Th. de D'Alembert-Gauss ~ Preuves

⚠ On confond abusivement $P \in \mathbb{C}[X]$ avec $\tilde{P} : \mathbb{C} \to \mathbb{C}$ la fonc$^{\underline{n}}$ poly. correspondante.

Démo. 1

1| Soit $P(X) = \sum_{k=0}^{n} p_k X^k \in \mathbb{C}_{\geq 1}[X]$ ($\deg P = n \geq 1$).

Mq $\inf_{\mathbb{C}} |P(z)| = \min_{\mathbb{C}} |P(z)|$.

- $|P(z)| \geq \underbrace{|p_n z|^n}_{\text{Terme dominant!}} - \sum_{k=0}^{n-1} |p_k z^k|$ clairem$^{\underline{t}}$, donc sur $\mathbb{C}^*$, on a :

$$|P(z)| \geq |z|^n \Big(\underbrace{|p_n| - \sum_{k=0}^{n-1} |p_k| \cdot |z|^{\overbrace{k-n}^{<0}}}_{\xrightarrow[|z| \to +\infty]{} |p_n| \neq 0} \Big)$$

On sait donc que $\underbrace{\lim_{|z| \to +\infty} |P(z)| = +\infty}$.

À mettre en regard avec la preuve via le th. de Liouville holomorphe.

- Soit alors $R > 0$ tq $|z| > R$ implique $|P(z)| \geq |P(0)|$ clairem$^{\underline{t}}$, $\inf_{\mathbb{C}} |P(z)| = \inf_{|z| \leq R} |P(z)|$.

Or $D_{\mathbb{C}}(0; R]$ est compact (fermé borné), et $P : \mathbb{C} \to \mathbb{C}$ est continue, donc on arrive à

$$\begin{aligned} \inf_{\mathbb{C}} |P(z)| &= \inf_{|z| \leq R} |P(z)| \\ &= \min_{|z| \leq R} |P(z)| \\ &= \min_{\mathbb{C}} |P(z)| \end{aligned}$$

$|P(z)| \geq |P(0)|$ si $|z| \geq R$.

2| Le point précédent donne $z_0 \in \mathbb{C}$ tq $|P(z_0)| = \inf_{\mathbb{C}} |P(z)|$ dès que $P(X) \in \mathbb{C}_{\geq 1}[X]$.

Posant $Q(X) = P(X + z_0)$, on voit que l'on se ramène au cas où $z_0 = 0$.

3) Soit donc $P(X) = \sum_{k=0}^{n} p_k X^k \in \mathbb{C}_{\geq 1}[X]$ tel que $|p_0| = |P(0)| = \inf_{\mathbb{C}} |P(z)|$.

Montrons par l'absurde que $P(0) = 0$.

- $P(X) = p_0 + p_k X^k + \sum_{j=k+1}^{n} p_j X^j$
$= p_0 + p_k X^k + X^{k+1} P_1(X)$

On isole p_0. On considère la valeur de $P(X) - p_0$.

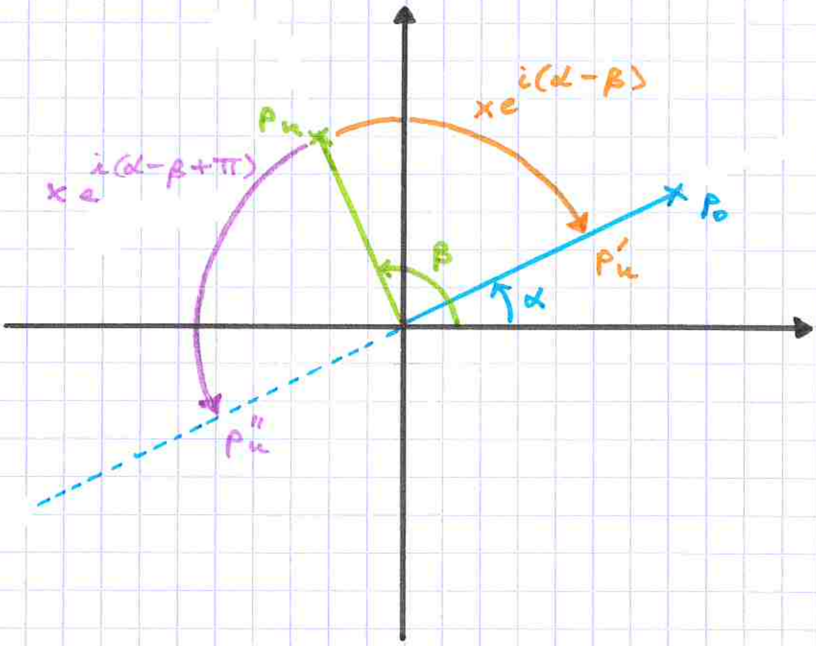
Ici $k = n$, ie $P_1 = 0$, est possible.

