unicité. Supposons que l'on ait

$$a(X) = p(X)u(X) + v(X)$$

avec $u(X)$ un polynôme de degré $< n$. Comme $a(X) = p(X)q(X) + r(X)$ on obtient par soustraction que

$$p(X)\big(q(X) - u(X)\big) = v(X) - r(X).$$

Si le polynôme $q(X) - v(X)$ était non nul, le degré du membre de gauche serait $\geq n$ car $\deg(p(X)) = n$. C'est absurde car le degré du membre de droite est $< n$. Donc, $q(X) - u(X) = 0$ et par suite $v(X) - r(X) = 0$. CQFD

On dit que que r est le *reste* de la division euclidienne de a par p et que q est le *quotient*. Le reste est nul ssi p divise a.

Par exemple, divisons le polynôme $a(X) = 2X^5+3X^3-X^2+X-1$ par le polynôme $p(X) = X^2+2X+1$. On obtient successivement

$$\begin{aligned}
&2X^5 + 3X^3 - X^2 + X - 1 = (X^2 + 2X + 1)(2X^3) - 4X^4 + X^3 - X^2 + X - 1\\
&-4X^4 + X^3 - X^2 + X - 1 = (X^2 + 2X + 1)(-4X^2) = 9X^3 + 3X^2 + X - 1\\
&9X^3 + 3X^2 + X - 1 = (X^2 + 2X + 1)(9X) - 15X^2 - 8X - 1\\
&-15X^2 - 8X - 1 = (X^2 + 2X + 1)(-15) = 22X + 14
\end{aligned}$$

Cela donne $q(X) = 2X^3 - 4X^2 + 9X - 15$ et $r(X) = 22X + 14$.

Proposition . *Le reste de la division d'un polynôme $p(X) \in K[X]$ par un polynôme $X - z$ est égal à $p(z)$. En particulier, $p(X)$ est divisible par $X - z$ ssi z est une racine de $p(X)$.*

Preuve: Par division euclidienne, on a $p(X) = (X - z)q(X) + r(X)$ avec $r(X)$ un polynôme de degré < 1. Donc $r(X) = r \in K$. En substituant $X = z$ dans l'égalité $p(X) = (X - z)q(X) + r$ on obtient que $p(z) = r$. CQFD

Proposition . *Soit $p(X) \in K[X]$ un polynôme s'annulant en n éléments distincts $z_1, \cdots, z_n \in K$. Alors $p(X)$ est divisible par le produit $(X - z_1) \cdots (X - z_n)$.*

Preuve: Raisonnons par induction sur n. On a une factorisation $p(X) = (X - z_n)q(X)$ puisque z_n est une racine de $p(X)$. Si $i < n$ on a $p(z_i) = (z_i - z_n)q(z_i) = 0$ et donc $q(z_i) = 0$ car $z_i - z_n \neq 0$. Par l'hypothèse de récurrence, on peut supposer que $q(X)$ est divisible par le produit $(X - z_1) \cdots (X - z_{n-1})$. Cela entraîne que $p(X) = (X - z_n)q(X)$ est divisible par le produit $(X - z_1) \cdots (X - z_{n-1})(X - z_n)$. CQFD

Proposition. *(Lagrange) Soient $z_1, z_2, \ldots, z_n$ des éléments distincts de K. Alors pour tout élements $y_1, y_2, \ldots, y_n \in K$ il existe un et un seul polynôme $p(X) \in K[X]$ de degré $< n$ tel que l'on ait $p(z_i) = y_i$ pour tout $1 \leq i \leq n$. De plus, on a*

$$p(X) = y_1 \frac{p_1(X)}{p_1(z_1)} + \cdots + y_n \frac{p_n(X)}{p_n(z_n)}$$

ou l'on a posé

$$p_k(X) = (X - z_1) \cdots (X - z_{k-1})(X - z_{k+1}) \cdots (X - z_n)$$

Preuve: Démontrons d'abord l'existence de $p(X)$. Posons

$$p(X) = y_1 \frac{p_1(X)}{p_1(z_1)} + \cdots + y_n \frac{p_n(X)}{p_n(z_n)}$$

Il suit de la définition de $p_k(X)$ que l'on a $p_k(z_i) = 0$ pour $i \neq k$. Par suite,

$$p(z_i) = y_1 \frac{p_1(z_i)}{p_1(z_1)} + \cdots + y_n \frac{p_n(z_i)}{p_n(z_n)} = y_i \frac{p_i(z_i)}{p_i(z_i)} = y_i.$$

