Résumé de CM7

Équation algébrique (la suite)

Nous avons vu qu'une équation algébrique de degré 2 avec les coefficients dans $\mathbb{C}$ admet toutes les racines dans $\mathbb{C}$. Alors, que peut-on dire pour une équation algébrique de degré > 2 ?

Traitons un cas simple: étant donné $w \in \mathbb{C} \setminus \{0\}$, trouver tous les $z \in \mathbb{C}$ vérifiant $z^n = w$ pour un $n > 1$. Ce problème est résoluble généralisant la deuxième méthode expliquée ci-dessus pour $n = 2$:

Racines n-ème: Travaillons avec la forme exponentielle: $w = Re^{i\theta}$ ($R \in \mathbb{R}_+^*$ et $\theta \in \mathbb{R}$). Cherchons $z = re^{i\varphi}$ ($r \in \mathbb{R}_+^*$ et $\varphi \in \mathbb{R}$) vérifions $w = z^n$. Or $z^n = r^n e^{n\varphi i}$, on a

$$R = |w| = |z^n| = |z|^n = r^n \quad \text{i.e.,} \quad r^n = R,$$

d'où $r = R^{\frac{1}{n}} = \sqrt[n]{R}$. Ensuite, $w = z^n$ implique que $Re^{\theta i} = r^n e^{n\varphi i} = Re^{n\varphi i}$, i.e., $e^{\theta i} = e^{n\varphi i}$. En tenant en compte du fait que la fonction $\theta \longmapsto e^{i\theta}$ est 2π-périodique, i.e., $e^{(\theta+2\pi)i} (= e^{\theta i} \cdot e^{2\pi i}) = e^{\theta i}$ d'après la formule d'Euler, l'égalité $e^{\theta i} = e^{n\varphi i}$ implique

$$n\varphi = \theta + 2k\pi \quad k \in \mathbb{Z} \qquad \text{i.e.,} \qquad \varphi = \frac{1}{n}\theta + \frac{2k\pi}{n} \quad k \in \mathbb{Z}.$$

Que signifie-t-il ? Par définition, $e^{\varphi i} = e^{\frac{1}{n}\theta i} \cdot e^{\frac{2k\pi i}{n}}$ $(k \in \mathbb{Z})$. Étudions les valeurs de $e^{\frac{2k\pi i}{n}}$ $(k \in \mathbb{Z})$. Tout d'abord, comme $(e^{\frac{2k\pi i}{n}})^n = e^{2k\pi i} = 1$, ces valeurs sont des n-ème racines d'unité ! De plus, puisque

$$e^{\frac{2(k+n)\pi i}{n}} = e^{\frac{2k\pi i + 2n\pi i}{n}} = e^{\frac{2k\pi i}{n}} \cdot e^{\frac{2n\pi i}{n}} = e^{\frac{2k\pi i}{n}} \cdot e^{2\pi i} = e^{\frac{2k\pi i}{n}} \qquad \text{i.e.,} \qquad e^{\frac{2(k+n)\pi i}{n}} = e^{\frac{2k\pi i}{n}},$$

$k \mapsto e^{\frac{2k\pi i}{n}}$ est n-périodique. Ceci implique l'égalité suivante

$$\{e^{\frac{2k\pi i}{n}}\}_{k\in\mathbb{Z}} = \{e^{\frac{2k\pi i}{n}}\}_{0\le k<n}.$$

On en conclut que les racines n-ème de $w = Re^{\theta i}$ sont

$$z = R^{\frac{1}{n}} e^{\frac{1}{n}\theta i} \cdot e^{\frac{2k\pi i}{n}} \quad 0 \le k < n.$$

Plus généralement, le théorème suivant est connu:

Théorème (D'Alembert-Gauss). Toute équation algébrique avec les coefficients complexes ont les racines dans $\mathbb{C}$. (On dit que le corps des nombres complexes $\mathbb{C}$ est **algébriquement clos**.) □

Ce théorème insiste que on peut toujours trouver les racines d'un polynôme avec les coefficients complexes dans $\mathbb{C}$, mais il ne dit rien comment les trouver.... Voici l'histoire:

1. En 1545, J. Cardano (1501 - 1576) a publié sa formule donnant les solution d'une équation algébrique de degré 3
2. En 1540, L. Ferrari (1522 - 1565) a trouvé une méthode permettant à résoudre une équation algébrique de degré 4.

