LES BEAUX THEOREMES DE SUP

ET MÊME LES AUTRES

Toute suite réelle croissante majorée converge vers son plus petit majorant.

Soit (a_n) une suite réelle croissante *($a_{n+1} \geqslant a_n$ pour tout n)*, majorée par un certaint M *($\forall n \in \mathbb{N},\ a_n \leqslant M$)*.
On notera que M est un majorant de la suite *(mais pas forcément "le meilleur", il n'a donc aucune raison d'être la limite μ de la suite, celle ci sera inférieure ou égale à M).*
On pose $A = \{a_n \mid n \in \mathbb{N}\}$ *(ensemble des valeurs prises par la suite, projection sur l'axe Oy).*
C'est une partie de $\mathbb{R}$ *(suite réelle)*, non vide *(on y trouve a_0)* et majorée *(par M).*
Elle admet donc un "**plus petit majorant**" ou "**borne supérieure**" *(axiomatique de $\mathbb{R}$).* On le note μ.

On va montrer que (a_n) converge vers μ avec la définition en $\forall\varepsilon, \exists N_\varepsilon$.
On se donne ε strictement positif.
Alors $\mu - \varepsilon$ n'est plus un majorant de A *(car plus petit que le plus petit majorant).*
Il existe donc au moins un élément de A entre $\mu - \varepsilon$ et μ. Un tel élément sera un certain a_N pour un certain entier N.
On constate qu'on a alors pour tout n plus grand que N : $\mu - \varepsilon \leqslant a_N \leqslant a_n \leqslant \mu \leqslant \mu + \varepsilon$ *(en utilisant : ce qu'on sait de a_N, la croissance de la suite, que μ majore et enfin que ε est positif).*
On a obtenu : $\forall\varepsilon > 0,\ \exists N \in \mathbb{N},\ \forall n \in \mathbb{N},\ n \geqslant N \Rightarrow |a_n - \mu| \leqslant \varepsilon$, c'est bien la convergence de la suite vers μ.

Dans un groupe, le neutre est unique, et chaque élément n'a qu'un symétrique.

Soit $(E, *)$ un groupe *(pas forcément commutatif).*
On suppose que deux éléments e et ε tiennent le rôle de neutre *(à droite comme à gauche) (objectif : $e = \varepsilon$).*
On calcule alors $e * \varepsilon$. On a $e = e * \varepsilon = \varepsilon$ car ε est neutre et e est neutre.
Par transitivité de l'égalité, on a $e = \varepsilon$.
Il n'est pas judicieux dans cette démonstration de faire intervenir d'autre élément du groupe E. De plus, il faut avoir prouvé l'unicité du neutre avant de parler de symétriques.
On suppose que deux éléments α et β tiennent le rôle de symétrique d'un élément a de E *(objectif : $\alpha = \beta$).*
On calcule alors $\alpha * a * \beta$ en expoitant l'associativité :
$\alpha * a * \beta = (\alpha * a) * \beta = e * \beta = \beta$
$\alpha * a * \beta = \alpha * (a * \beta) = \alpha * e = \alpha$
Par transitivité de l'égalité, on a $\alpha = \beta$.
On notera qu'il s'agit de preuves directes et non pas de raisonnements par l'absurde ; on prend deux éléments répondant à la définition et on montre que c'est le même.

Toute suite convergente est bornée.

On prend une suite (a_n), convergente de limite α.
La définition est $\forall \varepsilon > 0,\ \exists N_\varepsilon \in \mathbb{N},\ \forall n \in \mathbb{N},\ n \geqslant N_\varepsilon \Rightarrow |a_n - \alpha| \leqslant \varepsilon$.
En particulier, à partir du rang N_1, on a $|a_n - \alpha| \leqslant 1$. Par inégalité triangulaire $|a_n| \leqslant |a_n - \alpha| + |\alpha| \leqslant 1 + |\alpha|$.
La suite est donc bornée à partir du rang N_1 par $1 + |\alpha|$. Or, avant, il n'y a qu'un nombre fini de termes.
Globalement, la suite est bornée par $Max(|a_0|,\ |a_1|, \ldots |a_{N_1-1}|,\ 1 + |\alpha|)$.

L'intersection de sous-groupes d'un groupe $(G, *)$ est encore un sous-groupe de $(G, *)$.

On commence, même si c'est inutile par le cas de deux sous-groupes A et B.
On suppose donc que A et B sont deux sous groupes de $(G, *)$ *(inclusion, stabilité, présence du neutre, passage au symétrique).*
On montre que $A \cap B$
• est inclus dans G car A et B le sont,
• contient le neutre n de $(G, *)$ car n est à la fois dans A et dans B,
• est stable par composition :
on prend x et y dans $A \cap B$; comme x est dans A et y aussi, le "produit" $x * y$ est dans A *(stabilité de A)* ; comme x est dans B et y aussi, le produit $x * y$ est dans le sous-groupe B ; on reconnaît que $x * y$ est dans $A \cap B$,
• est stable par passage au symétrique :
on prend x dans $A \cap B$; comme il est dans le sous-groupe A, x^{-1} est dans A ; comme x est dans B, son symétrique x^{-1} est dans B ; on reconnaît que x^{-1} est dans $A \cap B$.

On passe au cas d'un nombre quelconque (même infini) *de sous-groupes A_i pour i décrivant un ensemble d'indexation I.*
On rappelle $\bigcap_{i \in I} A_i = \{x \in G \mid \forall i \in I,\ x \in A_i\}$.
• Par construction, $\bigcap_{i \in I} A_i$ est une partie de G.
• Chaque A_i est un sous-groupe de $(G, *)$, le neutre n de G en fait partie ; il est donc dans l'intersection.
• On prend x et y tous deux dans $\bigcap_{i \in I} A_i$. Pour chaque i de I, x est dans A_i et y est dans A_i. Comme chaque A_i est un sous-groupe de $(G, *)$, le "produit" $x * y$ est dans A_i. Comme $x * y$ est dans tous les A_i, il est dans $\bigcap_{i \in I} A_i$.
• On prend x dans $\bigcap_{i \in I} A_i$. Par définition, pour tout i, x est dans A_i. Comme chaque A_i est un sous-groupe de $(G, *)$, le symétrique x^{-1} est dans A_i. Comme ceci est vrai pour tout i, x^{-1} est dans $\bigcap_{i \in I} A_i$.

Intégration par parties : si u et v sont deux applications de classe C^1[a] de $[a,\ b]$ dans $\mathbb{R}$ (ou même $\mathbb{C}$), alors on a

$$\int_a^b u'(t).v(t).dt = \Big[u(t).v(t)\Big]_{t=a}^{t=} - \int_a^b u(t).v'(t).dt.$$

[a] applications dérivables dont les dérivées sont aussi continues

On écrit $\int_a^b u'(t).v(t).dt = \int_a^b \Big(u'(t).v(t) + u(t).v'(t)\Big).dt - \int_a^b u(t).v'(t).dt$.
Le terme $\int_a^b \Big(u'(t).v(t) + u(t).v'(t)\Big).dt$ est de la forme $\int_a^b f'(t).dt$ avec $f = u.v$. Il se calcule en $\Big[f(t)\Big]_{t=a}^{t=b}$.

Toute application numérique continue sur un segment est bornée et atteint ses bornes.

On prend donc f continue de $[a,\ b]$ *(segment de* $\mathbb{R}$*)*, dans $\mathbb{R}$.
On va montrer déjà de deux façons qu'elle est majorée.
En appliquant ensuite le raisonnement à $-f$, on montrera ensuite qu'elle est bornée. A moins que vous ne préfériez l'appliquer à $|f|$ tout de suite.

Méthode utilisant le théorème de Bolzano Weierstrass.
On va établir : $\exists M \in \mathbb{R},\ \forall x \in [a,\ b],\ f(x) \leqslant M$ **par l'absurde**.
On suppose donc $\forall M \in \mathbb{R},\ \exists x \in [a,\ b],\ f(x) > M$.
En particulier pour tout n de $\mathbb{N}$, il existe un x de $[a,\ b]$ vérifiant $f(x) > n$. On en prend un qu'on nomme u_n.
On a ainsi construit une suite (u_n) de $[a,\ b]$ vérifiant $f(u_n) > n$ pour tout n.
C'est une suite réelle *(on est dans* $[a,\ b]$*)*, bornée *(par* a *et* b*)*.
Elle admet donc au moins une sous-suite $(u_{\varphi(n)})$ qui converge *(vers une limite réelle qu'on va noter* α*)*.
Comme pour tout n on a $a \leqslant u_{\varphi(n)} \leqslant b$, alors par passage *(large)* à la limite, α est dans $[a,\ b]$.
Comme f est continue en tout point de $[a,\ b]$, elle l'est en particulier en α et on a donc $f(u_{\varphi(n)}) \to_{n\to+\infty} f(\alpha)$.
Mais dans le même temps, la minoration $f(u_{\varphi(n)}) \geqslant \varphi(n) \geqslant n$ donne $f(u_{\varphi(n)}) \to_{n\to+\infty} +\infty$.
On tient notre contradiction.

Méthode utilisant juste le principe de la borne supérieure.
Pour tout n, on pose $A_n = \{x \in [a,\ b] \mid f(x) \geqslant n\}$ *(les points dont l'image dépasse* n*)*.
Chaque A_n est une partie de $\mathbb{R}$, majorée par b.
Si chacune est non vide *(c'est que que commence la preuve par l'absurde)*, alors chacune admet une borne supérieure *(plus petit majorant)*, que l'on note α_n.
Par continuité de f, chaque borne supérieure α_n est dans son A_n.
On étudie la limite à droite en α_n, comme les x plus grands que α_n sont hors de A_n, ils vérifient $f(x) < n$ et par passage à la limite, $f(\alpha_n) \leqslant n$. On étudie la limite à gauche en α_n, comme c'est la borne supérieure de A_n, il existe des éléments x de A_n inférieurs ou égaux à α_n vérifiant $f(x) \geqslant n$, et par passage à la limite, $f(\alpha_n) \geqslant n$. Par antisymétrie, $f(\alpha_n) = n$.
Comme A_{n+1} est inclus dans A_n, tout majorant de A_n est un majorant de A_{n+1}.
En particulier α_n est un majorant de A_{n+1}, et donc le plus petit majorant α_{n+1} est plus petit que α_n.
La suite (α_n) est donc décroissante.
Elle est minorée par a puisque tous les α_n sont dans $[a,\ b]$.
En tant que suite décroissante minorée, elle admet une borne inférieure que l'on va noter β.
Comme tous les α_n vérifient $a \leqslant \alpha_n \leqslant b$, la limite β est dans $[a,\ b]$.
Par continuité de f en β : $f(\alpha_n) \to_{n\to+\infty} \beta$.
Mais on avait $f(\alpha_n) \geqslant n$ pour tout n, et donc par minoration $f(\alpha_n) \to_{n\to+\infty} +\infty$.
On tient notre contradiction.
C'est donc qu'au moins un des A_n est vide, pour un certain entier N.
Ayant $\{x \in [a,\ b] \mid f(x) \geqslant n\} = \emptyset$, on a bien $\forall x \in [a,\ b],\ f(x) < n$.

On sait maintenant que l'ensemble image $\{f(x) \mid x \in [a,\ b]\}$ *(noté* I*)* est une partie de $\mathbb{R}$ majorée *(et non vide)*.
On note μ sa borne supérieure *(plus petit majorant)*. On va montrer que cette borne supérieure est

atteinte, c'est à dire l'existance d'un γ de $[a,\ b]$ vérifiant $f(\gamma) = \mu$.
On se donne un entier naturel n. Par définition de "plus petit majorant", le réel $\mu - 2^{-n}$ n'est plus un majorant de I. Il existe donc au moins un élément x de $[a,\ b]$ vérifiant $\mu - 2^{-n} \leqslant f(x) \leqslant \mu$. On en note un c_n.
On a donc une suite (c_n) d'éléments de $[a,\ b]$ vérifiant $\mu - 2^{-n} \leqslant f(c_n) \leqslant \mu$ pour tout n.
Chaque c_n est dans $[a,\ b]$. On a donc une suite réelle bornée. On en extrait une sous-suite $(c_{\psi(n)})$ qui converge vers un certain γ *(qui est dans $[a,\ b]$ par passage à la limite sur "$a \leqslant c_n \leqslant b$ pour tout n").*
Par continuité de f en γ : $f(c_{\psi(n)}) \to_{n\to+\infty} f(\gamma)$.
Par encadrement dans $\mu - 2^{-\psi(n)} \leqslant f(c_{\psi(n)}) \leqslant \mu$, on a $f(c_{\psi(n)}) \to_{n\to+\infty} \mu$.
Par unicité de la limite : $f(\gamma) = \mu$.
La borne supérieure de f sur $[a,\ b]$ est un maximum, atteint.
On fait de même avec la borne inférieure.

Les sous-groupes de $(\mathbb{Z}, +)$ sont les ensembles de la forme $n.\mathbb{Z}$ (ensemble des multiples de n) pour n entier naturel.

Déjà, les ensembles de la forme $n.\mathbb{Z}$ sont bien des sous-groupes de $(\mathbb{Z}, +)$:
on se fixe n et on pose $n.\mathbb{Z} = \{n.p \mid p \in \mathbb{Z}\}$
• c'est une partie de $\mathbb{Z}$
• le neutre additf 0 y est, sous la forme $n.0$
• la somme de deux éléments de cet ensemble *($n.a$ et $n.b$)* est encore dans cet ensemble *(de la forme $n.(a+b)$ avec $a+b$ dans $\mathbb{Z}$)*
• l'opposé d'un élément de cet ensemble *(de la forme $n.a$)* est encore dans cet ensemble *(de la forme $n.(a-)$ avec $-a$ entier relatif)*.

On note que pour $n = 1$, l'ensemble $n.\mathbb{Z}$ est $\mathbb{Z}$ *(le plus grand)*, tandis que pour $n = 0$ c'est $\{0\}$ *(le plus petit)*.

On prend maintenant un sous-groupe G de $(\mathbb{Z}, +)$, il faut montrer que G est de la forme $n.\mathbb{Z}$ pour un n bien choisi.
Si G se réduit au seul neutre 0, c'est $0.\mathbb{Z}$ comme indiqué plus haut.
Sinon, il y a dans G au moins un élément non nul. Par stabilité par passage au symétrique si nécessaire, il y a dans G au moins un élément strictement positif.
On pose alors $P = G \cap \mathbb{N}^*$ *(les éléments strictement positifs de G)*.
C'est une partie de $\mathbb{N}$ non vide, comme on l'a dit plus haut.
Elle admet donc un plus petit élément.
On note celui ci n.
D'ores et déjà, en tant que plus petit élément de l'ensemble, n est dans P, donc dans G.
Par stabilité de G par addition, chaque nombre de la forme $n.a$ avec a dans $\mathbb{N}$ est dans G *(récurrence sur a)*.
Par passage à l'opposé, chaque élément de la forme $n.(-b)$ avec b dans $\mathbb{N}$ est dans G.
A ce stade, on a prouvé que G contient tous les $n.k$ avec k dans $\mathbb{Z}$: $n.\mathbb{Z} \subset G$.

