Clôture algébrique de $\mathbb{C}$

On a construit $\mathbb{C}$ pour pouvoir résoudre plus d'équations algébriques (on a déjà vu que l'on pouvait résoudre toutes celles de degré 2, par ailleurs le nombre i est apparu historiquement comme un artifice de calcul pour certaines équations de degré 3 dans $\mathbb{R}$). Or, il se trouve que dans $\mathbb{C}$, on peut résoudre non seulement toutes les équations de degré 2, mais toutes les équations polynomiales ! C'est la propriété de *clôture algébrique* du corps $\mathbb{C}$, parfois qualifiée de *théorème fondamental de l'algèbre*, ou encore restitué à deux de ses pères (*théorème de d'Alembert-Gauss*). Il en existe de très nombreuses démonstrations, nous en présentons ici celle qui fait appel aux outils les plus élémentaires (ce n'est pas la plus simple, ou plus exactement pas la plus courte : certaines preuves tiennent en une ligne, mais nécessitent de solides connaissances d'analyse complexe).

Soit P un polynôme non constant sur $\mathbb{C}$, n son degré. P s'écrit sous la forme :

$$\mathrm{P}(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0$$

où $a_0, \ldots, a_n$ sont des complexes, et a_n est non nul. On va chercher à exhiber une racine de P.

Théorème 1 *Soit* P *un polynôme non constant. Alors la fonction* $z \mapsto |\mathrm{P}(z)|$ *atteint sa borne inférieure sur* $\mathbb{C}$.

(La fonction $z \mapsto |\mathrm{P}(z)|$ est à valeurs dans $\mathbb{R}_+$, donc minorée par 0. Sa borne inférieure est donc bien définie.)

Démonstration : Lorsque z est non nul, on peut écrire $\mathrm{P}(z)$ sous la forme :

$$\mathrm{P}(z) = a_n z^n \left(1 + \frac{a_{n-1}}{a_n z} + \cdots + \frac{a_0}{a_n z^n}\right)$$

donc
$$|\mathrm{P}(z)| \geq |a_n|\,|z|^n \left(1 - \left|\frac{a_{n-1}}{a_n z} + \cdots + \frac{a_0}{a_n z^n}\right|\right)$$

Chacun des termes de la forme $a_i/a_n z^{n-i}$ « tend » vers 0 lorsque $|z|$ tend vers $+\infty$, c'est-à-dire que pour tout réel $\varepsilon > 0$, il existe des réels A_i tel que l'on ait $\left|a_i/a_n z^{n-i}\right| < \varepsilon$ pour $|z| > \mathrm{A}_i$. Il en va donc de même pour leur somme (on a un nombre fini de termes). En particulier, il existe un réel B tel que :

$$|z| > \mathrm{B} \Longrightarrow \left|\frac{a_{n-1}}{a_n z} + \cdots + \frac{a_0}{a_n z^n}\right| < \frac{1}{2}$$

D'autre part pour $|z| > \left|\dfrac{2\mathrm{P}(0)}{a_n}\right|^{1/n}$ on a $|a_n|\,|z|^n > 2\,|\mathrm{P}(0)|$. Il vient :

$$|z| > \max\left(\mathrm{B}, \left|\frac{2\mathrm{P}(0)}{a_n}\right|^{1/n}\right) \Longrightarrow |\mathrm{P}(z)| > |\mathrm{P}(0)|$$

On a exhibé un réel M tel que, pour $|z| > \mathrm{M}$, on ait $|\mathrm{P}(z)| > |\mathrm{P}(0)|$. On s'intéresse désormais uniquement à la partie du plan complexe :

$$\mathrm{A} = \{z \in \mathbb{C}, \quad |z| \leq \mathrm{M}\}$$

En effet, on sait par définition de cette partie que si $z \notin \mathrm{A}$, alors $|\mathrm{P}(z)| > |\mathrm{P}(0)|$. Donc la borne inférieure sur $\mathbb{C}$ de la fonction $z \mapsto |\mathrm{P}(z)|$ est égale à sa borne inférieure sur A.