3. En 1823, N. H. Abel (1802 - 1829) a montré qu'une équation algébrique de degré ≥ 5 n'est pas forcément résoluble, i.e., on ne peut pas forcément obtenir les solutions uniquement par des opérations algébrique, i.e., $\sqrt[n]{\cdot}$, $+, -, \times, \div$.

4. En 1828, Évariste Galois (1811 - 1832) lui a abordé le problème de détermination si une équation algébrique donnée est résoluble uniquement avec des opérations algébriques.

Aspect géométrique

Ici, nous interprétons géométriquement des opérations sur $\mathbb{C}$ via la correspondance biunivoque[1]:

$$\mathbb{C} = \{\, a + bi \,|\, a, b \in \mathbb{R} \,\} \longleftrightarrow \mathbb{R}^2;\ a + bi \longleftrightarrow (a, b).$$

Soit $z = x + yi \in \mathbb{C}$ $(x, y \in \mathbb{R})$. En particulier, pour $z \in \mathbb{C}^*$, soient $r \in \mathbb{R}_+^*$ et $\varphi \in \mathbb{R}$ tels que $z = re^{i\varphi}$.

1. $z \mapsto z + \alpha$ $(\alpha \in \mathbb{C})$. Pour $\alpha = a + bi$ $(a, b \in \mathbb{R})$,

$$\begin{array}{ccc} z = x + yi & \longmapsto & z + \alpha = (x + a) + (y + b)i \\ \updownarrow & & \updownarrow \\ (x, y) & \longmapsto & (x + a, y + b) \end{array}$$

, c'est-à-dire, cette transformation induit une **translation** sur le plan $\mathbb{R}^2$.

2. $z \mapsto \alpha z$ $(\alpha \in \mathbb{C}^*)$. Pour $\alpha = Re^{i\theta}$ $(R \in \mathbb{R}_+^*, \theta \in \mathbb{R})$,

$$\begin{array}{ccc} z & \longmapsto & \alpha z \\ \updownarrow & & \updownarrow \\ re^{i\varphi} & \longmapsto & Rre^{i(\theta+\varphi)} \end{array}$$

, en particulier,

1. lorsque $\theta = 0$, le diagramme ci-dessus nous donne $z \mapsto Rz$, i.e., $(x, y) \mapsto (Rx, Ry)$, d'où ça donne une **homothétie** ou **dilatation**, et

2. lorsque $r = 1$, le diagramme ci-dessus nous donne $z \mapsto e^{i\varphi}z$, i.e., c'est une **rotation**.

En générale, ça donne une composée d'un homothétie et une rotation !

3. $z \mapsto \dfrac{1}{z}z$. Calculons les images d'une droite (sans passer l'origine) et d'un cercle.

[1] autrement dit, application bijective

1. L'image de droite $\mathrm{Re}(z) = 1$ [2].
   Posons $w = \dfrac{1}{z}$. Alors, $\mathrm{Re}(z) = \dfrac{z+\bar{z}}{2} = 1$ implique que $\dfrac{1}{w} + \dfrac{1}{\bar{w}} = 2$. Cette dernière est équivalente à $\left|w - \dfrac{1}{2}\right| = \dfrac{1}{2}$ $\left(w \neq 0\right)$, d'où son image est un cercle de rayon $\dfrac{1}{2}$ avec centre $\left(\dfrac{1}{2}, 0\right)$, privé du l'origine $(0,0)$.

2. L'image du cercle

   i) $\left|z - \dfrac{1}{2}\right| = \dfrac{1}{2}$ [3] est la droite $\mathrm{Re}(z) = 1$ car en itérrant cette transformation deux fois, on obtient l'application identité.

   ii) $|z-2| = 1$. Posons $w = \dfrac{1}{z}$. Alors, cette équation implique que $\left|\dfrac{1}{w} - 2\right| = 1$, qui est équivalente à $\left|w - \dfrac{2}{3}\right| = \dfrac{1}{3}$, i.e., l'image de ce cercle est le cercle de rayon $\dfrac{1}{3}$ avec centre $\left(\dfrac{2}{3}, 0\right)$.

En générale, l'image d'une droite ou d'un cercle par la transformation $z \mapsto \dfrac{1}{z}$ est encore un cercle ou une droite (privé à un point au maximal).