- <u>Cas 1</u> : $P_1 = 0$, ie $P(X) = p_0 + p_n X^n$, où $p_0 \neq 0$ (on raisonne par l'absurde).

↳ $P(re^{i\theta}) = p_0 + p_n r^n e^{in\theta}$ où $(r;\theta) \in \mathbb{R}_+^* \times \mathbb{R}$.

↳ $p_0 = |p_0| e^{i\alpha}$ et $p_n = |p_n| e^{i\beta}$

↳ Prenons de la hauteur de vue.



Aller en p_n' : mauvais choix car $P(re^{i\theta})$ va "s'éloigner" de p_0, mais on a quand même un module facile à calculer.

Aller en p_n'' : on se "rapproche" de p_0 avec un module facile^t calculable.

↳ On choisit $n\theta = \alpha - \beta + \pi$, c'est-à-dire $\theta = \dfrac{\alpha - \beta + \pi}{n}$, ainsi que r assez petit pour avoir $|p_n''| \times r^n < |p_0|$. On a alors (cf. dessin) :

$$|P(re^{i\theta})| = |p_0| - |p_n r^n e^{in\theta}|$$
$$< |p_0|$$

On a une contradiction !

- $\underline{\text{Cas 2}}$: $P_1 \neq 0$

Le cas 1 donne $r_0 \in \mathbb{R}_+^*$ tq $0 \leq r \leq r_0$ implique

$$|P(re^{i\theta})| \leq |p_0| - |p_k| \cdot r^k + r^{k+1} |P_1(re^{i\theta})|$$

(via la classique inégalité triangulaire).

Ceci se réécrit :

$$|P(re^{i\theta})| \leq \underbrace{|p_0| - r^k \big(\underbrace{|p_k| - r\,|P_1(re^{i\theta})|}_{\xrightarrow[r \to 0]{} |p_k|} \big)}_{\xrightarrow[r \to 0]{} |p_0|^-}$$

On peut donc trouver $r \in \,]0 ; r_0[$ tq $|P(re^{i\theta})| < |p_0|$, d'où une contradiction finale !

Démo. 2

1) On commence comme dans la preuve 1 pour arriver au cas où $P(X) = \sum_{k=0}^{n} p_k X^k \in \mathbb{C}_{\geq 1}[X]$ tq $|P(0)| = \inf_{\mathbb{C}} |P(z)|$.

2) Mq par l'absurde que $P(0) = 0$.

- $P(X) = p_0 \left(1 + \frac{p_k}{p_0} X^k + X^{k+1} P_1(X) \right)$ où $p_k \neq 0$ avec éventuellement $P_1 = 0$.

- Soit w une racine k-ième de $-\frac{p_0}{p_k} \neq 0$. Pour $t \in \mathbb{R}$, on a :
$P(wt) = p_0 (1 - t^k + t^k . t Q(t))$ où $Q(X) \in \mathbb{C}[X]$.
On choisit $t > 0$ tq $|t Q(t)| < 1$ et $t < 1$, on a :

$$\begin{aligned} |P(wt)| &\leq |p_0| \left(|1 - t^k| + |t Q(t) . t^k| \right) \\ &< |p_0| (1 - t^k + t^k) \\ &= |p_0| \end{aligned}$$

on a une contradiction !

Démo. 3

1/ On va utiliser les ingrédients "algébriques" suivants.

a/ $\mathbb{R}$ est un corps ordonné tq $\mathbb{R}_+ = {}^2\mathbb{R}$ (ens. des carrés de $\mathbb{R}$). ⓘ On parle de corps euclidien.

b/ $\forall P \in \mathbb{R}[X]$ tq $\deg P \in 2\mathbb{N}+1$, il existe $\alpha \in \mathbb{R}$ tq $P(\alpha) = 0$.

2/ $\forall P(X) \in \mathbb{C}_2[X]$, $P(z) = 0$ admet "deux" sol. dans $\mathbb{C}$.