Mais la partie A est un disque fermé, c'est donc un « compact » de $\mathbb{C}$. La fonction $z \mapsto |\mathrm{P}(z)|$ est continue sur le compact A, elle atteint donc sa borne inférieure en (au moins) un point z_0. On a construit un complexe z_0 tel que :

$$|\mathrm{P}(z_0)| = \inf_{z \in \mathbb{C}} |\mathrm{P}(z)| \qquad \square$$

N.B. Détaillons un peu cet argument de compacité. Par définition de la borne inférieure, on peut construire une suite $(z_n)_{n \in \mathbb{N}}$ à valeurs dans A telle que :

$$\lim_{n \to +\infty} |\mathrm{P}(z_n)| = \inf_{z \in \mathrm{A}} |\mathrm{P}(z)|$$

Mais alors, la suite $(z_n)_{n \in \mathbb{N}}$ est bornée, on peut donc en extraire une sous-suite $\left(z_{\varphi(n)}\right)_{n \in \mathbb{N}}$ convergente (c'est là qu'intervient la compacité. Pour résumer, on commence par extraire une sous-suite dont les parties réelles convergent, de laquelle on extrait une sous-suite dont les parties imaginaires convergent. Cette dernière sous-suite converge dans $\mathbb{C}$). Soit z' la limite de la suite $\left(z_{\varphi(n)}\right)_{n \in \mathbb{N}}$. Par continuité de la fonction $z \mapsto |\mathrm{P}(z)|$, on a $\lim\limits_{n \to +\infty} \left|\mathrm{P}(z_{\varphi(n)})\right| = |\mathrm{P}(z')|$, et donc

$$\left|\mathrm{P}(z')\right| = \inf_{z \in \mathrm{A}} |\mathrm{P}(z)|$$

N.B. On a vraiment besoin de se ramener à un sous-ensemble borné de $\mathbb{C}$. Il existe en effet des fonctions minorées et continues mais qui n'atteignent pas leur borne inférieure. Par exemple, le polynôme à deux variables *réelles* définie par $\mathrm{P}(x, y) = x^2 + (xy - 1)^2$ est minoré (par 0), mais n'atteint pas sa borne inférieure (0 justement). Par identification de $\mathbb{C}$ et $\mathbb{R}^2$, on construit ainsi un contre-exemple sur $\mathbb{C}$ (la fonction $z \mapsto \mathfrak{Re}(z)^2 + (\mathfrak{Re}(z)\mathfrak{Im}(z) - 1)^2$).

Nous sommes désormais en mesure de prouver notre résultat principal :

Théorème 2 *Tout polynôme non constant admet une racine sur* $\mathbb{C}$.

Démonstration : Soit P un polynôme non constant, n son degré ($n > 0$). Pour tout complexe z, $\mathrm{P}(z)$ s'écrit sous la forme $\sum\limits_{i=0}^{n} a_i z^i$, avec $a_n \neq 0$.

D'après le théorème 1, il existe un complexe z_0 tel que :

$$|\mathrm{P}(z_0)| = \inf_{z \in \mathbb{C}} |\mathrm{P}(z)|$$

Nous allons montrer qu'en fait, z_0 est racine de P. Supposons qu'au contraire $\mathrm{P}(z_0) \neq 0$. L'idée est qu'au voisinage immédiat de z_0, on va alors trouver une direction dans laquelle le module de P va nécessairement diminuer, ce qui est absurde… (Ça contredira la minimalité de $|\mathrm{P}(z_0)|$.) On peut décomposer le polynôme $\mathrm{P}(z)$ comme une combinaison linéaire de termes de la forme $(z - z_0)^k$, avec k entier. Plus précisément, on a une relation du type :

$$\forall z \in \mathbb{C}, \quad \mathrm{P}(z) = \sum_{i=0}^{n} b_i (z - z_0)^i$$

En effet, la division euclidienne de P par le polynôme $(X - z_0)^n$ nous donne P sous la forme $P = a_n(X - z_0)^n + R_1$, avec R_1 de degré au plus $n - 1$. Il suffit alors d'effectuer la division euclidienne de R_1 par $(X - z_0)^{n-1}$, puis du reste suivant par $(X - z_0)^{n-2}$, etc. On obtient la décomposition annoncée, avec en plus $b_n = a_n \neq 0$. De plus, appliquant la relation en z_0, on a $P(z_0) = b_0$.