Soient $\alpha, \beta, \gamma, \delta \in \mathbb{C}$ tels que $\alpha\delta - \beta\gamma \neq 0$. considérons la transformation $z \mapsto \dfrac{\alpha z + \beta}{\gamma z + \delta}$, appelée une **transformation de Möbius**. Puisque

$$\frac{\alpha z + \beta}{\gamma z + \delta} = \frac{\alpha}{\delta}\left(z + \frac{\beta}{\alpha}\right)$$

si $\gamma = 0$ et sinon

$$\frac{\alpha z + \beta}{\gamma z + \delta} = \frac{\alpha\left(z + \frac{\delta}{\gamma}\right) - \frac{\alpha\delta - \beta\gamma}{\gamma}}{\gamma\left(z + \frac{\delta}{\gamma}\right)} = \frac{\alpha}{\gamma} - \frac{\alpha\delta - \beta\gamma}{\gamma^2} \cdot \frac{1}{z + \frac{\delta}{\gamma}},$$

cette transformation est une composée de transformations décrites ci-dessus. On en déduit que l'image d'un cercle ou d'une droite par une transformation de Möbius est encore un cercle ou une droite (privé à un point au maximum).

[2] Toute droite qui ne passe l'origine est un image de cette droite par une transformation de type 2 ci-dessus.
[3] Tout cercle qui ne passe l'origine est un image de ce cercle par une transformation de type 2 ci-dessus.

Arithmétique (sur $\mathbb{Z}$)

Divisibilité

Définition Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^* := \mathbb{Z} \setminus \{0\}$. Lorsqu'il existe un entier $q \in \mathbb{Z}$ tel que $a = bq$, on dit que a est un **multiple** de b et que b est un **diviseur** de a. On le note par $b|a$. □

Soient a, b et c des entiers tel que $a \neq 0$. Alors, on peut montrer que

1. $a \,|\, (b + c)$ si $a \,|\, b$ et $a \,|\, c$,
2. $a \,|\, bc$ si $a \,|b$ ou $a \,|\, c$.

Notons que ces deux conditions sont **suffisantes** mais pas **nécessaires**s.

Le théorème suivant est fondamental :

Théorème (Division euclidienne). Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^* := \mathbb{Z} \setminus \{0\}$. Alors, il existe un unique couple $(q, r) \in \mathbb{Z}^2$ vérifiant

$$a = qb + r, \qquad 0 \leq r < |b|.$$

□

Preuve Comme $\mathbb{R} = \coprod_{q \in \mathbb{Z}} [|b|q, |b|(q + 1)[$, $\exists! q \in \mathbb{Z}$ tel que $bq \leq a < bq + |b|$, d'où en posant $r = a - bq$, on voit que les deux conditions sont vérifiées. □

PGCD et PPCM

Soit $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$. Alors, l'ensemble

$$\mathcal{M} := \{\, m \in \mathbb{N} \,|\, a \,|\, m \text{ et } b \,|\, m \,\}$$

est non-vide car $ab \in \mathcal{M}$. Lorsque l'ensemble $\mathcal{M} \cap \mathbb{N}^*$ est non-vide, son plus petite élément est dit le plus petit commun multiple (**PPCM**), noté $\text{ppcm}(a, b)$. Sinon, $0 \in \mathcal{M}$ est dit le PPCM, noté également. L'ensemble

$$\mathcal{D} := \{\, d \in \mathbb{N} \,|\, d \,|\, a \text{ et } d \,|\, b \,\}$$

est non-vide car $1 \in \mathcal{D}$, de plus cet ensemble est fini. Le plus grand élément de $\mathcal{D}$ est dit le petit grand commun diviseur (**PGCD**), noté $\text{pgcd}(a, b)$.