Il nous manque l'autre inclusion. On prend N dans G.
On effectue la division euclidienne de N par n. Il existe deux entiers p et q vérifiant $N = n.q + r$ avec $0 \leqslant r < n$.
Mais alors on a $q = N - n.q$. Les deux entiers N et $n.p$ sont dans G *(hypothèse et résultat de la première inclusion)*. Par stabilité du sous-groupe G, la différence $N - n.q$ est aussi dans G.
Si cette différence est non nulle, c'est un élément de $G \cap \mathbb{N}^*$ strictement plus petit que n, ce qui contredit la définition de n.
Par élimination, l'entier r est nul.
On reporte : $N = n.p$, c'est un multiple de n.
On a cette fois $G \subset n.\mathbb{Z}$.La double inclusion donne l'égalité.

Noyau dit de Dirichlet : $\frac{1}{2}+\sum_{k=1}^{n}\cos(k.\theta)=\frac{\sin\left(\frac{2.n+1}{2}.\theta\right)}{2.\sin\left(\frac{\theta}{2}\right)}$ pour tout réel θ qui n'est pas multiple pair de π.

On prend θ qui n'appartient pas à $\{2.k.\pi \mid k\in\mathbb{Z}\}$ *(son cosinus ne vaut pas 1 et* $\sin(\theta/2)$ *est non nul).*
On part de la somme $\frac{1}{2}+\sum_{k=1}^{n}\cos(k.\theta)$ qu'on écrit $\frac{1}{2}+\sum_{k=1}^{n}\frac{e^{-i.k.\theta}+e^{i.k.\theta}}{2}$.
On met $\frac{1}{2}$ en facteur et on obtient $\frac{1}{2}\Big(\sum_{k=1}^{n}e^{-i.k.\theta}+1+\sum_{k=1}^{n}e^{i.k.\theta}\Big)$ qui donne même $\frac{1}{2}\Big(\sum_{k=-n}^{n}e^{i.k.\theta}\Big)$.
On reconnaît une série géométrique de premier terme $e^{-i.n.\theta}$, de terme à venir $e^{i.(n+1).\theta}$ et de raison $e^{i.\theta}$ *(différente de 1).*
On l'écrit donc $\frac{e^{-i.n.\theta}-e^{i.(n+1).\theta}}{2.(1-e^{i.\theta})}$.
On multiplie haut et bas par $e^{-i.\theta/2}$ et on a $\frac{e^{-i.(n+1/2).\theta}-e^{i.(n+1/2).\theta}}{2.(e^{-i.\theta/2}-e^{i.\theta/2})}$.
En utilisant $e^{-i.\alpha}-e^{i.\alpha}=-2.i.\sin(\alpha)$ on arrive à $\frac{2.\sin((n+1/2).\theta)}{4.\sin(\theta/2)}$.
Une autre preuve est possible par produit en croix, en utilisant $2.\sin(a).\cos(b)=\sin(a+b)-\sin(a-b)$ et une somme télescopique.

Inégalité de Markov : pour toute variable aléatoire A positive et tout réel a strictement positif : $P(A\geqslant a)\leqslant\frac{E(A)}{a}$.

Inégalité de Bienaymé-Tchebitchev : pour toute variable aléatoire X et tout réel strictement positif ε, on a $P(|X-E(X)|\geqslant\varepsilon)\leqslant Var(X)/\varepsilon^2$.

On prend une variable aléatoire positive A et un réel a strictement positif.
On écrit la définition : $E(A)=\sum_{x}x.P(A=x)$.
On coupe en deux $E(A)=\sum_{x<a}x.P(A=x)+\sum_{a\leqslant x}x.P(A=x)$.
La première somme est positive, car la variable aléatoire est positive.
Dans la seconde, on minore : $a\leqslant x$ donc $a.P(A=x)\leqslant x.P(A=x)$.
On a donc à ce stade $E(A)\leqslant\sum_{a\leqslant x}a.P(A=x)=a.\sum_{a\leqslant x}P(A=x)$.
Or, la somme $\sum_{a\leqslant x}P(A=x)$ est précisément $P(A\geqslant a)$.
Il ne reste plus qu'à diviser par a strictement positif.
Pour a trop proche de 0, cette inégalité est sans intérêt.

On prend une variable aléatoire X, d'espérance $E(X)$ et de variance $Var(X)$.
La variable aléatoire $(X-E(X))^2$ est positive. Elle a pour espérance $Var(X)$.
On lui applique l'inégalité de Markov avec $A=(X-E(X))^2$ et $a=\varepsilon^2$:
$P((X-E(X))^2\geqslant\varepsilon^2)\leqslant\frac{E((X-E(X))^2)}{\varepsilon^2}$.
C'est exactement $P(|X-E(X)|\geqslant\varepsilon)\leqslant\frac{Var(X)}{\varepsilon^2}$.

La réunion de deux sous-groupes d'un groupe $(G,*)$ n'est jamais un sous-groupe de $(G,*)$, sauf si l'un est inclus dans l'autre.

On considère deux sous groupes A et B d'un groupe $(G,*)$. On a trois cas

$A \subset B$	$B \subset A$	$A \not\subset B$ et $B \not\subset A$
$A \cup B = B$, sous groupe	$A \cup B = A$, sous groupe	$A \cup B$ n'est pas stable par $*$

Seule le troisième cas va être étudié ici, évidemment.
Comme A n'est pas inclus dans B, il existe au moins un élément a qui est dans A, mais pas dans B *(négation de $\forall a \in A,\ a \in B$)*.
Comme B n'est pas inclus dans A, il existe au moins un élément b qui est dans B, mais pas dans A.
Comme A et B sont des sous-groupes, on a

$a \in A$	$a \notin B$	$a \in A \cup B$	$a^{-1} \in A$
$b \notin A$	$b \in B$	$b \in A \cup B$	$b^{-1} \in B$

On regarde où se trouve l'élément $a * b$.
• Il n'est pas dans A, sinon $(a^{-1}) * (a * b)$ serait dans A *(stabilité de A)*.
• Il n'est pas dans B, sinon $(a * b) * (b^{-1})$ serait dans B *(stabilité de B)*.
N'étant ni dans A, ni dans B, il n'est pas dans $A \cup B$.
On reconnaît que $A \cup B$ n'est pas stable par la loi $*$.

Corollaire : un groupe ne peut pas être la réunion de deux sous-groupes propres [1].

Dans un espace vectoriel engendré par n vecteurs, toute famille de $n+1$ vecteurs est liée.
Corollaire : les bases d'un espace vectoriel[a] ont toutes le même cardinal, appelé dimension de cet espace vectoriel.

[a] engendré par une famille finie, sinon tous les cardinaux considérés sont infinis

On se place dans un espace vectoriel $(E,+,.)$ muni d'une famille génératrice $(\overrightarrow{a_1},\dots\overrightarrow{a_n})$ *(tout vecteur $\overrightarrow{u}$ est combinaison linéaire des $\overrightarrow{a_k}$)*. On prend une famille $(\overrightarrow{v_0},\dots\overrightarrow{v_n})$. L'objectif est de montrer qu'elle est liée.
On démontre le résultat par récurrence sur n.
On initialise à $n=0$.
On prend un espace vectioriel engendré par 0 vecteur. Ce ne peut être que $(\{\overrightarrow{0}\},+,.)$. La seule famille de un vecteur envisagée est $(\overrightarrow{0})$ et elle est liée par $1.\overrightarrow{0} = \overrightarrow{0}$.

On poursuit par principe à $n=1$.
On prend, dans un espace vectoriel engendré par un vecteur $\overrightarrow{a_1}$ une famille de deux vecteurs $(\overrightarrow{v_0},\overrightarrow{v_1})$. Les deux vecteurs sont colinéaires, la famille est liée.

On suppose maintenant pour un n donné que toute famille de $n+1$ vecteurs dans un espace vectoriel engendré par n vecteurs est liée *(hypothèse notée H_n)*.
On se place alors dans un espace vectoriel $(E,+,.)$ engendré par $(\overrightarrow{a_1},\dots\overrightarrow{a_{n+1}})$ et on y prend $n+2$ vecteurs $(\overrightarrow{v_0},\dots\overrightarrow{v_{n+1}})$. Il faut prouver en utilisant H_n que cette famille est liée.
On décompose suivant la famille génératrice *(sans garantie d'unicité, mais ça ne sert à rien)* :

$$\left\{\begin{array}{ccccccc|}
\overrightarrow{v_0} & = & \alpha_0^1.\overrightarrow{a_1} & +\dots & +\alpha_0^n.\overrightarrow{a_n} & +\alpha_0^{n+1}.\overrightarrow{a_{n+1}} \\
\overrightarrow{v_1} & = & \alpha_1^1.\overrightarrow{a_1} & +\dots & +\alpha_1^n.\overrightarrow{a_n} & +\alpha_1^{n+1}.\overrightarrow{a_{n+1}} \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\overrightarrow{v_n} & = & \alpha_n^1.\overrightarrow{a_1} & +\dots & +\alpha_n^n.\overrightarrow{a_n} & +\alpha_n^{n+1}.\overrightarrow{a_{n+1}} \\
\overrightarrow{v_{n+1}} & = & \alpha_{n+1}^1.\overrightarrow{a_1} & +\dots & +\alpha_{n+1}^n.\overrightarrow{a_n} & +\alpha_{n+1}^{n+1}.\overrightarrow{a_{n+1}}
\end{array}\right|$$

On étudie deux cas :

[1] on appelle sous-groupe propre un sous-groupe différent du groupe

• premier cas : tous les α_i^{n+1} sont nuls. Alors, la famille des $\overrightarrow{v_i}$ est dans l'espace vectoriel engendré par $(\overrightarrow{a_1},\dots\overrightarrow{a_n})$, et comme elle est formée de $n+2$ vecteurs *(soit plus que $n+1$)*, elle est liée par l'hypothèse H_n.
• second cas : l'un au moins des α_i^{n+1} est non nul. Quitte à réindexer la famille, on peut supposer que c'est α_{n+1}^{n+1} *(l'ordre des vecteurs l'intervient pas dans le caractère "libre ou lié" d'une famille)*. On définit alors les vecteurs suivants : $\overrightarrow{w_0}=\overrightarrow{v_0}-\dfrac{\alpha_0^{n+1}}{\alpha_{n+1}^{n+1}}.\overrightarrow{v_{n+1}}$, $\overrightarrow{w_1}=\overrightarrow{v_1}-\dfrac{\alpha_1^{n+1}}{\alpha_{n+1}^{n+1}}.\overrightarrow{v_{n+1}}$ jusqu'à $\overrightarrow{w_n}=\overrightarrow{v_n}-\dfrac{\alpha_n^{n+1}}{\alpha_{n+1}^{n+1}}.\overrightarrow{v_{n+1}}$ *(les plus observateurs identifieront la méthode du pivot de Gauss)*.
Par construction, ces $n+1$ vecteurs s'expriment à l'aide de $\overrightarrow{a_1}$ jusqu'à $\overrightarrow{a_n}$ *(on a tout fait pour effacer la "composante" suivant $\overrightarrow{a_{n+1}}$)*.

Par hypothèse de rang n, cette famille des $\overrightarrow{w_i}$ est liée par une relation du type $\sum_{i=0}^{n}\mu_i.\overrightarrow{w_i}=\overrightarrow{0}$ avec au moins un des μ_i non nul.

On remplace alors $\sum_{i=0}^{n}\mu_i.\left(\overrightarrow{v_i}-\dfrac{\alpha_i^{n+1}}{\alpha_{n+1}^{n+1}}.\overrightarrow{v_{n+1}}\right)=\overrightarrow{0}$ que l'on peut écrire $\sum_{i=0}^{n+1}\mu_i.\overrightarrow{v_i}=\overrightarrow{0}$ *(avec $\mu_{n+1}=-\sum_{i=0}^{n}\mu_i.\dfrac{\alpha_i^{n+1}}{\alpha_{n+1}^{n+1}}$ si l'on y tient vraiment, mais c'est sans importance)*, avec l'un au moins de μ_i non nul *(pour un i de 0 à n déjà)*.
On reconnaît que la famille $(\overrightarrow{v_0},\dots\overrightarrow{v_{n+1}})$ est liée, et la récurrence s'achève.

On passe au corollaire. On se place dans un espace vectoriel $(E,+,.)$ engendré par une famille finie $(\overrightarrow{a_1},\dots\overrightarrow{a_n})$.
C'est ce qu'on appelle un espace vectoriel de dimension finie, même si cette définition vient avant la notion même de dimension.
On sait déjà que les familles libres ne peuvent pas avoir plus de n vecteurs.
Les bases étant libres, leur cardinal sera inférieur ou égal à n.
On prend alors deux bases $(\overrightarrow{e_1},\dots\overrightarrow{e_p})$ et $(\overrightarrow{\varepsilon_1},\dots\overrightarrow{\varepsilon_q})$ *(objectif : $p=q$)*.
Comme $(\overrightarrow{e_1},\dots\overrightarrow{e_p})$ est génératrice de $(E,+,.)$, la famille libre $(\overrightarrow{\varepsilon_1},\dots\overrightarrow{\varepsilon_q})$ ne peut pas avoir un cardinal strictement supérieur à p *(théorème précédent)*. On a donc $q\leqslant p$.
Comme $(\overrightarrow{\varepsilon_1},\dots\overrightarrow{\varepsilon_q})$ est génératrice, la famille libre $(\overrightarrow{e_1},\dots\overrightarrow{e_p})$ ne peut pas avoir un cardinal strictement supérieur à q. On a donc $p\leqslant q$.
Par antisymétrie de l'ordre sur les entiers naturels : $p=q$.

Formule de Taylor avec reste intégrale : soit f de classe C^{n+1}[a] de $[a,\ a+h]$ dans $\mathbb{R}$, alors $f(a+h)=\sum_{k=0}^{n}\dfrac{f^{(k)}(a)}{k!}.h^k+\dfrac{h^{n+1}}{n!}.\int_0^1(1-t)^n.f^{(n+1)}(a+t.h).dt$.

