Le théorème fondamental de l'algèbre

Définition. Un polynôme $P \in \mathbb{K}[X]^*$ est dit **irréductible** si les seuls diviseurs de P sont soit des constantes, soit des multiples de P.

Il est immédiat que tout polynôme peut s'écrire comme un produit de polynômes irréductibles ; si P n'est pas sous forme de produit irréductibles, c'est qu'il peut s'écrire comme $P = F_1F_2$, avec $\deg(F_i) < \deg(P)$. En procédant donc à un argument de récurrence sur le degré du polynôme P, on peut par suite écrire les F_i sous forme irréductibles, ce qui conduit finalement à l'écriture de P comme un produit d'irréductibles.
Il se trouve que si $\mathbb{K} = \mathbb{C}$, la situation est particulièrement simple. Pour commencer, on va interpréter un élément de $\mathbb{C}[X]$ comme une fonction de $\mathbb{C}$ dans $\mathbb{C}$. Posons la

Définition. Une **suite complexe** est une fonction de $\mathbb{N}$ dans $\mathbb{C}$. On notera $\{z_n\}_{n\in\mathbb{N}}$ les éléments de la suite.
Une suite complexe $\{z_n\}_{n\in\mathbb{N}}$ **converge** vers un nombre complexe z ssi la suite des partie réels, respectivement des parties imaginaires, de $\{z_n\}_{n\in\mathbb{N}}$ converge vers la partie réelle, respectivement la partie complexe, de z.
Une fonction complexe $f : \mathbb{C} \to \mathbb{C}$ est dite **continue** en z_0 ssi $\lim_{n\to\infty} f(z_n) = f(z_0)$ pour toute suite complexe $\{z_n\}_{n\in\mathbb{N}}$ telle que $\lim_{n\to\infty} z_n = z_0$.

Il est facile de vérifier, que la limite de la somme de deux suites complexes convergentes est la somme de leur limite et que la limite du produit de deux suites complexes est le produit de leur limites. La somme ou le produit de deux fonctions complexes et continues et encore une fonction complexe continue. On a alors le

Lemme. Tout polynôme $P \in \mathbb{C}[X]$ est une fonction complexe continue. Similairement, la fonction $z \mapsto |P(z)|$ est continue.
De plus, si $P(Z) = a_nZ^n + \ldots + a_0$ et si $|z| \geq R$, avec $R = 1 + 2n \max_{0\leq k\leq n-1}\{|a_k|\}$, alors

$$|P(z)| \geq |z|^n \frac{|a_n|}{2}.$$

Démonstration. Comme un polynôme est une somme de monômes, il est suffisant de montrer, que $z \mapsto z^n$ est une fonction continue pour tout $n \in \mathbb{N}$. Or, z^n est n fois le produit de z avec lui-même, et il suffit alors de remarquer, que $z \to z$ est continue.
Clairement, $\lim_{n\to\infty} z_n = z$ ssi $\lim_{n\to\infty} \overline{z_n} = \overline{z}$, ce qui implique, que $z \mapsto \overline{z}$ est continue. De plus, $z \mapsto \overline{P(z)}$ est une somme de fonctions continue est donc elle-même continue. Puis, $|P(z)|^2 = \overline{P(z)}P(z)$ est continue et $|P(z)| = \sqrt{|P(z)|^2}$ l'est conséquemment aussi.
Si $P(z) = \sum_{k=0}^n a_kz^k$ alors on a pour $z \neq 0$,

$$|P(z)| = |z|^n|a_n - \sum_{k=0}^{n-1}(-a_k)z^{k-n}| \geq |z|^nK(z),$$

où $K(z) = |a_n| - \sum_{k=0}^{n-1}|a_k|\,|z|^{k-n}$. Dans la somme qui suit $|a_n|$ dans la définition de $K(z)$, on voit que les puissances de $|z|$ sont toutes négatives. Ainsi, si $|z|$ est suffisamment grand, i.e. pour $|z| > R$ donné dans l'énnoncé de ce lemme, $K(z) \geq \frac{|a_n|}{2}$ et $|P(z)| \geq |z|^n \frac{|a_n|}{2}$. $\square$

Théorème. Soit $P = a_n z^n + \ldots + a_0 \in \mathbb{C}[z]$. Alors, $|P(z)|$ atteint un minimum pour un certain z_0, i.e.

$$\exists z_0 \in \mathbb{C} \text{ tel que } \forall z \in \mathbb{C}, |P(z_0)| \leq |P(z)|.$$

Démonstration. Posons

$$m := \inf\{|P(z)| \text{ t.q. } z \in \mathbb{C}\}.$$

D'après le lemme précédent, $|P(z)| \geq |z|^n \frac{|a_n|}{2}$, si $|z| > R$ avec un R judicieusement choisi