Démontrons l'unicité. Soit $q(X)$ un polynôme de degré $< n$ tel que l'on ait $q(z_i) = y_i$ pour tout $1 \leq i \leq n$. Le polynôme $p(X) - q(X)$ s'annulle en $X = z_i$ pour $1 \leq i \leq n$. Il est donc divisible par le produit $(X - z_1) \cdots (X - z_n)$. Comme ce produit est de degré n et que $p(X) - q(X)$ est de degré $< n$ on a $p(X) - q(X) = 0$. CQFD

On dit que la formule

$$p(X) = y_1 \frac{p_1(X)}{p_1(z_1)} + \cdots + y_n \frac{p_n(X)}{p_n(z_n)}$$

est la *formule d'interpolation de Lagrange*. Si $n = 2$, on a

$$p(X) = y_1 \frac{X - z_2}{z_1 - z_2} + y_2 \frac{X - z_1}{z_2 - z_1}$$

Si $n = 3$, on a

$$p(X) = y_1 \frac{(X - z_2)(X - z_3)}{(z_1 - z_2)(z_1 - z_3)} + y_2 \frac{(X - z_1)(X - z_3)}{(z_2 - z_1)(z_2 - z_3)} + y_3 \frac{(X - z_1)(X - z_2)}{(z_3 - z_1)(z_3 - z_2)}$$

Définition : Soient $a, b \in K[X]$ des polynômes non nuls. Nous dirons qu'un polynôme p est un *plus grand diviseur commun* de a et de b si p divise a et b et si tout polynôme qui divise a et b est divisible par p. Nous dirons que a et b sont *relativement premiers* si tout diviseur commun de a et b est constant.

Les plus grands diviseurs communs de a et b sont associés car ils se divisent mutuellement.

Lemme . *Soit r le reste de la division euclidienne d'un polynôme a par un polynôme non nul p. Alors tout diviseur commun de a et p est un diviseur commun de p et r.*

Preuve: On a $a = pq + r$. Si un polynôme d divise a et p alors il divise $r = a - pq$. Réciproquement, si d divise p et r alors il divise $a = pq + r$. CQFD

Théorème . *Toute paire de polynômes non nuls $a, b \in K[X]$ possède un plus grand diviseur commun d. De plus, il existe des polynômes $u, v \in K[X]$ tels que $d = ua + vb$.*

Preuve: C'est une conséquence de la divison euclidienne. La démonstration est semblable à celle de ?. On effectue les divisions euclidiennes suivantes jusqu'à l'obtention d'un reste nul:

$$\begin{aligned}
a &= bq_1 + r_1 \quad \text{avec} \quad \deg(r_1) < \deg(b) \\
b &= r_1 q_2 + r_2 \quad \text{avec} \quad \deg(r_2) < \deg(r_1) \\
r_1 &= r_2 q_3 + r_3 \quad \text{avec} \quad \deg(r_3) < \deg(r_2) \\
&\cdots \qquad\qquad\qquad\quad \cdots \\
r_{n-2} &= r_{n-1} q_n + r_n \quad \text{avec} \quad \deg(r_n) < \deg(r_{n-1}) \\
r_{n-1} &= r_n q_{n+1} + 0
\end{aligned}$$

Il suit du lemme que tout diviseur commun de a et b est un diviseur de r_n et réciproquement. Cela montre que $d = r_n$ est un plus grand diviseur commun de a et de b. Il reste à montrer qu'il existe des polynômes $u, v \in K[X]$ tels que $d = ua + vb$. On peut raisonner par induction sur le degré de b. Comme d est un plus grand diviseurs commun de b et de r_1, il existe des polynômes $u, v \in K[X]$ tels que $d = u_1 b + v_1 r_1$. Comme $r_1 = a - bq_1$ on obtient que $d = u_1 b + v_1(a - bq_1) = v_1 a + (u_1 - v_1 q_1)b$, ce qui donne le résultat.