Soit p le plus petit indice strictement positif tel que $b_p \neq 0$. On peut alors écrire $P(z)$ sous la forme :

$$P(z) = P(z_0) + b_p(z - z_0)^p + \sum_{i=p+1}^{n} b_i(z - z_0)^i$$

c'est à dire qu'on a un polynôme $Q(z) = \sum_{i=p+1}^{n} b_i(z - z_0)^{i-p-1}$ tel que :

$$P(z) = P(z_0) + b_p(z - z_0)^p + (z - z_0)^{p+1}Q(z)$$

Écrivons le terme $P(z_0)$ sous forme exponentielle. On peut trouver R et θ tels que $P(z_0) = Re^{i\theta}$. On va chercher des z proches de z_0 pour lesquels le terme $b_p(z - z_0)^p$ sera dans la direction exactement opposée, c'est-à-dire d'argument $\theta+\pi$ (le terme $(z-z_0)^{p+1}Q(z)$ étant négligeable à côté de $b_p(z-z_0)^p$ au voisinage immédiat de z_0).

On écrit également le coefficient b_p sous la forme $re^{i\phi}$. On veut donc que l'argument de $re^{i\phi}(z - z_0)^p$ soit $\theta + \pi$, c'est-à-dire que $(z - z_0)^p$ soit d'argument $\theta - \phi + \pi$. Pour cela, il suffit de prendre z sous la forme $z_0 + ae^{i\alpha}$, avec a un réel positif et $\alpha = \dfrac{\theta - \phi + \pi}{p}$. Lorsque z est de cette forme, on a :

$$P(z_0) + b_p(z - z_0)^p = Re^{i\theta} + ra^p e^{i(\theta+\pi)} = (R - a^p r)e^{i\theta}$$

c'est-à-dire que, pour $0 < a < (R/r)^{\frac{1}{p}}$, on a bien trouvé quelquechose de module $R - a^p r$, strictement inférieur à $R = |P(z_0)|$, ce qui contredit la définition de z_0.

Reste à montrer que l'on peut effectivement négliger le terme $(z-z_0)^{p+1}Q(z)$. Soit M un majorant de $|Q(z)|$ sur la boule de centre z_0 et de rayon R/r (*i.e.* sur l'ensemble $\left\{z_0 + ae^{i\vartheta}, a \leq R/r, \vartheta \in]-\pi\,;\pi]\right\}$. Comme l'ensemble est fermé borné et la fonction $z \mapsto |Q(z)|$ continue, un tel majorant existe...)

Alors le terme $(z - z_0)^{p+1}Q(z)$ a son module majoré par Ma^{p+1}, où a est le réel tel que $z = z_0 + ae^{i\vartheta}$. Comme la quantité $\dfrac{Ma^{p+1}}{ra^p} = \dfrac{Ma}{r}$ tend vers 0 lorsque a tend vers 0, on en déduit bien que le terme $(z - z_0)^{p+1}Q(z)$ est négligeable devant le terme $b_p(z - z_0)^p$ au voisinage de z_0. En particulier, pour a suffisamment petit, on a $\left|(z - z_0)^{p+1}Q(z)\right| < |b_p(z - z_0)^p| = ra^p$, et donc :

$$|P(z)| \leq |P(z_0) + b_p(z - z_0)^p| + \left|(z - z_0)^{p+1}Q(z)\right| < (R - a^p r) + a^p r$$

soit finalement $$|P(z)| < |P(z_0)|$$ □

N.B. En fait, la technique précédente est fortement inspirée de l'analyse. Exprimer $P(z)$ sous la forme $P(z_0) + b_p(z - z_0)^p + (z - z_0)^{p+1}Q(z)$, c'est faire un développement limité de P au voisinage de z_0. Seul le premier terme non nul dudit développement limité est ensuite pris en compte : il « domine » tous les autres. Ici, dans la cas des polynômes, on a la chance de pouvoir écrire une telle décomposition de P sans parler de dérivées successive ni de développements limités...