- $az^2 + bz + c = 0 \iff a\left(z + \frac{b}{2a}\right)^2 = \frac{\Delta}{4a^2}$ où $\Delta = b^2 - 4ac$.
- $\forall \alpha + i\beta \in \mathbb{C}$, $(\alpha + i\beta)$ admet deux racines carrées.

$\hookrightarrow (x+iy)^2 = \alpha + i\beta$

$$\iff \begin{cases} x^2 - y^2 = \alpha \\ 2xy = \beta \end{cases}$$

$\hookrightarrow \beta = 0$

On a ici $xy = 0$ et $\alpha = x^2 - y^2$.

Si $\alpha \geq 0$, $y = 0$ et $x = \pm\sqrt{\alpha}$.

Si $\alpha < 0$, $x = 0$ et $y = \pm\sqrt{-\alpha}$.

$\hookrightarrow \beta \neq 0$

On doit avoir :

$$x^2 - \left(\frac{\beta}{2x}\right)^2 = \alpha$$

$$\iff x^4 - \alpha x^2 - \left(\frac{\beta}{2}\right)^2 = 0$$

$\tilde{\Delta} = \alpha^2 + \beta^2 > 0$ donne :

$$x^2 = \frac{1}{2}\left(\alpha \pm \sqrt{\alpha^2+\beta^2}\right)$$

$\alpha^2 + \beta^2 > \alpha^2$

$\Rightarrow \sqrt{\alpha^2+\beta^2} > |\alpha| \geq \alpha$

On a aussi : $\sqrt{\alpha^2+\beta^2} > -\alpha$

$$\Rightarrow x^2 = \frac{1}{2}\left(\alpha + \sqrt{\alpha^2+\beta^2}\right) > 0$$

$$\Rightarrow y^2 = \frac{1}{2}\left(-\alpha + \sqrt{\alpha^2+\beta^2}\right) > 0$$

Notant $x_+ = \sqrt{\dfrac{\alpha + \sqrt{\alpha^2+\beta^2}}{2}}$, $y_+ = \sqrt{\dfrac{-\alpha + \sqrt{\alpha^2+\beta^2}}{2}}$,
les deux racines carrées complexes de $\alpha + \beta i$ sont

- les deux pts précédents permettent de conclure.

3] $\forall P(X) \in \mathbb{R}_{\geq 1}[X]$, $\exists \alpha \in \mathbb{C}$ tq $P(\alpha) = 0$. Notant $n = \deg P$, on va raisonner par récurrence sur $v_2(n)$ la valua° 2-adique de n, ie $n = 2^{v_2(n)} m$ où $m \in 2\mathbb{N}+1$ (cf. 1-b !).

- Initialisa° : $v_2(\deg P) = 0$
c'est la prop. 1-b.

- Hérédité : on suppose que tt polyg. réel de degré d tq $v_2(d) = k$ admet une racine complexe.
On considère $P(X) \in \mathbb{R}[X]$ avec $v_2(\deg P) = k+1$, ie $\deg P = 2^{k+1} m$ avec $m \in 2\mathbb{N}+1$.

↳ On note E un corps de décomposi° de P (facile à construire via $K[X]/(\tilde{P}(X))$ où $\tilde{P}$ est irréduc.)
On a donc $P(X) = p_n \prod_{1 \leq k \leq n} (X - x_i)$ où $n = \deg P$, les x_i appartenant à E, et $p_n \in \mathbb{R}$ est le coef. domi. de P.

↳ $\forall c \in \mathbb{R}$, on pose :
$$Q_c(X) = \prod_{1 \leq i < j \leq n} (\underbrace{X - x_i - x_j - c x_i x_j}_{\text{Formule sym. paramétrée par } c.})$$

$$\deg Q_c = \sum_{k=1}^{n-1} k = \frac{n(n-1)}{2} = 2^k m (2^{k+1} m - 1)$$
donc $v_2(\deg Q_c) = k$.

↳ $\forall c \in \mathbb{R}$, $Q_c(X) \in \mathbb{R}[X]$.

En effet, les coef. de Q_c sont des poly. sym. des x_i, donc ils s'expriment tous comme des poly. de $\tilde{k}$-ième poly. sym. en les x_i, ceux-ci étant "directement" liés aux coef. de P (immédiat pour ce dernier point).

↳ L'hyp. de récur. s'applique à Q_c qui a donc une racine complexe α_c donc $\exists (i_c, j_c)$ tq $x_{i_c} + y_{j_c} + c\, x_{i_c} y_{j_c} \in \mathbb{C}$.