Inégalité de Taylor-Lagrange : si f est de classe C^{n+1} avec sa dérivée $n+1^{ieme}$ bornée en valeur absolue par M_{n+1} sur $[a,\ a+h]$ au moins, alors on a $\left|f(a+h)-\sum_{k=0}^{n}\dfrac{f^{(k)}(a)}{k!}.h^k\right|\leqslant\dfrac{M_{n+1}.|h|^{n+1}}{(n+1)!}$.

[a] f est $n+1$ fois dérivable et sa dérivée $n+1^{ieme}$ est continue

<u>La démonstration la plus naturelle se fait par récurrence sur n.</u>
Pour l'initialisation à $n=0$, on prend f dérivable à dérivée continue. On calcule l'intégrale $\int_0^1 h.f'(a+t.h).dt$ qui s'intègre précisément en $\Big[f(a+t.h)\Big]_{t=0}^{t=1}$ *(il suffit de dériver $t\to f(a+t.h)$)*. On

a donc bien $\int_0^1 h.f'(a+t.h).dt = f(a+h) - f(a)$ et il ne reste qu'à faire passer $f(a)$ de l'autre côté.

On suppose à un ordre n que la formule est correcte, et on suppose de surcroît que f est de classe C^{n+2}.

On calcule l'intégrale $\int_0^1 \frac{(1-t)^n}{n!}.h^{n+1}.f^{(n+1)}(a+t.h).dt$ par parties :

$$\left[\begin{array}{ccc} \frac{(1-t)^n}{n!} & \leftarrow & -\frac{(1-t)^{n+1}}{(n+1)!} \\ h^{n+1}.f^{(n+1)}(a+t.h) & \rightarrow & h^{n+2}.f^{(n+2)}(a+t.h) \end{array}\right] \textit{ (fonctions continues de } t\textit{)}$$

Le terme $\Big[- h^{n+1}.f^{(n+1)}(a+t.h).\frac{(1-t)^{n+1}}{(n+1)!}\Big]_{t=0}^{t=1}$ donne uniquement $h^{n+1}.\frac{f^{(n+1)}(a)}{(n+1)!}$ qui fait passer $\sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}.h^k$ à $\sum_{k=0}^{n+1} \frac{f^{(k)}(a)}{k!}.h^k$.

Le terme $\int_0^1 \frac{(1-t)^{n+1}}{(n+1)!}.h^{n+2}.f^{(n+2)}(a+t.h).dt$ avec ses deux signes moins est le reste d'ordre $n+1$.

La récurrence s'achève ainsi.

La démonstration judicieuse passe par la définition d'une application bien choisie à a, h et n fixés.

On définit donc $\varphi = t \rightarrow \sum_{k=0}^{n} \frac{(1-t)^k}{k!}.h^k.f^{(k)}(a+t.h)$ *(définie et dérivable sur* $[0,\ 1]$*).*

On calcule : $\varphi(0) = \sum_{k=0}^{n} \frac{h^k}{k!}.f^{(k)}(a)$ et $\varphi(1) = f(a+t.h)$ [2].

On dérive : $\varphi = t \rightarrow \sum_{k=0}^{n} \Big(- \frac{k.(1-t)^{k-1}}{k!}.h^k.f^{(k)}(a+t.h) + \frac{(1-t)^k}{k!}.h^{k+1}.f^{(k+1)}(a+t.h)\Big)$ *(dérivée d'une somme de produits).*

En séparant en deux et en réindexant la première somme $-\sum_{k=0}^{n} \frac{k.(1-t)^{k-1}}{k!}.h^k.f^{(k)}(a+t.h)$ *(qui ne contient plus de terme d'indice* 0*)*, on a une somme télescopique où il ne reste que le terme $\frac{(1-t)^k}{k!}.h^{k+1}.f^{(k+1)}(a+t.h)$ pour k égal à $n+1$.

En écrivant $\varphi(1) - \varphi(0) = \int_0^1 \varphi(t).dt$, on obtient la formule de Taylor avec reste intégrale.

Cette formule est valable aussi pour les fonctions à valeurs complexes.

On prend f $n+1$ fois dérivable avec f^{n+1} bornée en valeur absolue par M_{n+1}.

On écrit la formule de Taylor avec reste intégrale, on fait passer la somme de l'autre côté. La distance $\Big|f(a+h) - \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}.h^k\Big|$ est alors égale à $\Big|\int_0^1 \frac{(1-t)^n}{n!}.h^{n+1}.f^{(n+1)}(a+t.h).dt\Big|$.

Par inégalité triangulaire *(valeur absolue de l'intégrale plus petite que l'intégrale de la valeur absolue)*, on majore par $\int_0^1 \Big|\frac{(1-t)^n}{n!}.h^{n+1}.f^{(n+1)}(a+t.h)\Big|.dt$.

On sort de la valeur absolue ce qui est déjà assurément positif : $\int_0^1 \frac{(1-t)^n}{n!}.|h|^{n+1}.|f^{(n+1)}(a+t.h)|.dt$.

On majore $|f^{(n+1)}(a+t.h)|$ par M_{n+1} et on calcule $\int_0^1 \frac{(1-t)^n}{n!}.|h|^{n+1}.M_{n+1}.dt$ vaut $\frac{|h^{n+1}|}{n!}.M_{n+1}.\frac{1}{n+1}$.

[2] rappelons que $(1-1)^0$ vaut 1 ainsi que 0!

On aboutit à la majoration demandée.
Contrairement à des égalites de Taylor-Lagrange, cette inégalité est valable aussi pour les fonctions à valeurs complexes.

L'image d'une famille libre par une application linéaire injective est libre.

On prend $(\overrightarrow{u_1},\dots\overrightarrow{u_n})$ libre dans l'espace vectoriel $(E,+,.)$ et f injective.

On considère $(f(\overrightarrow{u_1}),\dots f(\overrightarrow{u_n}))$ dans l'espace vectoriel d'arrivée. On suppose $\sum_{k=1}^{n}\alpha_k.f(\overrightarrow{u_k})=\overrightarrow{0_F}$ *(objectif : les α_k sont tous nuls).*

Par linéarité de f , on obtient $f\Big(\sum_{k=1}^{n}\alpha_k.\overrightarrow{u_k}\Big)=\overrightarrow{0_F}=f(\overrightarrow{0_E})$.

Par injectivité de f, il vient $\sum_{k=1}^{n}\alpha_k.\overrightarrow{u_k}=\overrightarrow{0_E}$ puis par liberté de la famille $(\overrightarrow{u_1},\dots\overrightarrow{u_n})$: $\forall k,\ \alpha_k=0$.

Une application linéaire non injective peut transformer une famille libre en famille liée, il suffit de prendre un vecteur non nul du noyau, ou plus généralement une famille de vecteur qui réussit à engendrer un vecteur du noyau.

Théorème des valeurs intermédiaires : soit f continue de $[a,\ b]$ (intervalle de $\mathbb{R}$) dans $\mathbb{R}$, alors toute valeur comprise entre $f(a)$ et $f(b)$ est atteinte au moins une fois par f entre a et b.

L'image d'un intervalle par une application numérique continue est encore un intervalle.

On commence par un lemme. Soit f continue de $[a,\ b]$ dans $\mathbb{R}$, négative en a et positive en b, alors f s'annule au moins une fois entre a et b.

Démonstration du lemme par principe de la borne supérieure.

On pose $A=\{x\in[a,\ b]\mid f(x)\leqslant 0\}$.
C'est une partie de $[a,\ b]$, donc une partie de $\mathbb{R}$.
Elle est non vide car elle contient au moins a.
Elle est majorée par b.
Elle admet donc une borne supérieure *(plus petit majorant)*, noté α.
On va montrer par double encadrement et continuité que $f(\alpha)$ est nul.
• Par définition de la borne supérieure, il existe une suite (γ_n) de points de A qui tend vers α. Par continuité de f en α : $f(\gamma_n)\to_{n\to+\infty}f(\alpha)$.
Par appartenance à A : $f(\gamma_n)\leqslant 0$ pour tout n. Par passage à la limite : $f(\alpha)\leqslant 0$.
• Par continuité et stricte positivité de f en b, il existe un intervalle $[b-\beta,\ b]$ sur lequel f est plus grande que $f(b)/2$ *(définition de la continuité avec $\varepsilon=f(b)/2>0$).*
La borne supérieure α est donc inférieure ou égale à $b-\beta$, et donc elle n'est pas égale à b.
Les réels $\dfrac{n.\alpha+b}{n+1}$ sont donc strictement entre α et b, donc hors de A. Ainsi $f\Big(\dfrac{n.\alpha+b}{n+1}\Big)>0$ pour tout n.
Cette suite tend vers α quand n tend vers l'infini. Par continuité sa limite est $f(\alpha)$, mais par passage à la limite, cette limite est positive ou nulle.
Par double inégalité, $f(\alpha)$ est nul.

Démonstration par dichotomie (suites adjacentes).

On pose $a_0=a$ et $b_0=b$.
Pour tout entier naturel n, on pose $c_n=\dfrac{a_n+b_n}{2}$ et on étudie le signe de $f(c_n)$.

Si $f(c_n)$ est négatif *(comme $f(a_n)$)*, on pose $a_{n+1} = c_n$ et $b_{n+1} = b_n$.
Si $f(c_n)$ est positif *(comme $f(b_n)$)*, on pose $a_{n+1} = a_n$ et $b_{n+1} = c_n$.
Par construction, les suites (a_n) et (b_n) sont adjacentes *((a_n) croît et (b_n) décroît et la différence $b_n - a_n$ vaut $\frac{b-a}{2^n}$ et tend vers 0).*
Elles convergent vers une même limite α.
Pour tout n, on a $f(a_n) \leqslant 0$ et $f(b_n) \geqslant 0$.
Par continuité elles convergent vers $f(\alpha)$.
Par passage à la limite, $f(\alpha)$ est à la fois négatif et positif. Il est nul.

Quitte à étudier $-f$, on peut montrer que si f *(continue)* change de signe entre a et b, alors elle s'annule au moins une fois.
La contraposée de ce résultat est parfois utile :
Si une application continue de $[a,\ b]$ dans $\mathbb{R}$ ne s'annule pas, alors elle reste de signe constant.

On prend maintenant une simple application continue f de $[a,\ b]$ dans $\mathbb{R}$.
On prend un certain réel γ entre $f(a)$ et $f(b)$.
On veut montrer que f atteint la valeur γ en au moins un point c de $[a,\ b]$.
On considère l'application auxilliaire $f - \gamma$ *(simple translation).* Elle est encore continue de $[a,\ b]$ dans $\mathbb{R}$. En a elle vaut $f(a) - \gamma$ et en b elle vaut $f(b) - \gamma$. Ces deux réels sont de signes opposés.
Par le lemme précédent *(démontré de deux façons)*, $f - \gamma$ s'annule au moins une fois. Au point c où elle s'annule, f prend la valeur intermédiaire γ.

On prend un intervalle I *("ensemble sans trou")* et une application continue f de I dans $\mathbb{R}$. Il faut montrer que $f(I)$ est un intervalle.
Comme un intervalle peut être d'une des diverses formes possibles $[\alpha,\ \beta]$, $[\alpha,\ \beta[$, $]\alpha,\ \beta]$, $]\alpha,\ \beta[$, $]\alpha,\ +\infty[$, $[\alpha,\ +\infty[$, $]-\infty,\ \beta]$, $]-\infty,\ \beta[$ et enfin $]-\infty,\ +\infty[$ *(et pourquoi pas $\emptyset$)*, il faut utiliser la caractérisation d'un intervalle : si deux réels u et v sont dans l'intervalle, alors tout réel t entre u et v est encore dans l'intervalle.
On prend donc u et v dans l'ensemble image $f(I)$, puis un réel t entre les deux. Objectif : t est dans $f(I)$, c'est à dire "*t a au moins un antécédent dans I*".
Comme u et v sont dans $f(I)$, ils s'écrivent respectivement $f(a)$ et $f(b)$ pour a et b dans I.
Mais alors le segment $[a,\ b]$ est inclus dans I car I est un intervalle. f est donc continue sur $[a,\ b]$.
Toute valeur comprise entre $f(a)$ et $f(b)$ *(comme justement t)* est atteinte au moins une fois en un point c de $[a,\ b]$, donc de I.

Décomposition en éléments simples : si les a_k sont n complexes distincts, alors toute fraction de la forme $\dfrac{P(X)}{(X-a_1)\dots(X-a_n)}$ avec $P(X)$ de degré inférieur ou égale à $n-1$ se décompose d'une façon unique sous la forme $\dfrac{\alpha_1}{X-a_1} + \dots + \dfrac{\alpha_n}{X-a_n}$ (avec les α_k dépendant linéairement des coefficients du polynôme P).

On prend le problème à rebours et on utilise un théorème d'algèbre linéaire.
Pour tout n-uplet de complexes $(\alpha_1, \dots \alpha_n)$, on définit $\prod_{k=1}^{n}(X-a_k).\sum_{i=1}^{n}\frac{\alpha_i}{X-a_i}$.
L'objet obténu est un polynôme de degré inférieur ou égal à $n-1$ puisque c'est en fait
$\alpha_1.(X-a_2)\dots(X-a_n) + \alpha_2.(X-a_1).(X-a_3)\dots(X-a_n) + \dots + \alpha_n.(X-a_1)\dots(X-a_{n-1})$.
L'appplication ainsi définie est linéaire de $(\mathbb{C}^n, +, .)$ dans $(\mathbb{C}_{n-1}[X], +, .)$

(vérification purement technique $\prod_{k=1}^{n}(X-a_k).\sum_{i=1}^{n}\frac{\lambda.\alpha_i+\mu.\beta_i}{X-a_i}=\lambda.\prod_{k=1}^{n}(X-a_k).\sum_{i=1}^{n}\frac{\alpha_i}{X-a_i}+\mu.\prod_{k=1}^{n}(X-a_k).\sum_{i=1}^{n}\frac{\beta_i}{X-a_i}$*)*
.
On montre que cette application est injective par la "*méthode des pôles*".
Supposons en effet que $\prod_{k=1}^{n}(X-a_k).\sum_{i=1}^{n}\frac{\alpha_i}{X-a_i}$ soit le polynôme nul.
En le calculant en a_1 sous la forme développée
$\alpha_1.(X-a_2)\dots(X-a_n)+\alpha_2.(X-a_1).(X-a_3)\dots(X-a_n)+\dots+\alpha_n.(X-a_1)\dots(X-a_{n-1})$, on obtient que α_1 est nul. De même, en a_i, chaque α_i est nul. Le seul n-uplet d'image nulle est le n-uplet $(0,\dots 0)$.
Comme les deux espaces ont la même dimension *(n pour les deux)*, l'application linéaire injective est automatiquement bijective *(corollaire de la formule du rang)*.
Sa réciproque est aussi une application linéaire bijective. On traduit : pour tout polynôme $P(X)$ de degré inférieur ou égal à $n-1$ il existe un n-uplet tel que $P(X)$ s'écrive $\prod_{k=1}^{n}(X-a_k).\sum_{i=1}^{n}\frac{\alpha_i}{X-a_i}$.
On divise : $\frac{P(X)}{\prod_{k=1}^{n}(X-a_k)}=\sum_{i=1}^{n}\frac{\alpha_i}{X-a_i}$.
Le théorème reste valable si on remplace $\mathbb{C}$ par $\mathbb{R}$; si le degré du polynôme dépasse n, on effectue une division euclidienne pour arriver à $\frac{P(X)}{\prod_{k=1}^{n}(X-a_k)}=R(X)+\sum_{i=1}^{n}\frac{\alpha_i}{X-a_i}$; si les a_i ne sont pas tous distincts, on croise des termes en $\frac{\alpha_i}{X-a_i}+\frac{\beta_i}{(X-a_i)^2}$ voire $\frac{\alpha_i}{X-a_i}+\frac{\beta_i}{(X-a_i)^2}+\frac{\gamma_i}{(X-a_i)^3}$ et même plus, mais avec le même type de démonstration.

