Nombres complexes

La construction du corps des réels a permis de gagner, par rapport au corps des rationnels, des propriétés topologiques importantes : complétude, théorème de la borne supérieure... À partir de ces propriétés topologiques, on peut (entre autres par le biais du « théorème des valeurs intermédiaires ») gagner d'autres propriétés encore par rapport aux rationnels, de nature algébrique celles-ci : l'existence de solutions pour *certaines* équations algébriques (*i.e.* de la forme $\mathrm{P}(x) = 0$ avec $\mathrm{P}(x)$ un polynôme), par exemple lorsque $\mathrm{P}(x)$ est de la forme $x^2 - a$, avec $a \in \mathbb{R}_+$, ou encore lorsque $\mathrm{P}(x)$ est de degré impair.

Toutefois, certaines équations algébriques à coefficients dans $\mathbb{R}$ resteront sans solution réelle, par exemple $x^2 - a = 0$ si $a \in \mathbb{R}_-^*$... D'où la nécessité d'étendre encore une fois notre ensemble de nombres, en formant un sur-corps de $\mathbb{R}$ (noté $\mathbb{C}$, dont les éléments seront les *nombres complexes*) sur-corps que se révèlera *algébriquement clos*, c'est-à-dire dans lequel cette fois <u>toute</u> équation algébrique (à coefficients dans $\mathbb{C}$) aura des solutions.

Notre étude comportera trois chapîtres. L'objet de ce premier chapître est de définir l'ensemble $\mathbb{C}$ et de montrer, par des moyens élémentaires, que la propriété ci-dessus est vraie pour les équations du second degré. Pour obtenir la propriété dans le cadre générale (avec un degré quelconque), il faut un outillage théorique beaucoup plus important, qui nécessite en particulier la notion d'*argument* d'un complexe non nul (ce sera l'objet du prochain chapître) ; dans le troisième et dernier chapître, on montrera enfin la propriété de clôture algébrique de $\mathbb{C}$.

1 Le corps commutatif $(\mathbb{C}, +, \times)$

Définition Un *nombre complexe* est un élément $(a, b) \in \mathbb{R}^2$; on note $\mathbb{C}$ l'ensemble des nombres complexes (l'ensemble $\mathbb{C}$ n'est autre que $\mathbb{R}^2$, muni des lois que nous allons définir).

Addition sur $\mathbb{C}$: On définit la *somme* de deux complexes (a, b) et (c, d) par :

$$(a, b) + (c, d) = (a + c, b + d)$$

Multiplication sur $\mathbb{C}$: On définit le *produit* des complexes (a, b) et (c, d) par :

$$(a, b) \times (c, d) = (ac - bd, ad + bc)$$

Théorème 1.1 $(\mathbb{C}, +, \times)$ *est un corps commutatif.*

Démonstration :

- $(\mathbb{C}, +)$ est un groupe commutatif, d'élément neutre $(0, 0)$; le symétrique (ou *opposé*) d'un complexe (a, b) est le complexe $(-a, -b)$.

- Commutativité de la loi $\times$: Soient (a,b) et (c,d) deux complexes. Grâce à la commutativité de la multiplication sur $\mathbb{R}$, on a

$$(a,b)\times(c,d)=(ac-bd,ad+bc)=(ca-db,cb+da)=(c,d)\times(a,b)$$

- Associativité de la loi $\times$: Soient (a,b), (c,d) et (e,f) des complexes. Alors

$$\begin{aligned}((a,b)\times(c,d))\times(e,f)&=(ac-bd,ad+bc)\times(e,f)\\&=((ac-bd)e-(ad+bc)f,(ac-bd)f+(ad+bc)e)\\&=(ace-bde-adf-bcf,acf-bdf+ade+bce)\end{aligned}$$

$$\begin{aligned}(a,b)\times((c,d)\times(e,f))&=(a,b)\times(ce-df,cf+de)\\&=(a(ce-df)-b(cf+de),a(cf+de)+b(ce-df))\\&=(ace-adf-bcf-bde,acf+ade+bce-bdf)\end{aligned}$$

- Distributivité de $\times$ sur $+$: Toujours en revenant aux définitions des lois $+$ et $\times$ sur $\mathbb{C}$, on montre la relation :

$$((a,b)+(c,d))\times(e,f)=((a,b)\times(e,f))+((c,d)\times(e,f))$$

  Grâce à la commutativité de la multiplication, on a également la distributivité à gauche.