Le théorème ? a de nombreuses conséquences. Le résultats suivants se démontrent comme les résultats corespondants pour les entiers.

Proposition . *Deux polynômes non nuls $a, b \in K[X]$ sont relativement premiers si et seulement si il existe des polynômes $u, v \in K[X]$ tels que $1 = ua + vb$.*

Proposition . *Le produit de deux polynômes relativement premiers à un polynôme donné est relativement premier à ce polynôme.*

Definition: Nous dirons qu'un polynôme p de degré $n > 0$ à coefficients dans K est *factorisable* si l'on a $p = ab$ pour des polynômes $a, b \in K[X]$ de degré $< n$. Si p n'est pas factorisable nous dirons qu'il est *irréductible*.

Les notions de polynôme factorisable et de polynôme irréductible sont relatives au corps des coefficients K. Par exemple, le polynôme x^2+1 est irréductible en tant que polynôme à coefficients réels mais factorisable en tant que polynôme à coefficients complexes car $x^2+1=(x-i)(x+i)$. Tout polynôme de degré 1 est irréductible. Tout polynôme factorisable de degré $n>0$ possède un diviseur de degré $\leq n/2$. Un polynôme non nul $p(X)\in K[X]$ est divisible par un polynôme de degré 1 si et seulement si $p(X)$ possède une racine dans K. En particulier, un polynôme $p(X)$ de degré 2 ou 3 qui n'a pas de racines dans K est irréductible. Par exemple, les polynômes X^2-2 et X^3-2 sont irréductibles en tant que polynôme à coefficients rationnels.

Proposition . *Les polynômes unitaires irréductibles à coefficient complexes sont de la forme $X-z$ pour $z\in\mathbf{C}$.*

Preuve: Tout polynôme $p(X)\in\mathbf{C}[X]$ de degré >0 possède une racine $z\in\mathbf{C}$ d'après le théorème fondamental de l'algèbre. Il est donc divisible par $X-z$ par ?. Si p est irréductible on a $p(X)=c(X-z)$. Et si p est unitaire on a $p(X)=X-z$. CQFD

Proposition . *Les polynômes unitaires irréductibles à coefficient réels sont de deux formes:*
(i) les polynômes $X-a$ pour $a\in\mathbf{R}$;
(ii) les polynômes X^2+aX+b pour $a,b\in\mathbf{R}$ avec $a^2-4b<0$.

Preuve: Le polynôme $X-a$ est évidemment irréductible. Si $a^2-4b<0$, le polynôme X^2+aX+b n'a pas de racines réelles; il est donc irréductible. Inversement, montrons que tout polynôme unitaire irréductible $p(X)\in\mathbf{R}[X]$ est de la forme (i) ou (ii). C'est clair si $p(X)$ possède une racine réelle. Sinon, soit $z\in\mathbf{C}$ une racine complexe de $p(X)$. On a $\bar{z}\neq z$ puisque le nombre complexe z n'est pas réel. On a $p(\bar{z})=\overline{p(z)}$ puisque les coefficients de $p(X)$ sont réels. Donc $p(\bar{z})=0$. Le polynôme

$$(X-z)(X-\bar{z})=X^2-(z+\bar{z})X+z\bar{z}=X^2+aX+b$$

est à coefficient réels et $a^2-4b=(z-\bar{z})^2<0$ puisque $z-\bar{z}$ est purement imaginaire. Par division euclidienne, on a $p(X)=(X^2+aX+b)q(X)+r(X)$ avec $r(X)$ un polynôme de degré <2. Substituant $X=z$ et $X=\bar{z}$ dans cette égalité, on obtient que $r(z)=r(\bar{z})=0$. Comme $r(X)$ un polynôme de degré <2 et que $\bar{z}\neq z$ cela entraîne que $r(X)=0$. Nous avons montré que $p(X)$ est divisible par X^2+aX+b. Par suite, $p(X)=X^2+aX+b$ puisque $p(X)$ est irréductible et unitaire. CQFD