Injectivité et monotonie des applications numérique :
• si une application de $\mathbb{R}$ dans $\mathbb{R}$ est strictement monotone, alors elle est injective,
• si une application continue de $[a,\ b]$ dans $\mathbb{R}$ est injective, alors elle est monotone.

La première démonstration est de la pure logique ; on va montrer que toute application numérique strictement croissante est injective *(le cas "strictement décroissant" est similaire)*.
On montre le sens suivant de l'injectivité : $\forall(a,\ b),\ (a\neq b)\Rightarrow(f(a)\neq f(b))$.
On prend donc deux réels distincts a et b.
Comme l'ordre sur $\mathbb{R}$ est total, on n'a que deux possibilités : $a<b$ ou $b<a$.
Par stricte croissance de f, chaque cas conduit respectivement à $f(a)<f(b)$ ou $f(b)<f(a)$.
Dans tous les cas, on a bien $f(a)\neq f(b)$.

Pour la seconde, on va utiliser le théorème des valeurs intermédiaires sur une application auxilliaire.
On prend f de $[a,\ b]$ dans $\mathbb{R}$, que l'on suppose injective. Sans restreindre la généralité, on suppose $f(a)<f(b)$. On va montrer que f est strictement croissante sur tout l'intervalle et pas juste "*entre les deux extrémités*".
On prend donc x et y dans $[a,\ b]$ vérifiant $x<y$ *(objectif : $f(x)<f(y)$)*.
On construit l'application auxillaire $t\to f\big((1-t).y+t.b\big)-f\big((1-t).x+t.a\big)$ que l'on va noter φ *(pour t entre 0 et 1)*.
Quand t va de 0 à 1, le réel $(1-t).y+t.b$ *(respectivement $(1-t).x+t.a$)* restent entre y et b *(respectivement entre x et a)*, donc reste dans $[a,\ b]$. Il s'ensuit que par composition et soustraction, l'application φ est continue, de $[0,\ 1]$ dans $\mathbb{R}$.
On calcule $\varphi(0)=f(y)-f(x)$ et $\varphi(1)=f(b)-f(a)$ *(positif)*.

Par l'absurde, si $f(y)$ n'est pas plus grand que $f(x)$, alors $\varphi(0)$ est négatif ou nul.
Par le théorème des valeurs intermédiaires, il existe un t de $[0,\ 1]$ vérifiant $\varphi(t) = 0$.
On traduit pour ce t : $f\big((1-t).y + t.b\big) = f\big((1-t).x + t.a\big)$.
Par injectivité de f : $(1-t).y + t.b = (1-t).x + t.a$, soit $t = \dfrac{y-x}{(y-x)-(b-a)}$ *(simple calcul).*
Ce réel est bien défini, car $y-x$ *(distance entre les abscisses)* est strictement plus petit que $b-a$ *(longueur de l'intervalle).* Mais justement, le numérateur est positif et le dénominateur négatif, donc t est négatif.
C'est en contradiction avec "$t \in [0,\ 1]$".
C'est donc que $f(y)$ est bien plus grand que $f(x)$.

Petit théorème de Fermat : pour tout entier naturel premier p et tout entier n non multiple de p : $n^{p-1} = 1\ mod\ p$.

Corollaire : $(\{0,\ 1, \ldots p-1\}, +, \times)$ est un corps pour l'addition et la multiplication modulo p.

Théorème de Wilson : pour p premier, $(p-1)!$ est congru à -1 modulo p.

Dans tout ce qui suit, p est donc un nombre premier.

On commence par un lemme : les coefficients binomiaux $\binom{p}{k}$ pour k de 1 à $p-1$ sont des multiples de p.
Le résultat est vrai pour $k = 1$: $\binom{p}{k} = p$.
Supposons le résultat vrai pour un k entre 1 et $p-2$. On a alors $(k+1).\binom{p}{k+1} = (p-k).\binom{p}{k}$ *(formule classique sur les coefficients binomiaux en ligne).* Le second membre est un multiple de p par hypothèse. Comme $k+1$ est strictement plus petit que p et ne contient aucun facteur p, c'est que $\binom{p}{k+1}$ est multiple de p.

<u>On poursuit avec un second résultat :</u> pour tout entier naturel n, l'entier $n^p - n$ est un multiple de p *(par récurrence sur n).*
Pour n égal à 0 *(et même 1)*, cet entier est nul, donc multiple de p.
Supposons le résultat vrai pour un n de $\mathbb{N}$. On calcule alors $(n+1)^p - (n+1)$ par la formule du binôme :

$$(n+1)^p - (n+1) = \sum_{k=0}^{p} \binom{p}{k}.n^k - (n+1) = \sum_{k=1}^{p-1} \binom{p}{k}.n^k + (n^p+1) - (n+1) \text{ (on a isolé deux termes).}$$

La somme $\displaystyle\sum_{k=1}^{p-1} \binom{p}{k}.n^k$ est un multiple de p par le lemme précédent comme somme de multiple de p.
La différence $(n^p+1) - (n+1)$ est un multiple de p par hypothèse de rang n.
La somme est bien multiple de p.

On termine en factorisant dans le cas où n n'est pas multiple de p : $n.(n^{p-1}-1)$ est multiple de p.
Or, il n'y a pas de facteur p dans n, c'est donc que $n^{p-1}-1$ est multiple de p.
Il existe des entiers p non premiers (dits "*nombres de Carmichael*") qui vérifient cette propriété pour tous les entiers n.

On se place dans l'anneau des entiers de 0 à $p-1$ pour l'addition et la multiplication modulo p.

Il reste à prouver que tout entier non nul admet un inverse pour la multiplication modulo p.
On prend donc n entre 1 et $p-1$. On sait donc d'après le petit théorème de Fermat que $n^{p-1}-1$ est un multiple de p. On traduit : $n^{p-1} = 1 \ mod \ p$. On factorise : $n.n^{p-2} = 1 \ mod \ p$.
L'entier n^{p-2} *(réduit modulo p)* est l'inverse multiplicatif de n.

Dans le corps $(\{0, 1, \dots p-1\}, +, \times)$, on a donc $n^{p-1} = 1$ pour tout entier de 1 à $p-1$.
Le polynôme $X^{p-1}-1$ admet donc $p-1$ racines : les entiers de 1 à $p-1$.
On peut donc le factoriser sous la forme $\alpha.\big(X-1\big) \times \dots \big(X-(p-1)\big)$, avec α égal à 1 *(terme de plus haut degré)*.
Partant de $X^{p-1}-1 = \big(X-1\big)\dots\big(X-(p-1)\big)$, on obtient en 0 : $-1 = (-1)\times(-2)\dots(1-p)$.
Il y a dans le membre de droite $p-1$ signes "moins", ce qui fait un signe "plus" *(on traite à part le cas trivial $p=2$)*. Il reste $-1 = (p-1)!$ *(pour la multiplcation modulo p)*. C'est le théorème de Wilson.

Il existe une autre preuve du théorème de Wilson en regroupant les termes.
Dans le produit $(p-1)! = 1\times 2\times 3\dots(p-1)$, on regroupe dans la mesure du possible, les termes deux par deux :
• 1 et $p-1$ à part
• chaque élément de 2 à $p-2$ avec son inverse.
En effet, seul 1 et $p-1$ sont leur propre inverse puisque ce critère correspond à $x^2 = 1$, qui se factorise en $(x-1).(x+1) = 0$, d'uniques solutions 1 et -1 *(qui s'appelle aussi $p-1$)*.
Les éléments groupés deux à deux ont à chaque fois pour produit 1 par définition même de l'inverse.
Il reste (modulo p) : $(p-1)! = 1\times 1^{(p-3)/2}.(p-1) = p-1 = -1$.

Formule de Grassmann : si A et B sont deux sous-espaces vectoriels de dimension finie d'un espace vectoriel $(E,+,.)$, alors on a $\dim(A+B) = \dim(A)+\dim(B)-\dim(A\cap B)$.

Cette formule rappelle la formule $Card(A\cup B) = Card(A)+Card(B)-Card(A\cap B)$ pour deux ensembles. Mais la démonstration est différente.

Preuve par les cardinaux des bases.
On rappelle que $A\cap B$ est un sous-espace vectoriel de $(E,+,.)$ *(en tant que sous-espace vectoriel de A déjà de dimension finie)*.
On construit une base de $A\cap B$ *(par principe de la base incomplète)* : $(\overrightarrow{e_1}, \dots \overrightarrow{e_n})$ *(famille libre et génératrice de $A\cap B$)*.
Comme cette famille est libre dans $A\cap B$, elle l'est aussi dans A. On la complète en base de A : $(\overrightarrow{e_1}, \dots \overrightarrow{e_n}, \overrightarrow{a_{n+1}} \dots \overrightarrow{a_p})$.
De même, en tant que famille libre de B, on la complète en base de B : $(\overrightarrow{e_1}, \dots \overrightarrow{e_n}, \overrightarrow{b_{n+1}} \dots \overrightarrow{b_q})$.
On montre maintenant que $(\overrightarrow{e_1}, \dots \overrightarrow{e_n}, \overrightarrow{a_{n+1}} \dots \overrightarrow{a_p}, \overrightarrow{b_{n+1}} \dots \overrightarrow{b_q})$ est une base de $A+B$.

• On commence par l'appartenance à $A+B$: tous ces vecteurs sont dans A ou dans B donc dans $A+B$.

• On poursuit avec "**génératrice**". On prend un vecteur $\overrightarrow{u}$ de $A+B$. Par définition, il est de la forme $\overrightarrow{u} = \overrightarrow{a}+\overrightarrow{b}$ avec $\overrightarrow{a}$ dans A et $\overrightarrow{b}$ dans B. Par définition des deux bases, $\overrightarrow{a}$ s'écrit $\sum_{i=1}^{n} \alpha_i.\overrightarrow{e_i} + \sum_{j=n+1}^{p} \alpha_j.\overrightarrow{a_j}$. De même, $\overrightarrow{b}$ s'écrit $\sum_{i=1}^{n} \beta_i.\overrightarrow{e_i} + \sum_{k=n+1}^{q} \beta_k.\overrightarrow{b_k}$.
On somme : $\overrightarrow{u} = \sum_{i=1}^{n} (\alpha_i+\beta_i).\overrightarrow{e_i} + \sum_{j=n+1}^{p} \alpha_j.\overrightarrow{a_j} + \sum_{k=n+1}^{q} \beta_k.\overrightarrow{b_k}$.
Il est bien combinaison de $(\overrightarrow{e_1}, \dots \overrightarrow{e_n}, \overrightarrow{a_{n+1}} \dots \overrightarrow{a_p}, \overrightarrow{b_{n+1}} \dots \overrightarrow{b_q})$.

• On termine avec "**libre**". On suppose qu'une combinaison $\sum_{i=1}^{n} \lambda_i.\overrightarrow{e_i} + \sum_{j=n+1}^{p} \alpha_j.\overrightarrow{a_j} + \sum_{k=n+1}^{q} \beta_k.\overrightarrow{b_k}$ est nulle. On bascule $\sum_{i=1}^{n} \lambda_i.\overrightarrow{e_i} + \sum_{j=n+1}^{p} \alpha_j.\overrightarrow{a_j} = -\sum_{k=n+1}^{q} \beta_k.\overrightarrow{b_k}$. Ce vecteur, qu'on va noter $\overrightarrow{c}$ est à la fois dans A *(forme de gauche)* et dans B *(forme de droite)*. Il est donc dans $A \cap B$, et s'écrit comme combinaison de $(\overrightarrow{e_1}, \dots \overrightarrow{e_n})$.
On a donc à ce stade $\overrightarrow{c} = \sum_{i=1}^{n} \lambda_i.\overrightarrow{e_i} + \sum_{j=n+1}^{p} \alpha_j.\overrightarrow{a_j} = -\sum_{k=n+1}^{q} \beta_k.\overrightarrow{b_k} = \sum_{i=1}^{n} \gamma_i.\overrightarrow{e_i}$. En reprenant la dernière égalité, on a $\sum_{k=n+1}^{q} \beta_k.\overrightarrow{b_k} + \sum_{i=1}^{n} \gamma_i.\overrightarrow{e_i} = \overrightarrow{0}$. Comme $(\overrightarrow{e_1}, \dots \overrightarrow{e_n}, \overrightarrow{b_{n+1}} \dots \overrightarrow{b_q})$ est une base de B, elle est libre et on a $\beta_k = 0$ pour tout k et $\gamma_i = 0$ pour tout i. On reporte : $\overrightarrow{c}$ est nul. On re-reporte : $\overrightarrow{0} = \sum_{i=1}^{n} \lambda_i.\overrightarrow{e_i} + \sum_{j=n+1}^{p} \alpha_j.\overrightarrow{a_j}$. Comme $(\overrightarrow{e_1}, \dots \overrightarrow{e_n}, \overrightarrow{a_{n+1}} \dots \overrightarrow{a_p})$ est libre (dans A), on trouve cette fois que les λ_i et la α_j sont nuls. Finalement, tous les coefficients sont nuls.

Maintenant que $(\overrightarrow{e_1}, \dots \overrightarrow{e_n}, \overrightarrow{a_{n+1}} \dots \overrightarrow{a_p}, \overrightarrow{b_{n+1}} \dots \overrightarrow{b_q})$ est une base de $A+B$, on compte le nombre d'éléments : $p + (q - n)$.
On a donc $\dim(A + B) = \dim(A) + (\dim(B) - \dim(A \cap B))$ comme attendu.