Quelques remarques sur les polynômes dans un corps :

Théorème 3 *Soit $\mathbb{K}$ un corps. Soit n un entier, et P un polynôme de degré n à coefficients dans $\mathbb{K}$. Alors P a au plus n racines dans $\mathbb{K}$.*

Démonstration : On utilise constamment le

Lemme 4 *Si a est racine de P, alors P se factorise par $\mathrm{X} - a$.*

En effet, dans l'anneau euclidien $\mathbb{K}[\mathrm{X}]$, on peut effectuer la division euclidienne de P par $\mathrm{X} - a$. On obtient deux polynômes Q et R, avec R de degré strictement inférieur au degré de $\mathrm{X} - a$ (c'est-à-dire R constant), tels que :

$$\mathrm{P} = \mathrm{Q}(\mathrm{X} - a) + \mathrm{R}$$

Appliquant cette égalité en a, on obtient $\mathrm{P}(a) = \mathrm{R}(a)$. Si a est racine de P, ceci signifie que $\mathrm{P}(a) = 0$ donc R est le polynôme nul. □

Soit donc P un polynôme. Supposons que l'on ait trouvé au polynôme P n racines distinctes $x_1, \ldots, x_n$. Par récurrence, on montre que P se factorise par le produit $(\mathrm{X} - x_1) \ldots (\mathrm{X} - x_n)$:

- c'est immédiat pour une seule racine (c'est le lemme).
- supposons le résultat établi pour les k premières racines. P s'écrit comme un produit $(\mathrm{X} - x_1) \ldots (\mathrm{X} - x_k)\mathrm{Q}$, avec Q un polynôme. Soit x_{k+1} une racine de P, distincte des précédentes.

  Alors $$\mathrm{P}(x_{k+1}) = 0 = (x_{k+1} - x_1) \ldots (x_{k+1} - x_k)\mathrm{Q}(x_{k+1})$$

  Comme nous sommes dans un corps, si un produit est nul alors l'un des facteurs est nul. Or par hypothèse x_{k+1} est distinct des précédentes racines de P, c'est-à-dire que les termes $x_{k+1} - x_i$ sont non nuls. Donc $\mathrm{Q}(x_{k+1}) = 0$, et donc x_{k+1} est racine de Q. On peut donc factoriser Q par $\mathrm{X} - x_{k+1}$, et donc P se factorise par le produit $(\mathrm{X} - x_1) \ldots (\mathrm{X} - x_{k+1})$.

Si l'on prend le polynôme P de degré n, si $x_1, \ldots, x_n$ sont des racines de P, alors P se factorise par le produit $(\mathrm{X} - x_1) \ldots (\mathrm{X} - x_n)$, lui-même de degré n. On en conclut que P est de la forme $a(\mathrm{X} - x_1) \ldots (\mathrm{X} - x_n)$, où a est une constante non nulle (a est le coefficient dominant de P). Les racines de P sont alors exactement les nombres $x_1, \ldots, x_n$, et donc P a au plus n racines. En effet, si x est racine de P, on a :

$$a(x - x_1) \ldots (x - x_n) = 0$$

et donc l'un des termes $x - x_i$ est nul (même argument : dans un corps, il n'y a pas de diviseurs de 0). C'est-à-dire que x est l'un des nombres x_i ($i \leq n$). □

Combinant ces résultats avec notre théorème principal (tout polynôme a une racine dans $\mathbb{C}$), on obtient la propriété suivante :

Propriété 5 *Tout polynôme est scindé sur $\mathbb{C}$, c'est-à-dire peut s'écrire comme un produit de polynômes de degré 1.*

En effet, un polynôme non constant P a une racine a. Mais alors, on peut factoriser P sous la forme d'un produit $(\mathrm{X} - a)\mathrm{Q}$. Et l'on recommence avec Q, jusqu'à obtenir un polynôme constant. Enfin, on peut exprimer la clôture algébrique sous la forme :

Théorème 6 *Soit n un entier naturel non nul. Tout polynôme complexe de degré n admet exactement n racines (en tenant compte des multiplicités).*