Lemme . *Si un polynôme irréductible $p\in K[X]$ divise le produit de deux polynômes $a,b\in K[X]$, alors il divise l'un des facteurs.*

Preuve: Montrons que si p ne divise ni a ni b alors il ne divise pas ab. En effet, si p ne divise pas a alors les seuls diviseurs communs entre p et a sont les polynômes constants. Donc a est relativement premier à p. De même, b est relativement premier à p. Le produit ab est par suite relativement premier à p par le proposition ?. CQFD

Théorème . *Tout polynôme $a\in K[X]$ de degré $n>0$ se factorise en produit de polynômes irréductibles. Cette factorisation est unique à l'ordre de facteurs associés près.*

Preuve : Pour établir l'existence, nous raisonnerons par induction sur le degré n de $a(X)$. Le résultat est trivial si $a(X)$ est irréductible. Sinon, soit $p(X)$ un diviseur de $a(X)$ dont le degré >0 est minimum. Ce diviseur est forcément irréductible car son degré est minimum. On a $a(X)=p(X)b(X)$ pour un polynome $b(X)$ degré $<n$. Le polynôme $b(X)$ est un produit de polynomes irréductibles par l'hypothèse d'induction. Donc $a(X)=p(X)b(X)$ est un produit de polynômes irréductibles. Il reste à démontrer l'unicité d'une

dćomposition de $a(X)$ en facteurs irréductibles. Pour cela on peut supposer que $a(X)$ est unitaire. Supposons que l'on ait deux factorisations en facteurs irréductibles

$$a(X) = p_1(X) \cdots p_k(X) = q_1(X) \cdots q_r(X).$$

Les produit des coefficients dominants des facteurs de chaque des factorisations vaut 1 car $a(X)$ est unitaire. En divisant par ces coefficients dominants on peut supposer que tous les polynomes irréductibles sont unitaires. En cancellant les facteurs communs aux deux factorisations on peut supposer que les factorisations n'ont pas d'éléments communs. Dans ce cas montrons que $k = r = 0$. En effet si $k > 0$ le facteur $p_1(X)$ doit diviser l'un des facteurs $q_i(X)$ d'après le lemme. On a alors $q_i(X) = c \cdot p_1(X)$ pour une constante $c \in K$ puisque $q_i(X)$ est irréductible. Les polynômes $p_1(X)$ et $q_i(X)$ sont donc associés. Par suite, $p_1(X) = q_i(X)$ puisque ces polynômes sont unitaires. Ceci contredit le fait que les factorisations n'ont pas d'éléments communs. CQFD

Proposition . *Tout polynôme unitaire $p(X) \in \mathbf{C}[X]$ de degré $n > 0$ est le produit de polynômes du premier degré:*

$$p(X) = (X - z_1)(X - z_2) \cdots (X - z_n).$$

Cette décomposition est unique à l'ordre des facteurs près.

Preuve: C'est une conséquence immédiate du théorème et de la proposition ?.

Les nombres complexes $z_1, z_2, \ldots, z_n$ qui interviennent dans la décomposition

$$p(X) = c(X - z_1)(X - z_2) \cdots (X - z_n).$$

sont le racines de $p(X)$. Un nombre complexe w peut figurer plusieurs fois dans le liste $z_1, \ldots, z_n$. Dans ce cas, on dit que w est une *racine multiple*. En regroupant entre eux les facteurs égaux on obtient une décomposition

$$p(X) = c(X - w_1)^{k_1}(X - w_2)^{k_1} \cdots (X - w_r)^{k_r}.$$

avec $w_1, \ldots, w_r$ les racines distinctes. On dit que k_i est la *multiplicité* de w_i. Remarquer que

$$k_1 + k_2 + \cdots + k_r = n.$$

Les racines du polynôme $X^n - 1$ sont les racines n-ième de l'unité $e^{\frac{2k\pi}{n}}$ pour $1 \leq k \leq n$. Comme ces racines sont distinctes et au nombre de n on a

$$X^n - 1 = \prod_{k=1}^{n} (X - e^{\frac{2k\pi}{n}}).$$

Plus généralement, les racines du polynôme $X^n - z$ sont les racines n-ième de z. On obtient une décomposition

$$X^n - z = \prod_{k=1}^{n} (X - e^{\frac{2k\pi}{n}} z^{\frac{1}{n}}).$$

Proposition . *Tout polynôme unitaire $p(X) \in \mathbf{R}[X]$ de degré $n > 0$ est le produit de polynômes du premier degré $X - a$, avec $a \in \mathbf{R}$, et de polynômes du second degré $X^2 + aX + b$, avec $a, b \in \mathbf{R}$ et $b^2 - 4a < 0$. Cette décomposition est unique à l'ordre des facteurs près.*