Preuve en utilisant la formule du rang.
On définit l'application $(\overrightarrow{a},\ \overrightarrow{b}) \to \overrightarrow{a} + \overrightarrow{b}$ de $A \times B$ dans E *(notée φ)*.
Par définition même, son ensemble image est $A + B$.
Son noyau est formé des couples $(\overrightarrow{a},\ \overrightarrow{b})$ de $A \times B$ vérifiant $\overrightarrow{a} + \overrightarrow{b} = \overrightarrow{0}$. On a alors $\overrightarrow{a} = -\overrightarrow{b}$. Ce vecteur est à la fois dans A et dans B. Le noyau est donc formé des couples $(\overrightarrow{c},\ -\overrightarrow{c})$ avec $\overrightarrow{c}$ dans $A \cap B$.
Ce noyau est isomorphe à $A \cap B$. Il a donc la même dimension.
La formule $\dim(A \times B) = \dim(Ker(\varphi)) + \dim(Im(\varphi))$ donne $\dim(A) + \dim(B) = \dim(A \cap B) + \dim(A + B)$.

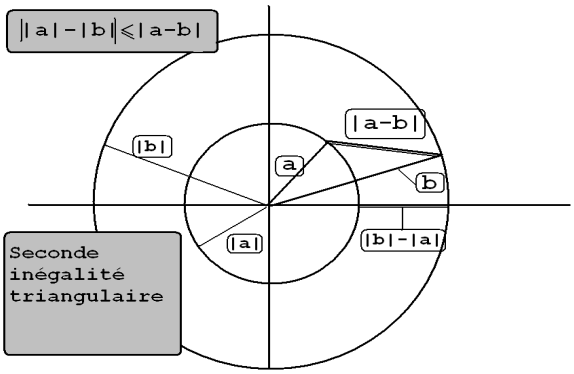
Séries à termes généraux positifs équivalents en $+\infty$: soient deux suites (a_n) et (b_n) réelles strictement positives, équivalentes en $+\infty$ [a], alors la série de terme général a_n est de même nature que la série de terme général (b_n) [b].

[a] le quotient a_n/b_n tend vers 1
[b] si l'une converge, l'autre converge aussi, si l'une diverge, l'autre diverge aussi

On considère deux suites réelles strictement positives *(ou pour le moins strictement positives à partir d'un certain rang)* : (a_n) *et* (b_n). Leurs séries associées sont notées (A_N) et (B_N) *(c'est à dire* $A_N = \sum_{n=0}^{N} a_n$*)*.
On suppose que le quotient bien défini $\frac{a_n}{b_n}$ converge vers 1 quand n tend vers l'infini.
On sait déjà que (A_N) et (B_N) sont croissantes ($A_{N+1} - A_N = a_N > 0$), elles convergent si et seulement si elles sont majorées.
Comme le quotient a_n/b_nconverge *(vers 1)*, il est majoré. On note β un de ses majorants.
Comme le quotient b_n/a_nconverge *(vers 1)*, il est majoré. On note α un de ses majorants.
On a donc $\alpha.a_n \leqslant b_n \leqslant \beta.a_n$ pour tout n *(produits en croix strictement positifs)*.
On somme de 0 à N *(entier naturel donné)* : $\alpha.A_N \leqslant B_N \leqslant \beta.A_N$.
Si la série (A_N) diverge, c'est en croissant vers $+\infty$ et la relation $\alpha.A_N \leqslant B_N$ pousse aussi B_N vers $+\infty$.

Si la série (B_N) diverge, c'est en croissant vers $+\infty$ et la relation $B_N \leqslant \beta.A_N$ pousse aussi $\beta.A_N$ *(et aussi A_N)* vers $+\infty$.
Les deux autres implications s'obtiennent par contraposée.
Attention, le théorème ne dit rien en revanche sur les valeurs des éventelles limites.
On peut quand même approfondir : dans le cas où les deux divergent, on a alors $A_N \sim_{N\to+\infty} B_N$ *(vitesse de divergence des termes généraux)*, et dans le cas où les deux convergent $\sum_{n=N}^{+\infty} a_n \sim_{N\to+\infty} \sum_{n=N}^{+\infty} b_n$ *(vitesse de cnvergence des restes).*

Deuxième inégalité triangulaire : pour tout couple de complexes $(a,\ b)$, on a $||a|-|b|| \leqslant |a-b|$.



On écrit pour a et b donnés la première inégalité triangulaire :
$|a| = |a-b+b| \leqslant |a-b| + |b|$ et $|b| = |b-a+a| \leqslant |b-a| + |a|$
On fait passer de l'autre côté dans les deux :
$|a| - |b| \leqslant |a-b|$ et $|b| - |a| \leqslant |a-b|$.
Or, le réel positif $\big||a|-|b|\big|$ est l'un des deux nombres $|a|-|b|$ ou son opposé $|b|-|a|$.
Qu'il soit l'un ou l'autre, il est plus petit que $|a-b|$.

Lemme d'agrandissement : dans un espace vectoriel $(E,+,.)$, soit un famille libre $(\overrightarrow{a_1},\dots\overrightarrow{a_n})$ et un vecteur $\overrightarrow{u}$. La famille $(\overrightarrow{a_1},\dots\overrightarrow{a_n},\overrightarrow{u})$ est liée si et seulement si $\overrightarrow{u}$ est combinaison linéaire de $(\overrightarrow{a_1},\dots\overrightarrow{a_n})$.

On prend donc une famille libre $(\overrightarrow{a_1},\dots\overrightarrow{a_n})$ *(la seule combinaison linéaire pouvant donner $\overrightarrow{0}$ est $\sum_{k=1}^{n} 0.\overrightarrow{a_k}$).*

• Si le vecteur $\overrightarrow{u}$ est combinaison de $(\overrightarrow{a_1},\dots\overrightarrow{a_n})$, alors l'un des vecteurs de $(\overrightarrow{a_1},\dots\overrightarrow{a_n},\overrightarrow{u})$ est combinaison des autres et la famille est liée.
• *L'autre sens est plus intéressant.*
On suppose la famille $(\overrightarrow{a_1},\dots\overrightarrow{a_n},\overrightarrow{u})$ liée par une relation du type $\alpha_1.\overrightarrow{a_1}\dots\alpha_n.\overrightarrow{a_n} + \alpha_0.\overrightarrow{u} = \overrightarrow{0}$ avec au moins un des α_i non nul. Il est impossible que α_0 soit nul, sinon on a une relation du type $\alpha_1.\overrightarrow{a_1}\dots\alpha_n.\overrightarrow{a_n} = \overrightarrow{0}$ avec au moins un des α_i non nul, ce qui contredit "famille libre".
On divise alors : $\overrightarrow{u} = \sum_{k=1}^{n} \frac{-\alpha_k}{\alpha_0}.\overrightarrow{a_k}$, et $\overrightarrow{u}$ est combinaison de la famille $(\overrightarrow{a_1},\dots\overrightarrow{a_n})$.

Théorème de Cantor : soit E un ensemble il ne peut pas y avoir d'application surjective de E dans $P(E)$ et donc pas de bijection entre E et $P(E)$.

Supposons qu'une telle application F de E dans $P(E)$ soit surjective.
On pose alors $A = \{a \in E \mid a \notin F(a)\}$ *(cette définition est cohérente, puisque a est un élément de E et $F(a)$ une partie de E ; l'élément peut appartenir ou non à la partie).*
L'ensemble A ainsi défini est une partie de E. Il a donc au moins un antécédent α par F puisque F est supposée surjective.
Mais alors, il n'y a que deux possibilités : α est dans A ou α n'est pas dans A.
• Si α est dans A, on a alors $\alpha \in F(\alpha)$ *(puisque $A = F(\alpha)$)*, et par définition, ceci donne $\alpha \notin A$. Contradiction.

• Si α n'est pas dans A, on a alors $\alpha \notin F(\alpha)$ *(puisque $A = F(\alpha)$)*, et par définition, ceci donne $\alpha \in A$. Contradiction.

Les deux seuls cas possibles condisent à une contradiction. C'est donc que l'hypothèse "*A admet au moins un antécédent α par F*" est impossible. F ne peut pas être surjective.

Première sommes de Newton : pour tout entier naturel n : $\sum_{k=0}^{n} k^0 = n+1$, $\sum_{k=0}^{n} k = \frac{n.(n+1)}{2}$, $\sum_{k=0}^{n} k^2 = \frac{n.(n+1).(2.n+1)}{6}$ et $\sum_{k=0}^{n} k^3 = \left(\frac{n.(n+1)}{2}\right)^2$.

La première formule est une évidence, il suffit de compter les termes.
On rappelle que k^0 vaut 1, même pour k égal à 0. L'entier 0^0 dénombre les applications d'un ensemble à 0 élément(s) dans lui même, et il y en a une, c'est l'identité. Ce qui est une forme indéterminée, c'est $(o(1))^{o(1)}$ au sens des limites de suites ou de fonctions.
On peut démontrer les autres par récurrence sur n, mais on va proposer ici d'autres preuves.

Pour tout n, on pose $A_n = \sum_{k=0}^{n} k$, **et** $B_n = \sum_{k=0}^{n} k^2$, $C_n = \sum_{k=0}^{n} k^3$.

Dans A_n, on fait un renversement d'indice : $p = n - k$. Quand k va de 0 à n, l'entier p va de n à 0.

On a donc $A_n = \sum_{p=0}^{n}(n-p)$ que l'on sépare en $A_n = \sum_{p=0}^{n} n - \sum_{p=0}^{n} p$. La somme $\sum_{p=0}^{n} n$ vaut $n.(n+1)$ *(nombre de termes)*. La somme $\sum_{p=0}^{n} p$ est encore A_n *(variable de sommation muette)*. On a donc $A_n = n.(n+1) - A_n$, qui donne bien $A_n = \frac{n.(n+1)}{2}$.

Pour calculer B_n, on calcule de deux façons $C_{n+1} - C_n$.

Par définition de $\sum_{k=0}^{n+1}$, on trouve déjà $(n+1)^3$.

Mais c'est aussi $\sum_{k=1}^{n+1} k^3 - \sum_{k=0}^{n} k^3$ (dans la première somme, on peut sommer à partir de $k = 1$, puisque le terme d'indice $k = 0$ est nul). On réindexe la première en posant $p = k - 1$: $C_{n+1} - C_n = \sum_{p=0}^{n}(p+1)^3 - \sum_{k=0}^{n} k^3$.

La seconde somme vaut aussi $\sum_{p=0}^{n} p^3$ puisque les variables sont muettes.

On a donc en fusionnant : $C_{n+1} - C_n = \sum_{p=0}^{n}\left((p+1)^3 - p^3\right)$.

On développe par la formule du binôme : $C_{n+1} - C_n = \sum_{p=0}^{n}\left(3.p^2 + 3.p + 1\right)$.

On sépare en trois sommes déjà nommées dans l'énoncé : $C_{n+1} - C_n = 3.B_n + 3.A_n + n + 1$.

On égale les deux calculs : $(n+1)^3 = 3.B_n + 3.A_n + n + 1$, et on extrait $B_n = \frac{n.(n+1).(2.n+1)}{6}$ *(et c'est bien toujours un entier naturel).*

Pour C_n, on définit la matrice de terme général $i.k$: $\begin{matrix} 1.1 & 1.2 & 1.3 & \dots & 1.n \\ 2.1 & 2.2 & 2.3 & \dots & 2.n \\ 3.1 & 3.2 & 3.3 & \dots & 3.n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ n.1 & n.2 & n.3 & \dots & n.n \end{matrix}$ et on en somme tous les termes.

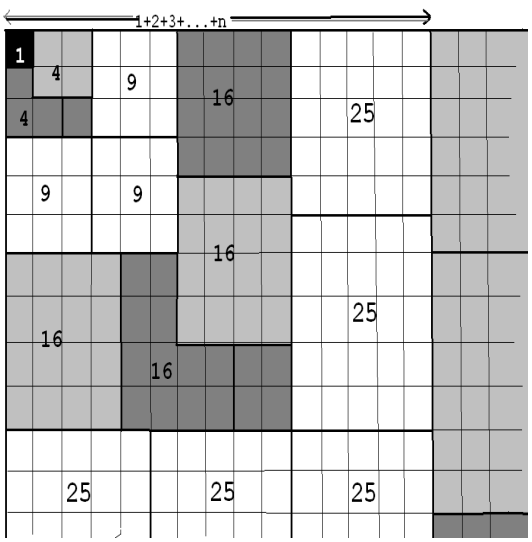
Il s'agit de $\sum_{\substack{i\leqslant n \\ k\leqslant n}} i.k$ qui se sépare *(indépendance des variables de sommation)* en $\Big(\sum_{i\leqslant n} i\Big).\Big(\sum_{k\leqslant n} k\Big)$. Les deux sommes sont égales, c'est $\Big(A_n\Big)^2$, soit encore justement $\Big(\frac{n.(n+1)}{2}\Big)^2$.

Mais on peut aussi sommer par zones visuellement délimitées comme suit

$1.1 \dots .$	$. \; 1.2 \; . \dots .$	$. \; . \; 1.3 \dots .$		$. \; . \; . \dots 1.n$
$. \dots .$	$2.1 \; 2.2 \; . \dots .$	$. \; . \; 2.3 \dots .$		$. \; . \; . \dots 2.n$
$. \dots .$	$. \; . \; . \dots .$	$3.1 \; 3.2 \; 3.3 \dots .$	jusqu'à	$. \; . \; . \dots 3.n$
$\vdots \; \ddots \; \vdots$	$\vdots \; \vdots \; \ddots \; \vdots$	$\vdots \; \vdots \; \vdots \; \ddots \; \vdots$		$\vdots \; \vdots \; \vdots \; \ddots \; \vdots$
$. \dots .$	$. \; . \; . \dots .$	$. \; . \; . \dots .$		$n.1 \; n.2 \; n.3 \dots n.n$

Proprement, on écrit $\sum_{j=1}^{n}\Big(\sum_{Max(i,k)=j} i.k\Big)$.

A j fixé, une somme $\sum_{Max(i,k)=j} i.k$ est faite de deux sommes $\sum_{\substack{i=j \\ k\leqslant j}} i.k + \sum_{\substack{k=j \\ i<j}} i.k$ *(dans une des deux sommes, on accepte $i=k=j$, mais pas dans l'autre pour ne pas compter deux fois le même terme "en coin").*



On sort ce qui est indépendant de la variable de sommation :

$$\sum_{Max(i,k)=j} i.k = j.\sum_{k\leqslant j} k + j.\sum_{i<j} i.$$

On utilise le résultat du calcul de A_j :

$$\sum_{Max(i,k)=j} i.k = j.\frac{j.(j+1)}{2} + j.\frac{(j-1).j}{2} = j^3.$$

On a donc $\sum_{j=1}^{n}\Big(\sum_{Max(i,k)=j} i.k\Big) = \sum_{j=1}^{n} j^3 = C_n$.