- $(1,0)$ est élément neutre de $\times$:

$$\forall(a,b)\in C,\quad (a,b)\times(1,0)=(a\times1-b\times0,a\times0+b\times1)=(a,b)$$

- Inverse d'un complexe $(a,b)\neq(0,0)$: Soit (a,b) un complexe non nul. Si $a^2+b^2=0$, alors nécessairement $a^2=0$ et $b^2=0$, donc $a=0$ et $b=0$, ce qui est absurde. Donc $a^2+b^2>0$, et

$$(a,b)\times(c,d)=(1,0)\Longleftrightarrow\left\{\begin{array}{l}ac-bd=1\\ad+bc=0\end{array}\right.\Longleftrightarrow\left\{\begin{array}{l}c=\dfrac{a}{a^2+b^2}\\d=\dfrac{-b}{a^2+b^2}\end{array}\right.$$

□

<u>NOTATION :</u> L'opposé d'un complexe z se note $-z$. Si z_1 et z_2 sont deux complexes, on note z_1-z_2 le complexe $z_1+(-z_2)$.

L'inverse d'un complexe z non nul se note $1/z$. Si z_1 et z_2 sont deux complexes avec z_2 non nul, on note $\dfrac{z_1}{z_2}$ le complexe $z_1\times1/z_2$.

2 Plongement de $\mathbb{R}$ dans $\mathbb{C}$

Soit $\mathbb{C}'$ l'ensemble des complexes de la forme $(a,0)$. L'ensemble $\mathbb{C}'$ est non vide, et pour tous réels a et b :

$$(a,0)-(b,0)=(a-b,0)\in\mathbb{C}'$$

et

$$(a,0)\times(b,0)=(ab,0)\in\mathbb{C}'$$

Enfin $(1,0)\in\mathbb{C}'$ et, si $a\neq0$:

$$\frac{1}{(a,0)}=(\frac{1}{a},0)\in\mathbb{C}'$$

En conclusion, $(\mathbb{C}', +, \times)$ est un sous-corps de $(\mathbb{C}, +, \times)$.

Soit alors l'application $f : \mathbb{R} \longrightarrow \mathbb{C}', a \mapsto f(a) = (a, 0)$.
f est bijective par définition de $\mathbb{C}'$. Pour tous réels a et b, on a manifestement :

$$f(a+b) = f(a) + f(b) \quad \text{et} \quad f(ab) = f(a)f(b)$$

Donc f est un isomorphisme de $(\mathbb{R}, +, \times)$ sur $(\mathbb{C}', +, \times)$.

Convention : L'isomorphisme f permet d'identifier $\mathbb{R}$ à $\mathbb{C}'$ (d'où, par abus de langage, $\mathbb{R} \subset \mathbb{C}$), les lois $+$ et $\times$ sur $\mathbb{C}$ prolongeant alors celles de $\mathbb{R}$ (méthode déjà suivie pour de précédentes extensions d'ensembles de nombres). Pour tout $x \in \mathbb{R}$, on notera donc x le complexe $(x, 0)$; en particulier 0 est le complexe $(0, 0)$ et 1 le complexe $(1, 0)$.

Remarque $\forall x \in \mathbb{R}\ \forall (a, b) \in \mathbb{C}, \quad x \times (a, b) = (xa, xb)$.

En effet $x \times (a, b) = (x, 0) \times (a, b) = (xa - 0 \times b, xb + 0 \times a) = (xa, xb)$

Définition $z \in \mathbb{C}$ est *imaginaire* si et seulement si $z \notin \mathbb{R}$ (*i.e.* $z = (a, b)$ avec $b \neq 0$). Si z s'écrit $(0, b)$, avec b non nul, on dit que z est un *imaginaire pur.*

<u>Notation :</u> On note i le complexe $(0, 1)$. On a en particulier :

$$i^2 = (0, 1) \times (0, 1) = (-1, 0) = -1$$

Tout complexe $z = (a, b)$ peut alors s'écrire grâce au nombre i sous la forme $a + ib$, avec a et b réels. En effet, soit $z = (a, b)$ un complexe.

Alors $$z = (a, 0) + (0, b) = a \times (1, 0) + b \times (0, 1) = a + ib$$

Définition Le réel a est la *partie réelle* de z (notée $\mathfrak{Re}(z)$), b est sa *partie imaginaire de* z (notée $\mathfrak{Im}(z)$). L'expression $a + ib$ est appelée *écriture algébrique* du complexe z.