Preuve: C'est une conséquence immédiate du théorème et de la proposition ?.

Par exemple, si n est impair calculons la décomposition de $X^n - 1$ en facteurs réels irréductibles. Remarquer que

$$(X - e^{i\theta})(X - e^{-i\theta}) = X^2 - 2\cos\theta\, X + 1.$$

On obtient

$$X^n - 1 = (X-1)\prod_{k=1}^{\frac{n-1}{2}}(X - e^{\frac{2k\pi}{n}})(X - e^{\frac{-2k\pi}{n}}) = (X-1)\prod_{k=1}^{\frac{n-1}{2}}\Big(X^2 - 2\cos\big(\frac{2k\pi}{n}\big)X + 1\Big).$$

Par suite,

$$X^{n-1} + \cdots + X + 1 = \prod_{k=1}^{\frac{n-1}{2}}\Big(X^2 - 2\cos\big(\frac{2k\pi}{n}\big)X + 1\Big).$$

Exercices

Exercice : Montrer que

$$X^4 + X^3 + X^2 + X + 1 = \Big(X^2 - 2\sin\big(\frac{\pi}{5}\big)X + 1\Big)\Big(X^2 + 2\cos\big(\frac{\pi}{5}\big)X + 1\Big)$$

3. Polynômes cyclotomiques

On dit qu'un nombre complexe v est une *racine de l'unité* s'il existe un entier $n > 0$ tel que $v^n = 1$. Le produit de deux racines de l'unité est une racines de l'unité. L'*ordre* d'une racine de l'unité v est le plus petit entier $n > 0$ tel que $v^n = 1$. Par exemple, -1 est une racine d'orde 2 alors que i et $-i$ sont d'ordre 4. On dit qu'une racine n-ième de l'unité v est *primitive* si v est d'ordre n.

Proposition . *Soit v une racine primitive n-ième de l'unité Alors on a $v^k = 1$ ssi $n \mid k$.*

Preuve: Si $n \mid k$ alors on a $k = qn$ pour un entier q. Par suite, $u^k = u^{qe} = (a^e)^q = 1$. Inversement, supposons que l'on ait $u^k = 1$. Raisonnons par l'absurde en supposant que n ne divise pas k. Dans ce cas, on a $k = nq + r$ avec $0 < r < n$. Par suite, $1 = u^k = u^{qn+r} = (u^{nq})u^r = u^r$. C'est une contradiction car $r < n$ et u est d'ordre n. CQFD

Proposition . *Posons $u = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$. Si $k > 0$ et $d = pgdc(k,n)$ alors $u^k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$ est d'ordre n/d. En particulier u^k est une racine primitive n-ième de l'unité ssi k est relativement premier n.*

Preuve: On voit facilement que u est d'ordre n. Si k est relativement premier à n montrons que u^k est d'ordre n. En effet, on a $u^{kr} = 1$ ssi $n \mid kr$ puisque u est d'ordre n. Mais la condition $n \mid kr$ équivaut à la condition $n \mid r$ puisque n est relativement premier à k. Cela montre u^k est d'ordre n. Si $k > 0$ et $d = pgdc(k,n)$, montrons que u^k est d'ordre n/d. En effet, on a

$$u^k = \cos\frac{2(k/d)\pi}{n/d} + i\sin\frac{2(k/d)\pi}{n/d}$$

et k/d est relativement premier à n/d. Il suffit donc d'appliquer la première partie de la preuve pour conclure que u^k est d'ordre n/d. En particulier, si u^k est une racine primitive n-ième de l'unité on a $d = 1$. Cela montre que k est relativement premier à n. CQFD