On a donc bien finalement $(A_n)^2 = \sum_{\substack{i\leqslant n \\ k\leqslant n}} i.k = C_n$.

Théorème du rang :
• version isomorphisme : toute application linéaire entre deux espaces vectoriels induit un isomorphisme entre un supplémentaire du noyau et l'ensemble image.
• version base : si f est une application linéaire de $(E,+,.)$ dans $(F,+,.)$, avec $(\overrightarrow{e_1},\dots\overrightarrow{e_k})$ une base de $Ker(f)$ qu'on complète en base de $(E,+,.)$: $(\overrightarrow{e_1},\dots\overrightarrow{e_k},\overrightarrow{e_{k+1}},\dots\overrightarrow{e_n})$, alors $(f(\overrightarrow{e_{k+1}}),\dots\overrightarrow{f(e_n)})$ est une base de $Im(f)$.
• version dimensions : si f est une application linéaire de $(E,+,.)$ dans $(F,+,.)$, alors $\dim(Im(f)) = \dim(E) - \dim(Ker(f))$.

On prend donc f linéaire de $(E,+,.)$ dans $(F,+,.)$, espaces vectoriels sur un même corps $(\mathbb{K},+,.)$ *(on*

ne supposera E de dimension finie que pour les versions "base" et "dimension", et la dimension de $(F,+,.)$ n'a aucune importance).

Version "isomorphisme".

On note S un suppplémentaire de $Ker(f)$ dans E, on a donc $E = Ker(f) \oplus S$ *(tout vecteur de E se décompose d'une façon unique comme somme d'un vecteur de $Ker(f)$ et d'un vecteur de S).*
On sait déjà que f reste linéaire sur le sous-espace vectoriel S.
On notera $\overline{f}$ l'application f quand on la considèrera de S dans F *(cas particulier).*
L'image de tout vecteur de S est dans $Im(f)$, comme image d'un vecteur de E (c'est $Im(\overline{f}) \subset Im(f)$, et on verra $Im(\overline{f}) = Im(f)$).
$\overline{f}$ est alors injective de S dans $Im(f)$. On passe pour celà par le noyau de $\overline{f}$. On prend un vecteur $\overrightarrow{s}$ de S d'image nulle par $\overline{f}$. Il vérifie $\overline{f}(\overrightarrow{s}) = \overrightarrow{0}$. Le vecteur $\overrightarrow{s}$, vu comme vecteur de E est donc dans $Ker(f)$. Etant à la fois dans $Ker(f)$ et S, il est nul *(somme directe).*
Enfin, $\overline{f}$ est surjective de S sur $Im(f)$. On prend un vecteur $\overrightarrow{v}$ dans $Im(f)$. Par définition, il a au moins un antécédent $\overrightarrow{u}$ dans E. Par définition de la somme *(directe)*, $\overrightarrow{u}$ s'écrit $\overrightarrow{k} + \overrightarrow{s}$ avec $\overrightarrow{k}$ dans $Ker(f)$ et $\overrightarrow{s}$ dans S. On a alors $\overrightarrow{v} = f(\overrightarrow{u}) = f(\overrightarrow{k} + \overrightarrow{s}) = f(\overrightarrow{k}) + f(\overrightarrow{s}) = \overline{f}(\overrightarrow{s})$. Le vecteur $\overrightarrow{v}$ de $Im(f)$ a donc un antécédent $\overrightarrow{s}$ dans S *(unique comme vu plus haut).*

Version "bases".

On suppose $(E,+,.)$ de dimension finie n. Comme $Ker(f)$ est un sous-espace vectoriel de $(E,+,.)$, il est aussi de dimension finie, et par théorème de la base incomplète *(en partant de la famille vide)*, on peut le doter d'une base *(éventuellement vide si f est injective)* : $(\overrightarrow{e_1}, \dots \overrightarrow{e_k})$ avec $k = \dim(Ker(f)) \leqslant n$.
Encore par théorème de la base incomplète, on agrandit en base de E : $(\overrightarrow{e_1}, \dots \overrightarrow{e_k}, \overrightarrow{e_{k+1}}, \dots \overrightarrow{e_n})$.
On sait déjà que la famille image de cette base $(f(\overrightarrow{e_1}), \dots f(\overrightarrow{e_k}), f(\overrightarrow{e_{k+1}}), \dots f(\overrightarrow{e_n}))$ est génératrice de $Im(f)$. Comme $f(\overrightarrow{e_1})$ à $f(\overrightarrow{e_k})$ sont nuls, on a déjà $(f(\overrightarrow{e_{k+1}}), \dots f(\overrightarrow{e_n}))$ qui engendre $Im(f)$.
On montre à présent que cette famille est libre. On part d'une combinaison $\alpha_{k+1}.f(\overrightarrow{e_{k+1}}), \dots + \alpha_n.f(\overrightarrow{e_n})$ qu'on suppose nulle *(objectif : les α_i snt nuls).* Par linéarité, on a donc $f(\alpha_{k+1}.\overrightarrow{e_{k+1}}, \dots + \alpha_n.\overrightarrow{e_n}) = \overrightarrow{0_F}$.
On reconnaît que $\alpha_{k+1}.\overrightarrow{e_{k+1}}, \dots + \alpha_n.\overrightarrow{e_n}$ est dans $Ker(f)$ et s'écrit donc $\beta_1.\overrightarrow{e_1} + \dots + \beta_k.\overrightarrow{e_k}$. On écrit alors $\beta_1.\overrightarrow{e_1} + \dots + \beta_k.\overrightarrow{e_k} - \alpha_{k+1}.\overrightarrow{e_{k+1}} - \dots - \alpha_n.\overrightarrow{e_n} = \overrightarrow{0_E}$. Par liberté de la base : les α_i et les β_j sont nuls.

Version "dimensions".

Avec la démonstration précédente, il suffit de compter les cardinaux des bases :

base de $Ker(f)$	base de E	base de $Im(f)$
$(\overrightarrow{e_1}, \dots \overrightarrow{e_k})$	$(\overrightarrow{e_1}, \dots \overrightarrow{e_k}, \overrightarrow{e_{k+1}}, \dots \overrightarrow{e_n})$	$(f(\overrightarrow{e_{k+1}}), \dots f(\overrightarrow{e_n}))$
k	n	$n-k$

On a bien $\dim(Im(f)) = \dim(E) - \dim(Ker(f))$.
On préfèrera cette formulation à $\dim(Im(f)) + \dim(Ker(f)) = \dim(E)$, afin d'éloigner $Ker(f)$ et $Im(f)$ l'un de l'autre car ce ne sont pas des sous-espaces vectoriels d'un même espace vectoriel.

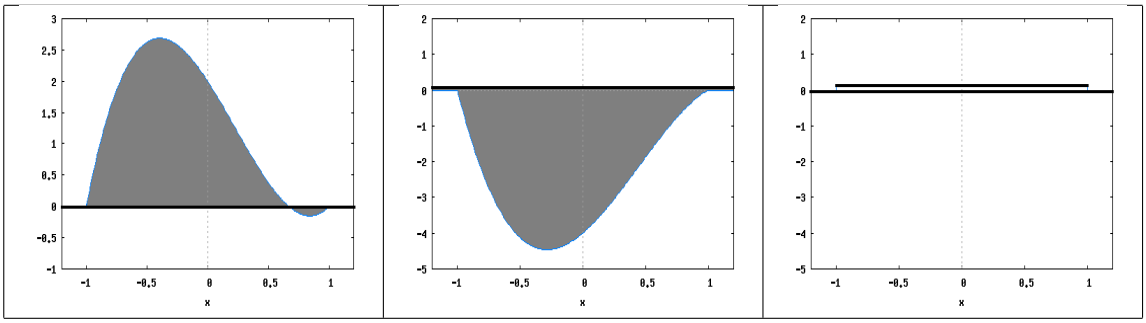
Théorème de Rolle : soit φ continue de $[a,\ b]$ dans $\mathbb{R}$ et dérivable au moins sur $]a,\ b[$, vérifiant $\varphi(a) = \varphi(b)$, alors il existe au moins un point c de $]a,\ b[$ vérifiant $\varphi'(c) = 0$.
Théorème des accroissements finis : soit f continue de $[a,\ b]$ dans $\mathbb{R}$ et dérivable au moins sur $]a,\ b[$, alors il existe au moins un point c de $]a,\ b[$ vérifiant $f(b) - f(a) = f'(c).(b - a)$.

Théorème de Rolle en cascade : soit f n fois dérivable de I (intervalle de $\mathbb{R}$) dans $\mathbb{R}$, admettant la même valeur en $n + 1$ points, alors il existe au moins un pointoù $f^{(n)}$ s'annule.

Théorème sur les variations des fonctions sur un intervalle par le signe de la dérivée : une application numérique dérivable dont la dérivée est positive sur un intervalle y est croissante.

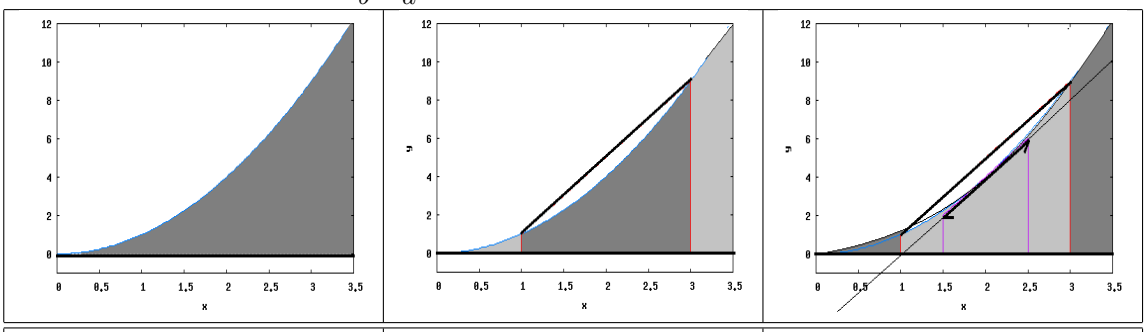
Formule de l'Hopital : si f et g sont continues de $[a,\ b]$ dans $\mathbb{R}$, dérivables au moins sur $]a,\ b[$, avec g' strictement positive, alors il existe au moins un point c vérifiant $\dfrac{f(b) - f(a)}{g(b) - g(a)} = \dfrac{f'(c)}{g'(c)}$.

On commence par le théorème de Rolle, avec φ continue de $[a,\ b]$ dans $\mathbb{R}$ et dérivable au moins sur $]a,\ b[$. ON ajoute l'hypothèse $\varphi(a) = \varphi(b)$.
Par théorème de compacité *(continue sur un segment)*, φ est bornée et atteint ses bornes *(maximum atteint en α et minimum atteint en β)*.
• Si le maximum est atteint en α de $]a,\ b[$ *(ouvert)*, alors on étudie la dérivabilité de φ à droite de α et à gauche. Chaque $\dfrac{\varphi(\alpha) - \varphi(x)}{\alpha - x}$ pour x entre a et α est positif *(maximum)*. La limite quand x tend vers α par valeur inférieure est positive ou nulle (et c'est $\varphi'(\alpha)$). Chaque $\dfrac{\varphi(\alpha) - \varphi(x)}{\alpha - x}$ pour x entre α et b est négatif *(maximum)*. La limite quand x tend vers α par valeur supérieure est négative ou nulle *(et c'est encore $\varphi'(\alpha)$)*. Par antisymétrie, $\varphi'(\alpha)$ est nul.
• Si le maximum est atteint en α qui n'est pas dans $]a,\ b[$, c'est que α est en a ou en b puisque $\varphi(a) = \varphi(b)$. On regarde alors le points β où le minimum est atteient, avec deux sous cas :
◦ β est strictement entre a et b. On refait alors le raisonnement précédent : chaque $\dfrac{\varphi(\beta) - \varphi(x)}{\beta - x}$ pour x entre a et β est négatif et la limite quand x tend vers β par valeur inférieure est positive ou nulle, tandis que chaque $\dfrac{\varphi(\beta) - \varphi(x)}{\beta - x}$ pour x entre β et b est négatif, la limite quand x tend vers β par valeur supérieure est positive ou nulle. Par antisymétrie de l'ordre, $\varphi'(\beta)$ est nul.
◦ β est en a ou b. φ est alors constante. Et sa dérivée est nulle en tout point de $]a,\ b[$.
Dans nos différents cas et sous cas, il suffit de prendre $c = \alpha$ ou $c = \beta$ ou enfin $c = \dfrac{a + b}{2}$, on a bien $\varphi'(c) = 0$.
Pour les applications de $\mathbb{R}$ dans $\mathbb{C}$, le résultat n'est plus valable comme le prouve l'application $x \to e^{i.x}$ sur le segment $[0,\ 2.\pi]$.



cas $\alpha \in]a,\ b[$	cas $\alpha = a$, $\beta \in]a,\ b[$	cas $\alpha = a$ et $\beta = b$

Si l'on n'a plus d'hypothèse $f(a) = f(b)$, on peut créer une fonction auxiliaire qui étudie en fait la distance entre la corde et le graphe : $x \to f(x) - \left(\dfrac{f(b)-f(a)}{b-a}.(x-a) + f(a)\right)$, que l'on va noter φ.
Cette application est continue sur $[a,\ b]$, dérivable au moins sur $]a,\ b[$, et surtout, vérifie $\varphi(a) = \varphi(b)$ *(d'ailleurs égal à 0)* par construction.
Le théorème de Rolle donne l'existence d'au moins un c vérifiant $\varphi'(c) = 0$. Cette dernière égalité donne précisément $f'(c) = \dfrac{f(b)-f(a)}{b-a}$.



le graphe	la corde	la tangente

une accroissement infinitésimal coïncide avec un accroissement "fini", ce qui s'écrit $\left(\dfrac{dy}{dx}\right)_{x=c} = \frac{\Delta y}{\Delta x}$

Le théorème de Rolle en cascade se démontre par récurrence sur le nombre de points où la fonction prend la même valeur.
Le cas $n = 0$ correspond exactement au théorème de Rolle : la fonction dérivable qui prend la même valeur en deux points a une dérivée qui s'annule au moins une fois.