Remarque Il n'existe pas d'ordre total sur $\mathbb{C}$ prolongeant l'ordre $\leq$ sur $\mathbb{R}$ et qui fasse de $(\mathbb{C}, +, \times)$ un corps totalement ordonné (*i.e.* tel que la relation d'ordre soit compatible avec la loi $+$ sur $\mathbb{C}$ et avec la loi $\times$ sur $\{z \in \mathbb{C} \mid 0 \leq z\}$).

Si un tel ordre $\leq$ existait, on aurait nécessairement $i^2 \geq 0$ (ou bien $i \geq 0$, auquel cas $i^2 \geq 0$, ou bien $i \leq 0$ donc $0 = i - i \leq -i$ et donc $i^2 = (-i)^2 \geq 0$). Or $i^2 = -1$, on a donc $-1 \geq 0$, ce qui est incompatible avec l'ordre sur $\mathbb{R}$.

3 Racines des polynômes de degré 2

Nous venons de voir que dans $\mathbb{C}$, il existe un nombre noté i et qui vérifie $i^2 = -1$. Multipliant i par des réels, on obtient ainsi facilement des nombres vérifiant une équation du type $x^2 + a = 0$, ce quel que soit a réel positif. Mais ça ne s'arête pas là :

Lemme 3.1 *Tout complexe z non nul admet exactement deux racines carrées (c'est-à-dire que l'équation $x^2 = z$ admet deux solutions dans $\mathbb{C}$).*

Démonstration : Soit donc $z = (a, b)$ un complexe. On cherche à résoudre l'équation $(x, y)^2 = (a, b)$, c'est-à-dire le système :

$$\begin{cases} x^2 - y^2 = a \\ 2xy = b \end{cases}$$

- Si $b = 0$ et $a > 0$, alors $2xy = 0$, donc nécessairement $x = 0$ ou $y = 0$. Le cas $x = 0$ est alors absurde puisqu'il mène à l'équation $-y^2 = a$, avec $-y^2 \leq 0$ et $a > 0$.
  L'équation $x^2 - y^2 = a$ devient donc $x^2 = a$. Elle admet alors deux racines qui sont $\sqrt{a}$ et $-\sqrt{a}$. Le système a alors pour solutions les deux complexes $(\sqrt{a}, 0) = \sqrt{a}$ et $(-\sqrt{a}, 0) = -\sqrt{a}$.
- Si $b = 0$ et $a < 0$, on a toujours $x = 0$ ou $y = 0$, et cette fois c'est le cas $y = 0$ qui est absurde, car alors $0 \leq x^2 = a < 0$.
  On obtient donc l'équation $-y^2 = a$, donc $y = \pm\sqrt{-a}$. Le système a donc pour solutions les complexes $\left(0, \sqrt{-a}\right) = i\sqrt{-a}$ et $\left(0, -\sqrt{-a}\right) = -i\sqrt{-a}$.
- Si enfin $b \neq 0$, alors nécessairement $x \neq 0$ et $y \neq 0$. L'équation $2xy = b$ nous donne alors $y = \dfrac{b}{2x}$, soit en remplaçant dans la première équation :
  $$x^2 - \frac{b^2}{4x^2} = a \quad \Longleftrightarrow \quad x^4 - ax^2 - \frac{b^2}{4} = 0$$
  En posant $\mathrm{X} = x^2$, cette dernière équation se ramène à l´équation du second degré $\mathrm{X}^2 - a\mathrm{X} - \dfrac{b^2}{4} = 0$, de discriminant $a^2 + b^2 > 0$, et de racines :
  $$\frac{a - \sqrt{a^2 + b^2}}{2} < 0 \quad \text{et} \quad \frac{a + \sqrt{a^2 + b^2}}{2} > 0$$
  Soit deux solution pour x exactement : comme on a posé $\mathrm{X} = x^2$, il faut que X soit positif, et donc $x = \pm\sqrt{\dfrac{a + \sqrt{a^2 + b^2}}{2}}$. Notre système a là encore deux solutions complexes :
  $$\sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}} + \frac{ib}{2\sqrt{\dfrac{a + \sqrt{a^2 + b^2}}{2}}}$$
  et
  $$-\sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}} - \frac{ib}{2\sqrt{\dfrac{a + \sqrt{a^2 + b^2}}{2}}}$$
  □

Théorème 3.2 *Tout polynôme de degré 2 sur $\mathbb{C}$ possède deux racines.*

Démonstration : Soit donc un polynôme de degré 2 à coefficients complexes : $\mathrm{P}(z) = az^2 + bz + c$, avec $a \neq 0$.