Si v est une racine primitive n-ième de l'unité, alors les nombres complexes $v^1, v^2, \ldots, v^n$ sont distincts. En effet, si on avait $v^k = v^r$ avec $0 \leq k < r \leq n$ on aurait $v^{r-k} = 1$ avec $0 < r - k < n$ ce qui est absurde puisque v est d'ordre n. Comme il y en tout n racines de l'unité on en déduit que la liste de racines $v^1, v^2, \ldots, v^n$ est exaustive. On a donc

$$x^n - 1 = (x - v^0)(x - v^1)(x - v^2)\cdots(x - v^{n-1}).$$

Soit P_n l'ensemble des racines primitives n-ième de l'unité. Le nombre délément de P_n est égal à $\phi(n)$ d'après ?. Le polynôme

$$\Phi_n(x) = \prod_{u \in P_n} x - v$$

est donc de degré $\phi(n)$. On dit que c'est le n-ième *polynôme cyclotomique*. Par exemple, on a

$$\begin{aligned}
\Phi_1(x) &= x - 1 \\
\Phi_2(x) &= x + 1 \\
\Phi_3(x) &= x^2 + x + 1 \\
\Phi_4(x) &= x^2 + 1
\end{aligned}$$

Proposition . *On a*

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Preuve: Soit R_n l'ensemble des racines n-ième de l'unité. L'ordre d'un élement $v \in R_n$ est un diviseur d de n puisque $v^n = 1$. De plus, si $d \mid n$, alors l'ensemble des éléments d'ordre d de R_n est égal à P_d. Par suite,

$$x^n - 1 = \prod_{v \in R_n} (x - v) = \prod_{d|n} \prod_{v \in P_d} (x - v) = \prod_{d|n} \Phi_d(x).$$

Par exemple, si p est un nombre premier la proposition ? montre que l'on a $X^p - 1 = \Phi_p(X)\Phi_1(X)$. Comme $\Phi_1(X) = X - 1$ on obtient que

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

Plus généralement, si $a > 0$ la proposition ? montre que l'on a

$$X^{p^a} - 1 = \Phi_{p^a}(X)\Phi_{p^{a-1}}(X)\cdots\Phi_1(X)$$

d'après ?. Par suite,

$$\Phi_{p^a}(X) = \frac{X^{p^a} - 1}{X^{p^{a-1}} - 1} = \Phi_p(X^{p^{a-1}}) = X^{p^{a-1}(p-1)} + X^{p^{a-1}(p-2)} + \cdots + X^{p^{a-1}} + 1$$

Nous allond donner une formule permettant de calculer $\Phi_n(X)$ pour un entier n quelconque. Posons

$$\mu(n) = \begin{cases} (-1)^k & \text{si } n \text{ est produit de } k \text{ nombres premiers } \textit{distincts}; \\ 0 & \text{sinon.} \end{cases}$$

Par exemple, $\mu(1) = 1$, $\mu(2) = -1$, $\mu(3) = -1$, $\mu(4) = 0$, $\mu(5) = -1$ et $\mu(6) = 1$. On dit que $\mu(n)$ est la *fonction de Mœbius*. Nous verrons dans la prochaine section que l'on a

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

Proposition . *On a*

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

Preuve: Si $\delta \mid n$ alors on a

$$\begin{aligned}\sum_{\delta|d|n}\mu\Big(\frac{n}{d}\Big)&=\sum_{\delta|d|n}\mu\Big(\frac{n/\delta}{d/\delta}\Big)\\ &=\sum_{d'|(n/\delta)}\mu\Big(\frac{n/\delta}{d'}\Big)=\begin{cases}1 & \text{if } n=\delta\\ 0 & \text{sinon}\end{cases}\end{aligned}$$

Par suite,

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

CQFD

Par exemple

$$\Phi_6(X)=\frac{(X^6-1)(X-1)}{(X^3-1)(X^2-1)}=X^2-X+1$$

$$\Phi_{12}(X)=\frac{(X^{12}-1)(X^2-1)}{(X^6-1)(X^4-1)}=X^4-X^2+1$$