Pour l'hérédité, on suppose que toute application numérique qui prend la même valeur en $n+1$ points d'un intervalle a sa dérivée n^{ieme} qui s'annule au moins une fois. On prend alors une application f *($n+1$ fois dérivable)* qui prend la même valeur en $n+2$ points d'un intervalle, qu'on va noter a_0 jusqu'à a_{n+1}, et qu'on va supposer triés par ordre croissant.
On applique le théorème de Rolle sur chacun des intervalles $[a_k,\ a_{k+1}]$ *(f y est continue, dérivable, et prend la même valeur aux deux extrémités).* Pour chacun, il existe au moins un point α_k de l'intervalle ouvert $]a_k,\ a_{k+1}[$ où f' s'annule :
$a_0 < \alpha_0 < a_1 < \alpha_1 < a_2 \ldots < \alpha_n < a_{n+1}$
L'application f' est alors $n+1$ fois dérivable et prend la même valeur *(nulle)* en $n+1$ points distincts *(les α_k pour k de 0 à n).* Par hypothèse de récurrence, sa dérivée n^{ieme} s'annule au moins une fois. En ce point β on a $(f')^{(n)}(\beta = 0$ c'est à dire $f^{(n+1)}(\beta) = 0$.

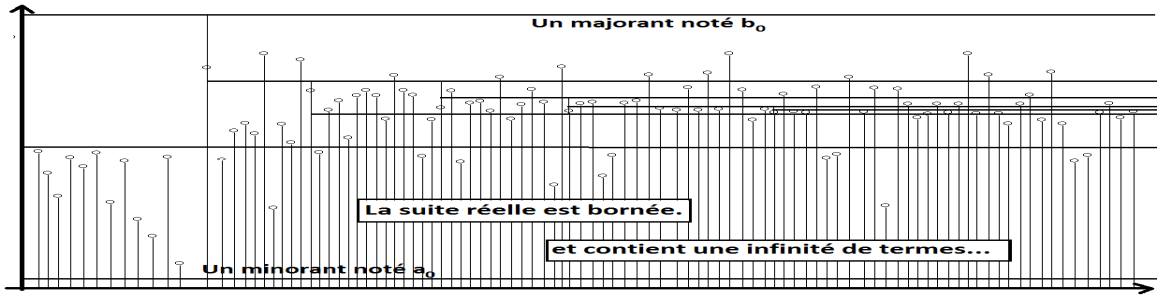
On prend à présent f dérivable de I *(intervalle de $\mathbb{R}$)* dans $\mathbb{R}$, et on suppose f' positive ou nulle sur I.

On va prouver "directement" que f est croissante.
On se donne a et b dans I vérifiant $a < b$ (objectif $f(a) < f(b)$).
On est en droit sous nos hypothèses d'appliquer le théorème des accroissements finis à f entre a et b : il existe un c vérifiant $f(b) - f(a) = (b-a).f'(c)$. Tous les termes du second membre sont positifs, le premier membre l'est aussi, et c'était notre objectif.
Le sens "f dérivale et croissante implique f' psitive" est bien plus simple à prouver, puisqu'il résulte d'un passage à la limite (dont l'existence est supposée) dans les taux d'accroissement de la forme $\dfrac{f(x+h)-f(x)}{h}$ quand h tend vers 0.

Cette fois, on a f et g continues de $[a,\ b]$ dans $\mathbb{R}$, dérivables au moins sur $]a,\ b[$, et on suppose de plus g' strictement positive sur $]a,\ b[$.
Il s'ensuit que g est strictement croissante, on a donc $g(b) > g(a)$.
On n'obtient pas le résultat voulu en appliquant le théorème des accroissements finis à f puis à g, il faut un "changement d'échelle commun".
On définit l'application auxiliaire φ inspirée de la preuve du théorème des accroissements finis $x \to f(x) - \Big(\dfrac{f(b)-f(a)}{g(b)-g(a)}.\big(g(x)-g(a)\big) + f(a)\Big)$.
Elle est continue de $[a,\ b]$ dans $\mathbb{R}$, dérivable sur $]a,\ b[$, et prend la même valeur *(nulle)* en a et b. Sa dérivée $x \to f'(x) - \dfrac{f(b)-f(a)}{g(b)-g(a)}.g'(x)$ s'annule au moins une fois en un point c de $]a,\ b[$. En ce point, on a par produits en croix : $\dfrac{f(b)-f(a)}{g(b)-g(a)} = \dfrac{f'(c)}{g'(c)}$.
Dans le cas où g est l'application identité, on retrouve le théorème des accroissements finis.

Théorème de Bolzano-Weiestrass réel : de toute suite réelle bornée, on peut extraire au moins une sous-suite convergente.
Version complexe : de toute suite complexe bornée, on peut extraire au moins une sous-suite convergente.

Soir (u_n) une suite réelle bornée par deux réels qu'on va appeler α_0 et β_0 *(pour tout n de $\mathbb{N}$, on a $\alpha_0 \leqslant u_n \leqslant \beta_0$).*

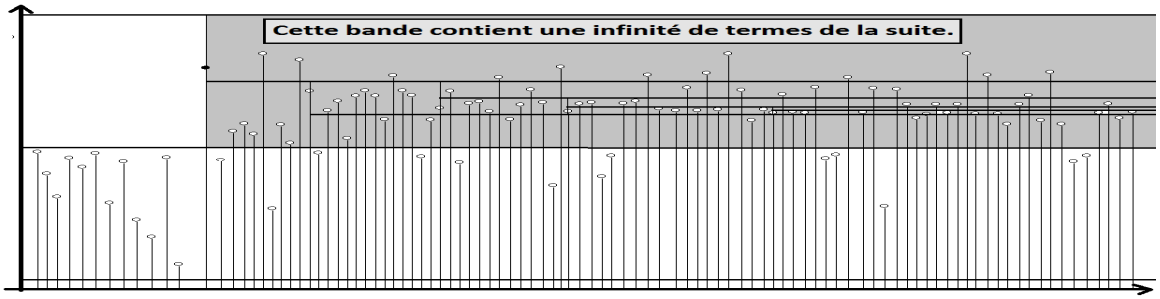


On pose alors : $\gamma_0 = \dfrac{\alpha_0+\beta_0}{2}$ | $A_0 = \{n \in \mathbb{N} \mid \alpha_0 \leqslant a_n \leqslant \gamma_0\}$ | $B_0 = \{n \in \mathbb{N} \mid \gamma_0 < a_n \leqslant \beta_0\}$
On a immédiatement : $A_0 \cup B_0 = \mathbb{N}$. L'un des deux ensembles A_0 ou B_0 est donc infini *(et peut être même les deux).*

Si A_0 est infini	on pose $\varphi(0) = ppe(A_0)$	$N_0 = A_0 - \{\varphi(0)\}$	$\alpha_1 = \alpha_0$	$\beta_1 = \gamma_0$
Si A_0 est fini alors B_0 est infini	on pose $\varphi(0) = ppe(B_0)$	$N_0 = B_0 - \{\varphi(0)\}$	$\alpha_1 = \gamma_0$	$\beta_1 = \beta_0$

Dans les deux cas, on a

$\alpha_0 \leqslant \alpha_1 \leqslant u_{\varphi(0)} \leqslant \beta_1 \leqslant \beta_0$	$\beta_1 - \alpha_1 = \dfrac{\beta_0-\alpha_0}{2}$	$Card(N_0) = +\infty$	$\forall n \in N_0,\ \alpha_1 \leqslant u_n \leqslant \beta_1$



On pose ensuite :

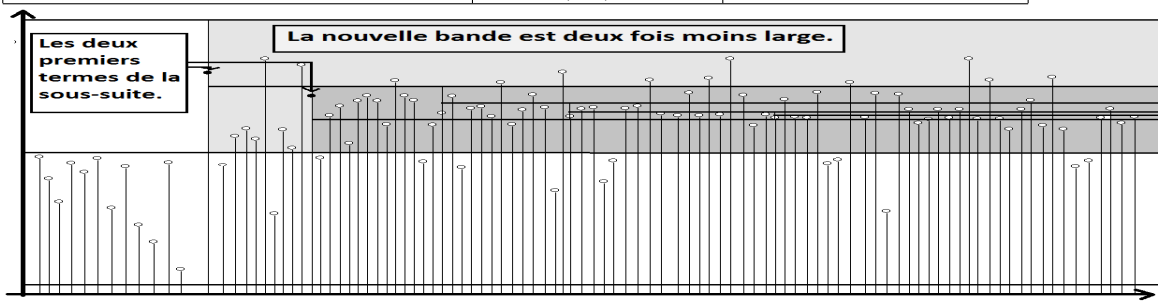
$\gamma_1 = \dfrac{\alpha_1 + \beta_1}{2}$	$A_1 = \{n \in N_0 \mid \alpha_1 \leqslant u_n \leqslant \gamma_1\}$	$B_1 = \{n \in N_0 \mid \gamma_1 < u_n \leqslant \beta_1\}$

On a alors $A_1 \cup B_1 = N_0$, ce qui prouve que l'un au moins des deux ensembles est infini. On refait la même disjonction de cas :

Si A_1 est infini	alors $\varphi(1) = ppe(A_1)$	$N_1 = A_1 - \{\varphi(1)\}$	$\alpha_2 = \alpha_1$	$\beta_2 = \gamma_1$
sinon (B_1 est infini)	alors $\varphi(1) = ppe(B_1)$	$N_1 = B_1 - \{\varphi(1)\}$	$\alpha_2 = \gamma_1$	$\beta_2 = \beta_1$

Dans les deux cas, on a

$\alpha_0 \leqslant \alpha_1 \leqslant \alpha_2 \leqslant u_{\varphi(1)} \leqslant \beta_2 \leqslant \beta_1 \leqslant \beta_0$	$\beta_2 - \alpha_2 = \dfrac{\beta_0 - \alpha_0}{4}$	$\varphi(0) < \varphi(1)$
	$Card(N_1) = +\infty$	$\forall n \in N_1,\ \alpha_2 \leqslant u_n \leqslant \beta_2$



Passons maintenant à la construction effective par récurrence de l'extraction φ.

On suppose qu'au rang p, on a obtenu

$\alpha_0 \leqslant \ldots \leqslant \alpha_p \leqslant u_{\varphi(p-1)} \leqslant \beta_p \leqslant \ldots \leqslant \beta_0$	$\beta_p - \alpha_p = \dfrac{\beta_0 - \alpha_0}{2^p}$	$\varphi(0) < \varphi(1) < \ldots < \varphi(p-1)$
	$Card(N_{p-1}) = +\infty$	$\forall n \in N_{p-1},\ \alpha_p \leqslant u_n \leqslant \beta_p$

On pose encore

$\gamma_p = \dfrac{\alpha_p + \beta_p}{2}$	$A_p = \{n \in N_{p-1} \mid \alpha_p \leqslant u_n \leqslant \gamma_p\}$	$B_p = \{n \in N_{p-1} \mid \gamma_p < u_n \leqslant \beta_p\}$

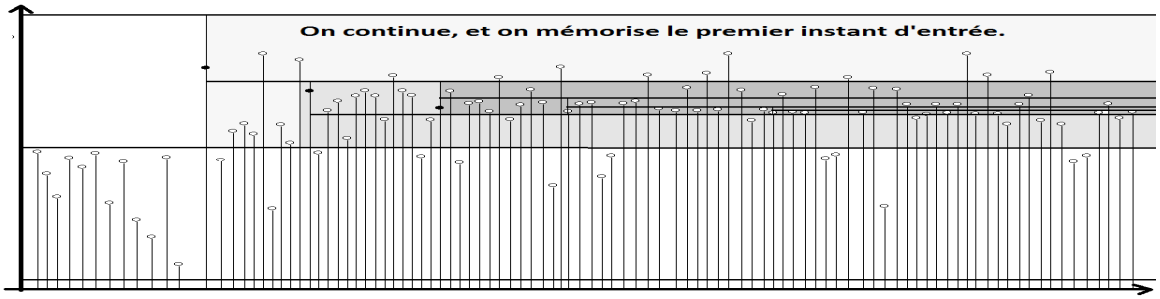
.

Ayant encore $A_p \cup B_p$ de cardinal infini *(c'est N_{p-1})*, on choisit suivant que A_p ou B_p est infini :

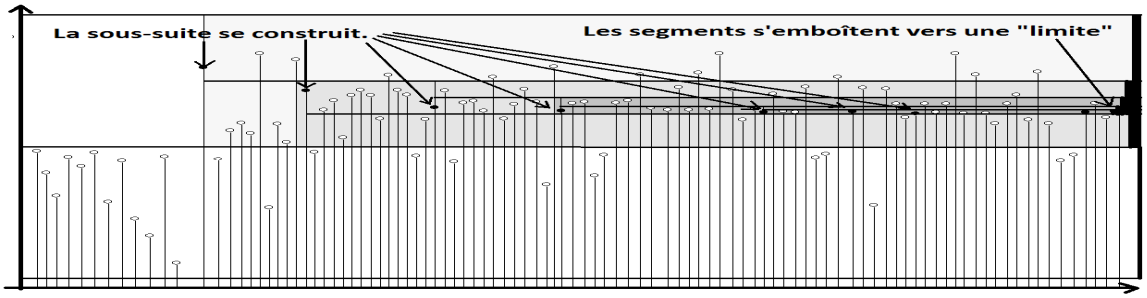
Si A_p est infini	alors $\varphi(p) = ppe(A_p)$	$N_p = A_p - \{\varphi(p)\}$	$\alpha_{p+1} = \alpha_p$	$\beta_{p+1} = \gamma_p$
sinon	alors $\varphi(p) = ppe(B_p)$	$N_p = B_p - \{\varphi(p)\}$	$\alpha_{p+1} = \gamma_p$	$\beta_{p+1} = \beta_p$

On est assuré qu'on a encore

$\alpha_0 \leqslant \ldots \leqslant \alpha_{p+1} \leqslant u_{\varphi(p)} \leqslant \beta_{p+1} \leqslant \ldots \leqslant \beta_0$	$\beta_{p+1} - \alpha_{p+1} = \dfrac{\beta_0 - \alpha_0}{2^{p+1}}$	$\varphi(0) < \ldots < \varphi(p-1) < \varphi(p)$
	$Card(N_p) = +\infty$	$\forall n \in N_p,\ \alpha_{p+1} \leqslant u_n \leqslant \beta_{p+1}$