Si $|P(0)| = 0$, alors on pose $z_0 = 0$ et le théorème est prouvé. Sinon, on choisit $R' := \max\{R, \left(\frac{2}{|a_n|}|P(0)|\right)^{1/n}\}$, et on saura que si $|z| > R'$, alors $|P(z)| \geq |P(0)|$. Ainsi,

$$m := \inf\{|P(z)|\, z \in \mathbb{C}\} = \inf\{|P(z)|\, |z| \leq R'\}.$$

Par définition de l'infimum, il existe pour tout $k \in \mathbb{N}^*$ un z_k tel que $|P(z_k)| - m < \frac{1}{k}$. Ecrivons $z_k = [r_k, \varphi_k]$. Comme $0 \leq r_r \leq R'$, il existera une ss-suite z_j de z_k telle que r_j converge vers un $r \leq R'$. Puis, il existera dans cette ss-suite une ss-suite z_l telle que les φ_l convergent vers un φ. On aura donc que $\lim_{l\to\infty}[r_l, \varphi_l] = [r, \varphi] \equiv z_0$ et $m = \lim_{l\to\infty} |P(z_l)| = |P(\lim_{l\to\infty} z_l)| = |P(z_0)|$. $\square$

Théorème. Si $P \in \mathbb{C}[z]$ et $\deg(P) = n \geq 1$, alors il existe un $z \in \mathbb{C}$ tel que $P(z) = 0$.

Démonstration. Par le théorème précédant, on sait que qu'il existe un $z_0 \in \mathbb{C}$ tel que pour tout nombre complexe z, $|P(z)| \geq |P(z_0)| = m$. Supposons que $|P(z_0)| \neq 0$. On pose alors $Q(z) := P(z + z_0) = b_0 + b_k z^k + \ldots + b_n z^n$ avec $b_k \neq 0$. De plus, $|b_0| = m$. Posons encore $c \in \mathbb{C}$ tel que $c^k = -b_0/b_k$ et $f(t) := |Q(ct)|$ où t est un paramètre réel. On a

$$f(t) = |b_0 - b_0 t^k + c_{k+1} t^{k+1} + \ldots + c_n t^n|,$$

avec $c_j = b_j c^j$. Si $0 < t < 1$, on estime que

$$f(t) \leq m(1 - t^k) + t^{t+1}|c_{k+1} + \ldots + c_n t^{n-k-1}| \leq m + t^k(-m + Nt),$$

avec $N = |c_{k+1}| + \ldots + |c_n|$. Si on choisit maintenant $t < \min\{1, \frac{m}{2N}\}$, on aura que $f(t) < m$, et on en conclut, que $f(t) = |Q(ct)| = |P(z_0 + ct)| < m$, ce qui est une contradiction. D'où $P(z_0) = 0$. $\square$

Une conséquence très importante de ce dernier théorème est le

Théorème fondamental de l'algèbre. Soit $P(z) = a_n z^n + \ldots + a_0 \in \mathbb{C}[Z]$ et $n > 0$. Alors, il existe k nombres complexes $r_1, \ldots, r_k$ et k entiers naturels non nuls $n_1, \ldots, n_k$, tels que $n_1 + \ldots + n_k = n$ et tels que

$$P(z) = a_n (z - r_1)^{n_1} \ldots (z - r_k)^{n_k}.$$

Démonstration. On procède par récurrence sur le degré de $P(z)$.
Si $n = 1$, $P(z) = a_1 z + a_0$, avec $a_1 \neq 0$, et $P(z) = a_1(z - \frac{a_0}{a_1})$.
Supposons le résultat vérifié pour n et soit $P(z) = a_{n+1} z^{n+1} + \ldots + a_0$, un polynôme à coefficients complexes d'ordre $n+1$. Par le théorème précédent, il existe un nombre z_0, tel que $P(z_0) = 0$. Une division euclidienne nous livre alors

$$P(z) = M(z)(z - z_0) + R,$$

où R est un nombre complexe. Puisque $P(z_0) = 0$, il faut que $R = 0$, et ainsi, $P(z) = M(z)(z - z_0)$. Le degré de $M(z)$ étant égal à n, on a par l'hypothèse de récurrence, que $M(z) = m_n(z - r_1)^{n_1} \ldots (z - r_k)^{n_k}$ et $n_1 + \ldots + n_k = n$. De plus, il est facile de voir, que $m_n = a_n$. Ainsi, $P(z) = a_n(z - z_0)(z - r_1)^{n_1} \ldots (z - r_k)^{n_k}$. $\square$