Clairement, on a $(c, d) \in \mathbb{R}^2$ tq $(i_c, j_c) = (i_d, j_d)$ avec $c \neq d$

puis $x_{\tilde{i}} + y_{\tilde{j}} + c\, x_{\tilde{i}} y_{\tilde{j}} \in \mathbb{C}$,

et $x_{\tilde{i}} + y_{\tilde{j}} + d\, x_{\tilde{i}} y_{\tilde{j}} \in \mathbb{C}$ (où $\tilde{i} = i_c$, $\tilde{j} = j_c$).

$c \neq d$ donne $(c-d)\, x_{\tilde{i}} y_{\tilde{j}} \in \mathbb{C}$ puis

$x_{\tilde{i}} y_{\tilde{j}} \in \mathbb{C}$, et ensuite $x_{\tilde{i}} + y_{\tilde{j}} \in \mathbb{C}$

↳ $x_{\tilde{i}} y_{\tilde{j}} \in \mathbb{C}$ et $x_{\tilde{i}} + y_{\tilde{j}} \in \mathbb{C}$ donne $x_{\tilde{i}}$ et $y_{\tilde{j}}$ sont rac. d'un trinôme complexe du 2^{e} degré.

Le point 2 donne $(x_{\tilde{i}}, y_{\tilde{j}}) \in \mathbb{C}^2$ puis $\alpha = x_{\tilde{i}} + y_{\tilde{j}} + c\, x_{\tilde{i}} y_{\tilde{j}} \in \mathbb{C}$ une racine complexe de P. CQFD !

(i) On comprend ici le choix de $x_i + x_j$ et $x_i x_j$. Par contre, $c(x_i + x_j) + x_i x_j$ fait aussi l'affaire.

4) $\forall P \in \mathbb{C}_{n}[X]$, $\exists \alpha \in \mathbb{C}$ tq $P(\alpha) = 0$.

- $R(X) = P(X) \cdot \overline{P}(X) \in \mathbb{R}[X]$ si l'on note $\overline{P}(X) = \sum_{k=0}^{n} \overline{p_k}(X)$.

- $\alpha \in \mathbb{C}$ annule $R(X) \Rightarrow \alpha$ annule $P(X)$ ou $\overline{P}(X)$.
$\Rightarrow \alpha$ ou $\overline{\alpha}$ annule $P(X)$

QUELQUES REMARQUES

- Un corps vérifiant 1-a et 1-b est dit réel clos. Un tel corps $\mathbb{K}$ est caractérisé de façon équivalente par l'une des prop. suivantes.

Deux déf. algébriques !

α/ $-1 \notin {}^2\mathbb{K}$ et $\mathbb{K}(i)$ est alg. clos où i est une rac. de X^2+1 (dans un corps de rupture de X^2+1).

β/ La clôture alg. de $\mathbb{K}$ est une ext. finie propre.

γ/ $\mathbb{K}$ admet un ordre pour lequel le th. des val. intermédiaires "polynomial" est vrai.

- La démo. 3 s'applique à $\forall$ corps réel clos en remplaçant $\mathbb{R}$ et $\mathbb{C}$ par $\mathbb{K}$ et $\mathbb{K}(i)$.

- <u>Th. Artin-Schreier</u> : $\forall$ corps totalement ordonné ($\mathbb{K}$) admet une ext. alg. réelle close avec un ordre prolongeant celui de $\mathbb{K}$.

Une preuve algo. de 1980 existe aussi.

Via ce th. et la théorie des modèles des corps ordonnés, il est "simple" de résoudre le 17ième pb de Hilbert.

<u>17e pb de Hilbert</u> : si $F(X) \in \mathbb{R}(X)$ vérifie $\forall x \in \mathbb{R}$, $F(x) \geq 0$, alors F est une somme de carrés de $F(X)$.

Démo. 4

1) Th. Liouville (AC)

f entière et bornée sur $\mathbb{C}$

$\Rightarrow$ f cte

ⓘ Si f entière vérifie $\forall z \in \mathbb{C}$, $|f(z)| \leq A + B|z|^k$ où $k \in \mathbb{N}$, alors $f \in \mathbb{C}_{\leq k}[X]$.

2) Si $P(X) \in \mathbb{C}[X]$ ne s'annule pas sur $\mathbb{C}$, alors $\frac{1}{P}$ est entière et bornée, d'où $P = $ Cte !