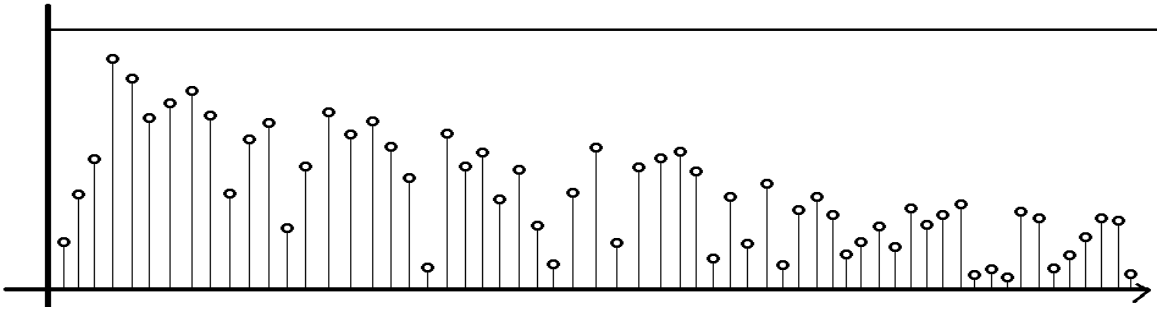
φ est une application strictement croissante de $\mathbb{N}$ dans $\mathbb{N}$ *(c'est pour s'en assurer qu'on prend à chaque fois* $N_p = A_p - \{\varphi(p)\}$ *ou* $N_p = B_p - \{\varphi(p)\}$*, ce qui ne fait qu'enlever un élément à un ensemble infini).*
On reconnaît que les deux suites encadrantes (α_p) et (β_p) forment un couple de suites réelles adjacantes. Elles convergent donc toutes deux vers une même limite λ.
Pour tout p, on a $\alpha_{p+1} \leqslant u_{\varphi(p)} \leqslant \beta_{p+1}$, ce qui permet par théorème d'encadrement de forcer $(u_{\varphi(p)})$ à converger aussi vers λ.
On a donc bien extrait *(explicitement*[3]*)* une sous-suite de (u_n) qui converge *(vers* λ*).*



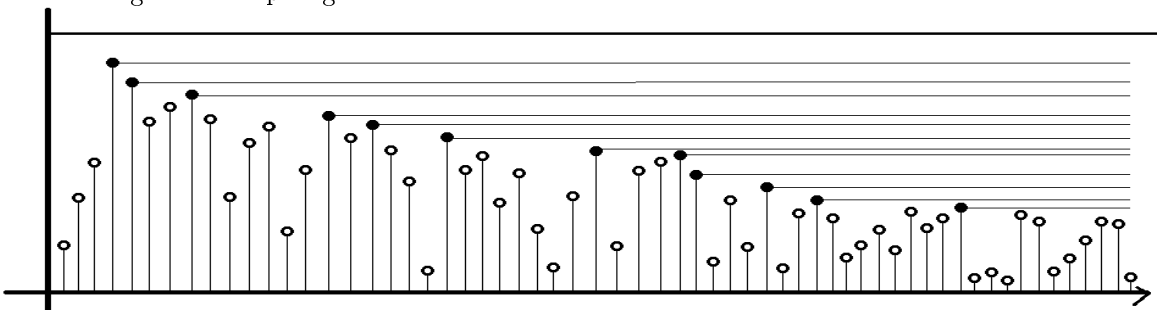
On prend une suite complexe bornée (z_n) qu'on écrit sous la forme $(u_n + i.v_n)$ avec les deux suites u et v réelles.
Comme la suite z est bornée, les deux suites u et v le sont aussi.
Comme la suite (u_n) est bornée, on peut en extraire au moins une sous-suite $(u_{\varphi(p)})$ qui converge *(vers un réel* λ*).*
La sous-suite $(v_{\varphi(p)})$ est alors bornée *(extraite d'une suite bornée).* Par le théorème de Bolzano-Weierstrass réel, on peut en extraire une sous-(sous-)suite $(v_{\varphi(\psi(q))})$ qui converge *(vers un réel* μ*).*
La sous-(sous-)suite $(u_{\varphi(\psi(q))})$ continue à converger vers λ.
Par théorème algébrique, $(u_{\varphi(\psi(q))} + i.v_{\varphi(\psi(q))})$ converge vers $\lambda + i.\mu$.
L'extraction $\varphi \circ \psi$ permet de faire converger une suite extraite de (z_n).
Les deux extractions doivent se faire l'une après l'autre et non pas "en parallèle".

Pour les suites réelles bornées, il existe aussi une autre démonstration :
si l'on ne peut pas extraire "facilement" une sous-suite décroissante, alors on peut extraire une sous-suite croissante.
On prend donc une suite réelle (u_n) bornée par α_0 et β_0.
On définit l'esemble d'indices suivant : $\mathbb{A} = \{n \in \mathbb{N} \mid \forall p \geqslant n,\ u_p \leqslant u_n\}$ (il s'agit des indices des termes qui majorent tous les termes qui suivent).
$\mathbb{A}$ est une partie de $\mathbb{N}$ qui est soit infinie, soit finie.
Premier cas : si $\mathbb{A}$ est infini, alors on en indexe les éléments par ordre croissant : $\varphi \begin{array}{ccc} \mathbb{N} & \longrightarrow & \mathbb{A} \\ n & \longmapsto & \varphi(n) \end{array}$
($\varphi(0)$ est le plus petit élément de $\mathbb{A}$, $\varphi(1)$ est le plus petit élément de $\mathbb{A} - \{\varphi(0)\}$ et ainsi de suite).

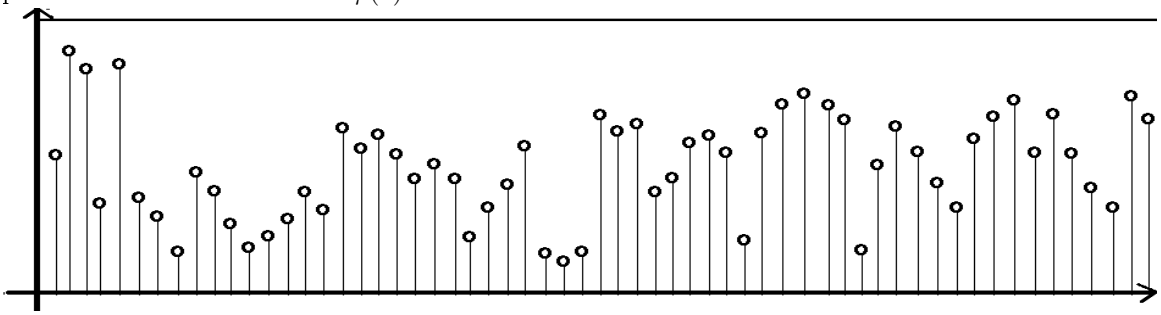
[3] *la construction choisie ici la fait converger vers la plus petite valeur d'adhérence, il se peut qu'on ait le choix dans le cas de suites ayant plusieurs valeurs d'adhérence*



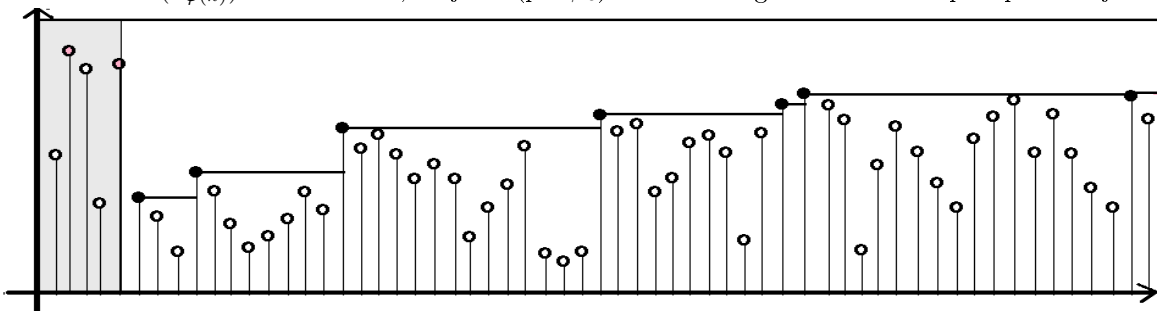
Par construction, chaque indice $\varphi(k)$ vérifie $\forall p \geqslant \varphi(k),\ u_p \leqslant u_{\varphi(k)}$; en particulier $u_{\varphi(k+1)} \leqslant u_{\varphi(k)}$.
La suite $(u_{\varphi(k)})$ est décroissante. Elle est extraite de la suite (a_n), donc elle est minorée.
Elle converge vers son plus grand minorant.



Second cas : si $\mathbb{A}$ est fini, alors au delà d'un certain entier M, tous les entiers sont dans $\mathbb{A}^c$.
On pose alors $\varphi(0) = M + 1$. Par définition de $\varphi(0) \notin \mathbb{A}$, il existe au moins un élément p plus grand que $\varphi(0)$ vérifiant $u_p > u_{\varphi(0)}$. On prend le premier d'entre eux (qui ne peut pas être égal à $\varphi(0)$ par inégalité stricte) et on le note $\varphi(1)$.
On recommence : $\varphi(1)$ n'est pas dans $\mathbb{A}$, il existe donc au moins un indice p vérifiant $u_p > u_{\varphi(1)}$. Le premier d'entre eux sera noté $\varphi(2)$.



De proche en proche, on construit φ vérifiant $\varphi(k+1) > \varphi(k)$ pour tout k (ainsi que $\varphi(k+1) > \varphi(k)$).
La sous-suite $(u_{\varphi(k)})$ est croissante, majorée (par β_0). Elle converge donc vers son plus petit majorant.



Dans les deux cas, on a construit une sous-suite monotone bornée, donc convergente.

Déterminant de VanDerMonde : si les a_k (pour k de 0 à $n-1$) sont n complexes, alors le déterminant de la matrice $V[a_0, \dots a_n]$ de terme général $(a_i)^k$ (i et k de 0 à $n-1$) est égal à $\prod_{i<j}(a_j - a_i)$ (formé de $\frac{n.(n-1)}{2}$ termes).

On démontre ce résultat par récurrence sur n.
• Pour n égal à 0, la formule est cohérente par pure logique *(déterminant de matrice vide, produit vide).*
• Pour n égal à 1, le déterminant est celui de $\left|\ (a_0)^0\ \right|$, il vaut 1, et le produit est encore vide.
• Pour n égal à 2, le déterminant se calcule : $\begin{vmatrix} 1 & a_0 \\ 1 & a_1 \end{vmatrix} = (a_1 - a_0)$, c'est bien le produit à un terme attendu.
• On peut aussi vérifier pour n égal à 3 : $\begin{vmatrix} 1 & a_0 & (a_0)^2 \\ 1 & a_1 & (a_1)^2 \\ 1 & a_2 & (a_2)^2 \end{vmatrix} = (a_1 - a_0).(a_2 - a_0).(a_2 - a_1)$.
On suppose à présent le résultat vrai au rang n, et on prend la matrice de taille $n+1$: $V[a_0, \dots a_{n-1}, x] = \begin{pmatrix} 1 & a_0 & \dots & (a_0)^{n-1} & (a_0)^n \\ 1 & a_1 & \dots & (a_1)^{n-1} & (a_1)^n \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & a_{n-1} & \dots & (a_{n-1})^{n-1} & (a_{n-1})^n \\ 1 & x & \dots & x^{n-1} & x^n \end{pmatrix}$.
Si deux des a_j sont égaux, le déterminant est nul, et bien égal à $\prod_{i<j\leqslant n}(a_j - a_i)$. On passe donc au cas où tous les a_j sont distincts.
On développe $\det(V[a_0, \dots a_{n-1}, x])$ par rapport à la dernière ligne. On a un polynôme en x, dont le terme dominant est $x^n.det(V[a_0, \dots a_{n-1}])$.
Ce polynôme est nul si x est égal à l'un des a_k, car il y a alors deux lignes égales.
Il se factorise donc par $\prod_{k=0}^{n-1}(x - a_k)$. Comme de terme est d'ores et déjà de degré n, et comme on connaît le coefficient dominant, ce polynôme est $det(V[a_0, \dots a_{n-1}]).\prod_{k=0}^{n-1}(x - a_k)$.
On décide d'appeler x plus simplement a_n et on a bien
$det(V[a_0, \dots a_n]) = det(V[a_0, \dots a_{n-1}]).\prod_{k=0}^{n-1}(a_n - a_k) = \prod_{i<j<n}(a_j - a_i).\prod_{k=0}^{n-1}(a_n - a_k) = \prod_{i<j\leqslant n}(a_j - a_i)$.

Noyau et injectivité : une application linéaire f de $(E, +, .)$ dans $(F, +, .)$ est injective si et seulement si son noyau est réduit à $\overrightarrow{0_E}$.

Pour le premier sens, on prend f linéaire et injective de $(E, +, .)$ dans $(F, +, .)$.
On rappelle la définition : $Ker(f) = \{\overrightarrow{u} \in E \mid f(\overrightarrow{u}) = \overrightarrow{0_F}\}$.
Déjà, $\overrightarrow{0_E}$ est dans le noyau, puisque $f(\overrightarrow{0_E}) = f(0 \times \overrightarrow{0_E}) = 0 \times f(\overrightarrow{0_E}) = \overrightarrow{0_F}$ par linéarité.
Tout autre élément $\overrightarrow{u}$ de $Ker(f)$ vérifie $f(\overrightarrow{u}) = \overrightarrow{0_F} = f(\overrightarrow{0_E})$. Par injectivité, $\overrightarrow{u}$ est forcément égal à $\overrightarrow{0_E}$.

Pour le second sens, on suppose le noyau réduit au seul vecteur nul, et on montre l'injectivité de f.
On prend deux vecteurs $\overrightarrow{a}$ et $\overrightarrow{b}$ ayant la même image *(objectif : ils sont égaux).* On écrit $f(\overrightarrow{a}) = f(\overrightarrow{b})$, puis $f(\overrightarrow{a}) - f(\overrightarrow{b}) = \overrightarrow{0_F}$, et même $f(\overrightarrow{a} - \overrightarrow{b}) = \overrightarrow{0_F}$ par linéarité. $\overrightarrow{a} - \overrightarrow{b}$ est dans le noyau, il est donc nul. On est bien arrivé à $\overrightarrow{a} = \overrightarrow{b}$.

On note que l'existence d'un noyau non trivial transmet le défaut d'injectivité partout.
Pour f linéaire de $(E,+,.)$ dans $(F,+,.)$, l'équation $f(\overrightarrow{u}) = \overrightarrow{v}$ d'inconnue $\overrightarrow{u}$ et de paramètre $\overrightarrow{v}$ se résout ainsi :

$\overrightarrow{v} \in Im(f)$	$\exists \overrightarrow{u_0} \in E,\ f(\overrightarrow{u_0}) = \overrightarrow{v}$	$S = \{\overrightarrow{u_0} + \overrightarrow{k} \mid \overrightarrow{k} \in Ker(f)\}$
$\overrightarrow{v} \notin Im(f)$	$\forall \overrightarrow{u} \in E,\ f(\overrightarrow{u}) \neq \overrightarrow{v}$	$S = \emptyset$

De plus, si B est un sous-espace vectoriel de $(F,+,.)$ alors on a $Ker(f) \subset f^{-1}(B)$.
Enfin, si A est un sous-espace vectoriel de $(E,+,.)$ alors on a $f^{-1}(f(A)) = A + Ker(f)$.