Un complexe z est racine de P si et seulement s'il vérifie l'équation :
$$z^2 + \frac{b}{a}z + \frac{c}{a} = 0 \quad \Longleftrightarrow \quad \left(z + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2}$$
Or le lemme précédent nous permet d'affirmer que cette dernière équation admet deux racines dans $\mathbb{C}$ lorsque le second membre est non nul (une seule sinon). On en déduit que P a exactement 2 racines (une racine double lorsque $b^2 - 4ac = 0$).

□

En réalité, le résultat est bien plus fort que cela : tout polynôme complexe admet une racine (et donc n racines, où n est son degré). On dit que $\mathbb{C}$ est *algébriquement clos*. C'est ce que nous verrons lorsque nous auront tous les outils nécessaires.

4 Conjugué, module d'un complexe

Définition Le *conjugué* du complexe $z = a + ib$ (avec $a, b \in$ R) est le complexe $\overline{z} = a - ib$

Les propriétés suivantes découlent de la définition du conjugué :

Propriétés
Pour tout complexe z, on a :

1. $z + \overline{z} = 2\mathfrak{Re}(z)$
2. $z - \overline{z} = 2i\mathfrak{Im}(z)$
3. Et donc $z = \overline{z} \iff z \in \mathbb{R}$
4. Enfin $z\overline{z} = (\mathfrak{Re}(z))^2 + (\mathfrak{Im}(z))^2 \in \mathbb{R}_+$

Théorème 4.1 *L'application conjugaison :* $\left\{ \begin{array}{rcl} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \overline{z} \end{array} \right.$
est un automorphisme involutif de $(\mathbb{C}, +, \times)$

Démonstration : Soient $z = a + ib$ et $z' = a' + ib'$ deux complexes.

On a $$\overline{z + z'} = a + a' - i\,(b + b') = a - ib + a' - ib' = \overline{z} + \overline{z}'$$

et $$\overline{zz'} = (aa' - bb') - i\,(ab' + ba') = (a - ib)\,(a' - ib') = \overline{z} \cdot \overline{z}'$$

Enfin $$\overline{\overline{z}} = \overline{a - ib} = a + ib = z$$

donc la conjugaison est involutive donc bijective (d'inverse égale à elle-même).

□

Théorème 4.2 *L'application* $n : \left\{ \begin{array}{rcl} \mathbb{C}^* & \longrightarrow & \mathbb{R}_+^* \\ z & \longmapsto & n(z) = z\overline{z} \end{array} \right.$

est un homomorphisme de $(\mathbb{C}^*, \times)$ *dans* $(\mathbb{R}_+^*, \times)$

Démonstration : n est bien à valeur dans $\mathbb{R}_+^*$. En effet, si z est un complexe non nul, alors $n(z) = (\mathfrak{Re}(z))^2 + (\mathfrak{Im}(z))^2$ est un réel strictement positif (il est non nul car sinon on aurait $\mathfrak{Re}(z) = \mathfrak{Im}(z) = 0$, c'est-à-dire $z = 0$.

Soient alors z et z' deux complexes non nuls.

$$n\,(zz') = (zz') \cdot \overline{zz'} = z \cdot z' \cdot \overline{z} \cdot \overline{z}' = (z\overline{z}) \cdot (z'\overline{z}') = n(z)n(z')$$ □

Remarque On prolonge bien sûr n en 0 en posant $n(0) = 0$.

Dans $\mathbb{R}$, on a la propriété $\forall x \in \mathbb{R}^+ \ \exists! y \in \mathbb{R}^+, \quad x = y^2$
Ce réel positif y, noté $\sqrt{x}$, est la *racine carrée de* x.

Définition Appliquant ce résultat, on appelle *module* du complexe z le réel positif $\sqrt{n(z)}$, que l'on note $|z|$.

Le théorème précédent se traduit alors par la propriété :

$$\forall z, z' \in \mathbb{C}, \quad |zz'| = |z| \cdot |z'|$$