JP Wintenberger : bureau 204.
http://www-irma.u-strasbg.fr/ wintenb/

Problèmes de Mathématiques. 04-05.

Vélu : Mathématiques générales.
Dixmier : Cours de Mathématiques du premier cycle.

1. Racines des polynômes à coefficients complexes.

2. Suites définies par itération d'une fonction. Méthode de Newton pour la recherche numérique des zéros d'une fonction.

1.1. Polynômes à coefficients complexes.

Soit $\mathbf{C}$ les nombres complexes.
Un polynôme $P(X)$ à coefficients dans $\mathbf{C}$ s'écrit :

$$P(X) = a_0 + a_1 X + a_2 X^2 + ... + a_n X^n$$

les a_i étant des nombres complexes. Les a_i sont les coefficients. Notation : $\mathbf{C}[X]$. Si $a_n \neq 0$, P est de degré n : $\deg(P) = n$. Sinon, P est de degré $\leq n$. Se donner un polynôme de degré $\leq n$ revient à se donner $n+1$ nombres complexes. $P = a \in \mathbf{C}$ est un polynôme constant. Si $a \neq 0$, $P = a$ est de degré 0 ; si $a = 0$, on convient que $\deg(P) = -\infty$.
Si P est de degré d et si $n \geq d$, on peut écrire :

$$P(X) = a_0 + a_1 X + a_2 X^2 + ... + a_n X^n$$

avec $a_{d+1} = ... = a_n = 0$. C'est intéressant pour additionner deux polynômes P et Q. Si $n \geq \deg(P)$ et $n \geq \deg(Q)$, on peut écrire P comme ci-dessus et :

$$Q(X) = b_0 + b_1 X + b_2 X^2 + ... + b_n X^n.$$

On a :

$$(P+Q)(X) = (a_0 + b_0) + (a_1 + b_1)X + ... + (a_n + b_n)X^n.$$

Proposition. $\deg(P+Q) \leq \max(\deg(P), \deg(Q))$. On a $\deg(P+Q) = \max(\deg(P), \deg(Q))$ si $\deg(P) \neq \deg(Q)$.

Remarque. Compatible avec la convention $\deg(0) = -\infty$.
Preuve. On suppose $\deg(P) \geq \deg(Q)$ et on prend $n = \deg(P)$.

Multiplication des polynômes P et Q. Si P ou Q est $= 0$, $PQ = 0$. Sinon, soient d et d' les degrés de P et Q.

$$(PQ)(X) = \sum_{i=0}^{d+d'} c_i X^i,$$

avec $c_i = \sum_{j=0}^{i} a_j b_{i-j} = \sum_{j\geq 0, j'\geq 0, j+j'=i} a_j b_{j'}$.
Cas c_0, c_1, c_2, $c_{d+d'}$.
Exercice : $c_{d+d'-1}$.

Proposition. $\deg(PQ) = \deg(P) + \deg(Q)$. En particulier, si $P \neq 0$ et $Q \neq 0$, $PQ \neq 0$.

Si P et Q sont à coefficients dans $\mathbf{R}$, $\mathbf{Q}$ et $\mathbf{Z}$, idem $P+Q$ et PQ. Notation $\mathbf{R}[X]$, $\mathbf{Q}[X]$ et $\mathbf{Z}[X]$.

1.2. Enoncé du théorème d'Alembert-Gauss.

Soit $P \in \mathbf{C}[X]$. Soit $x \in \mathbf{C}$. On peut substituer à l'indéterminée X la valeur x. On obtient un nombre complexe $P(x)$:

$$P(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n.$$

On a $(P+Q)(x) = P(x) + Q(x)$ et $(PQ)(x) = P(x)Q(x)$.
Définition. On dit que x est racine de P si $P(x) = 0$.
Remarque triviale : 0 racine de P équivaut à $a_0 = 0$.

Théorème (d'Alembert-Gauss). Soit P un polynôme de degré $d \geq 1$ à coefficients dans $\mathbf{C}$. Alors, P a une racine complexe.

Remarques.

Enoncé au 17-ième siècle. Gauss en donne une preuve incomplète dans sa thèse (1799) et en publie deux preuves irréfutables en 1815-1816. Au 16-ième siècle, on a des formules avec radicaux pour les racines de polynômes de degré 3, et (par exemple Cardan) considère les racines imaginaires.

Faux dans $\mathbf{R}$: $P(X) = X^2 + 1$. Faux $d = 0$.

Trivial si $d = 1$.

$d = 2$. $P(X) = X^2 + a_1X + a_0$. On cherche à écrire $P(X) = (X + c)^2 + d$. Autrement dit, on pose $Y = X + c$, on définit Q par $Q(Y) = P(X)$, soit $Q(Y) = P(Y - c)$, ce qui donne une bijection $y \mapsto y - c$ des racines de Q vers les racines de P. Cela marche avec $c = a_1/2$.