Théorème (PPCM) Soient a et b deux entiers non nuls. Alors, un entier m qui est un multiple commun de a et de b et un multiple de $\text{ppcm}(a, b)$. □

Preuve Posons $l = \text{ppcm}(a, b)$. Alors, $\exists!(q, r) \in \mathbb{Z}^2$ tel que

$$m = ql + r \qquad 0 \leq r < l.$$

Comme $r = m - ql$ et m et l sont multiples de a et de b, r l'est aussi. Comme $0 \leq r < l$, la minimalité de l implique que $r = 0$, i.e., $m = ql$. □

Théorème (PGCD) Soient a et b deux entiers non nuls. Alors, un entier d qui est un diviseur commun de a et de b et un diviseur de $\text{pgcd}(a, b)$. □

Preuve Posons $m = \text{pgcd}(a, b)$. Il suffit de montrer que $l := \text{ppcm}(m, d) = m$. Comme a est un multiple de m et de d, a est un multiple de l. De même, b est un multiple de l, d'où l est un diviseur commun de a et de b. En particulier, ceci implique que $l \leq m$. Par la définition de l, on a $l \geq m$, d'où $l = m$. □

Maintenant, montrons le théorème suivant:

Théorème Soient $a, b \in \mathbb{N}^*$. Alors, $a \cdot b = \text{ppcm}(a, b) \cdot \text{pgcd}(a, b)$. □

Preuve Notons $d = \text{pgcd}(a, b)$. Alors, i existe $a', b' \in \mathbb{N}^*$ tels que $a = a'd$ et $b = b'd$. Le PGCD de a' et b' est 1, car sinon, $d \cdot \text{pgcd}(a', b')$ divise deux entiers a et b qui contredit à la maximalité de $\text{pgcd}(a, b)$. Alors, le PPCM de a' et b' étant $a'b'$, le PPCM de a et b est égale à $da'b' = ab' = a'b$, d'où

$$\text{pgcd}(a, b) \cdot \text{ppcm}(a, b) = d \cdot da'b' = da' \cdot db' = a \cdot b.$$

□

Étant donnée deux entiers $a, b \in \mathbb{N}^*$, ce théorème indique que sachant l'un des deux ($\text{pgcd}(a, b)$ ou $\text{ppcm}(a, b)$), on pourra calculer l'autre. L'algorithme suivant nous donne une méthode pratique pour calculer le PGCD de a et b.

Algorithme d'Euclide

Le principe de cet algorithme est suivant: soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. Par la division euclidienne, il existe un unique $(q, r) \in \mathbb{Z}^2$ tel que $a = bq + r$ et $0 \leq r < |b|$. Alors,

$$\text{pgcd}(a, b) = \text{pgcd}(a - bq, b) = \text{pgcd}(b, r). \tag{1}$$

Basé sur ce principe, l'**algorithme d'Euclide** est présenté comme suit.

Soit $a, b \in \mathbb{Z}^*$ tel que $|a| > |b|$. Alors, $\exists!(q, r) \in \mathbb{Z}^2$ tel que

$$a = qb + r \qquad 0 \leq r < |b|.$$

Si $r = 0$, alors, $a = qb$ et $\text{pgcd}(a, b) = b$. Supposons que $r \neq 0$. Alors, il existe $n \in \mathbb{N}^*$ vérifiant la propriété suivante:

$$\begin{aligned}
\exists!\,(q_1, r_1) \in \mathbb{Z}^2 \quad &\text{t.q.} \quad b = q_1 r + r_1 \qquad 0 < r_1 < r, \\
\exists!\,(q_2, r_2) \in \mathbb{Z}^2 \quad &\text{t.q.} \quad r = q_2 r_1 + r_2 \qquad 0 < r_2 < r_1, \\
&\vdots \\
\exists!\,(q_{n-1}, r_{n-1}) \in \mathbb{Z}^2 \quad &\text{t.q.} \quad r_{n-3} = q_{n-1} r_{n-2} + r_{n-1} \qquad 0 < r_{n-1} < r_{n-2}, \\
\exists!\,q_n \in \mathbb{Z} \quad &\text{t.q.} \quad r_{n-2} = q_n r_{n-1}.
\end{aligned}$$

Alors, le principe (1) expliqué ci-dessus implique que

$$\begin{aligned}
\text{pgcd}(a, b) =& \text{pgcd}(a - qb, b) = \text{pgcd}(b, r) \\
=& \text{pgcd}(b - q_1 r, r) = \text{pgcd}(r, r_1) \\
=& \text{pgcd}(r - q_2 r_1, r_1) = \text{pgcd}(r_1, r_2) \\
&\vdots \\
=& \text{pgcd}(r_{n-3} - q_{n-1} r_{n-2}, r_{n-2}) = \text{pgcd}(r_{n-2}, r_{n-1}) \\
=& r_{n-1},
\end{aligned}$$

d'où $\boxed{\text{pgcd}(a, b) = r_{n-1}}$! □