Exercice. Plus généralement, si $P(X)$ est de degré $d \neq 0$, on peut choisir c tel que le terme de degré $d - 1$ de $Q(Y) = P(Y - c)$ soit nul.

On a $d = P(-c) = -\Delta/4$. On a à résoudre $y^2 = \Delta/4$.

- soit $\Delta = 0$, on a $y = 0$, $x = -c$

- soit $\Delta \neq 0$. On est ramené à l'équation : $\delta^2 = \Delta$. On pose $\Delta = \rho\ e^{i\theta}$ et $\delta = y\ e^{i\alpha}$ (rappel sur $e^{i\theta}$, θ défini modulo 2π , formule $e^{i(\theta+\theta')} = e^{i\theta}e^{i\theta'}$ équivalente aux formules de trigonométrie).

On a à résoudre :

$$y^2 = \Delta,\ \alpha = \theta/2 + k\pi,$$

$k \in \mathbf{Z}$. Deux solutions opposées pour δ selon la parité de k. $x = -c + \delta/2$.

Remarque. De même, le polynôme $X^n - a$, $a \neq 0$, a comme racines $\rho^{1/n}e^{i\theta/n+2\pi ik/n}$, pour $k = 0, 1, ..., n - 1$, si $a = \rho e^{i\theta}$.

1.3. Factorisation des polynômes à coefficients dans $\mathbf{C}$.

Division. Soient $A \in \mathbf{C}[X]$ et $B \in \mathbf{C}[X]$. On suppose $B \neq 0$. Alors, il existe $Q \in \mathbf{C}[X]$ et $R \in \mathbf{C}[X]$, $\deg(R) < \deg(B)$ avec $A = BQ + R$. B et R sont uniquement déterminés par ces conditions.

Remarque. Il se peut que $R = 0$; alors, on dit que B divise P.

Preuve.

Existence.

Si P est un polynôme, on abrège $\deg(P)$ eb $d(P)$.

Si $d(A) < d$, il n'y a rien à prouver. On prend : $B = 0$ et $R = A$.

Supposons $d(A) \geq d(B)$. Posons $A = a_{d(A)}X^{d(A)} + ...$ et $B = b_{d(B)}X^{d(B)} + ...$ Soient $Q_1 = (a_{d(A)}/b_{d(B)})X^{d(A)-d(B)}$ et $A_1 = A - Q_1B$. On a $A = BQ_1 + A_1$ et $d(A_1) < d(A)$. En effet, on a $d(A_1) \leq d(A)$. En fait $d(A_1) \leq d(A) - 1$ car le terme de degré $d(A)$ de A_1 est $a_{d(A)}X^{d(A)} - (a_{d(A)}/b_{d(B)})X^{d(A)-d(B)}b_{d(B)}X^{d(B)} = 0$.

On a $d(A_1) < d(A)$. Si $d(A_1) < d(B)$, on a gagné, on prend : $R = A_1$ et $Q = Q_1$. Si $d(A_1) \geq d(B)$, on recommence. On écrit $A_1 = BQ_2 + A_2$ avec $d(A_2) < d(A_1)$. On a :

$A = (Q_1 + Q_2)B + A_2$. Si $d(A_2) < d(B)$, on prend : $Q = Q_1 + Q_2$ et $R = A_2$. Sinon, on recommence. On obtient pour un i : $A = (Q_1 + Q_2 + ... + Q_i)B + A_i$, avec $d(A_i) < d(B)$. On prend $Q = Q_1 + Q_2 + ... + Q_i$ et $R = A_i$.

Remarque. On a ainsi un algorithme pour trouver Q et R. On voit que si A et B sont à coefficients dans $\mathbf{R}$ (resp. $\mathbf{Q}$), il en est de même de Q et R.

Exemple. $A = X^4 + X^3 + 1$ et $B = X^2 + 1$.

$A = X^2(X^2+1)+(X^3-X^2+1) = (X^2+1)(X^2+X)+(-X^2-X+1) = (X^2+1)(X^2+X-1)+(-X+2).$

Unicité. $A = BQ + R = CQ + D$. On a $(B - C)Q = D - R$. Comme $\deg(D - R) \leq d$ (ou $D = R$) et $d = \deg(Q) = d$, on a $B = C$ et $D = R$.

Soit $P \in \mathbf{C}[X]$ et $x \in \mathbf{C}$. Divisons P par $X - x$. On obtient $\lambda \in \mathbf{C}$ tel que : $P = (X - x)Q + \lambda$.

Proposition. On a $\lambda = P(x)$.

Preuve. On fait $X = x$ dans l' égalité $P = (X - x)Q + \lambda$.

Corollaire. Si x est racine de P, il existe Q tel que $P = (X - x)Q$.

Proposition. Soit $P = a_d X^d + ... + a_0 \in \mathbf{C}[X]$ de degré $d > 0$. Alors, on peut écrire :

$$P(X) = a_d \Pi_{i=1}^{d}(X - x_i),$$

les x_i étant des racines de P. De plus, si x est une racine de P, il existe un entier i tel que $x = x_i$.

Raisonnons par récurrence sur d. Si $d = 1$, $P(X) = a_1(X + a_0/a_1)$. Supposons $d > 1$. Le théorème d'Alembert-Gauss dit que P a une racine x_1. On peut donc écrire $P = (X - x_1)P_1$. On a $\deg(P_1) = d - 1$. On applique l'hypothèse de récurrence à P_1. Il existe des complexes c et x_2,..., x_d tels que $P_1(X) = c\Pi_{i=_2}^{d}(X - x_i)$. On a :

$$P(X) = c\Pi_{i=1}^{d}(X - x_i).$$

Le coefficient de X^d dans le membre de droite est c ; dans celui de gauche : a_d. Donc $c = a_d$. Les x_i sont des racines de P.

Si x est une racine de P, on a : $a_d\Pi_{i=1}^{d}(x - x_i) = 0$. Comme $a_d \neq 0$, il existe i tel que $x = x_i$.

Proposition. Soient $P = a\Pi_{i=1}^{d}(X - x_i) = a'\Pi_{j=1}^{d}(X - y_j)$ deux factorisations de P. Alors, $a = a'$ et les x_i sont égaux aux y_j, à l'ordre près.

Preuve. $a = a'$ est le coefficient du terme de degré d de P. On raisonne par récurrence sur le degré de P. x_1 est une racine de P, donc il existe j_1 tel que $x_1 = y_{j_1}$. On renumérote les y_j de sorte que $y_1 = y_{j_1}$. Le quotient de la division de P par $a_d(X - x_1)$ est $\Pi_{i=2}^{d}(X - x_i) = \Pi_{j=2}^{d}(X - y_j)$. On peut numéroter les y_j de sorte que $x_i = y_i$ (hypothèse de récurrence).

Remarque. On peut aussi dire que l'on a une bijection σ de $\{1, 2, ..., n\}$ dans lui-même telle que $x_i = y_{\sigma(i)}$.

Définition. Soit $P \in \mathbf{C}[X]$, $P \neq 0$ et $x \in \mathbf{C}$. Si x est racine de P, on appelle *mutiplicité* de x le nombre de $i \in \{1, 2, ..., n\}$ tel que $x = x_i$. On la note $m(P, x)$. Si x n'est pas racine de P, on pose $m(P, x) = 0$.

La multiplicité m de x dans P est caractérisé par la propriété suivante. Il existe $Q(X)$ tel que $P(X) = (X - x)^m Q(X)$, avec $Q(x) \neq 0$.

On peut aussi écrire la factorisation de P sous la forme suivante. On numérote les racines de sorte que $\{x_1, x_2, ..., x_r\}$ soit l'ensemble des racines de P (donc $x_1, x_2, ..., x_r$ sont distinctes et toute racine de P est égale à l'une des x_i pour $i = 1, 2, ..., r$). Soit m_i la multiplicité de x_i pour $i = 1, 2, ..., r$. On a :

$$P(X) = a_0 \Pi_{i=1}^{r}(X - x_i)^{m_i}.$$

On a $\sum_{i=1}^{r} m_i = \deg(P)$.

Proposition. a) Si x est racine de P, on a : $m(P', x) = m(P, x) - 1$.

Preuve. Soit m la multiplicité de x. On a : $m \geq 1$. On a : $P(X) = (X - x)^m Q(X)$, avec $Q(x) \neq 0$. D'où : $P'(X) = (X - x)^{m-1} Q_1(X)$ avec $Q_1(X) = mQ(X) + (X - x)Q'(X)$. On a : $Q_1(x) = mQ(x) \neq 0$, donc $m(P', x) = m - 1$

Attention. La proposition suppose que x est racine de P. Soit $P(X) = X^{n+1} + 1 : 0$ a multipicité n dans $P'(X)$.

Corollaire. On a $P(x) = P'(x) = P''(x)... = P^{(m-1)}(x) = 0$ et $P^{(m)}(x) \neq 0$.
Le corollaire permet de calculer m.

1.4. Relations entre coefficients et racines (relations de Viète, 17-ième siècle).

Soit $P(X) = a_2 X^2 + a_1 X + a_0$ un polynôme de degré 2 ($a_2 \neq 0$). Soit :

$$P(X) = a_2(X - x_1)(X - x_2)$$

la factorisation de P. En développant :

$$x_1 + x_2 = -a_1/a_2, \; x_1 \times x_2 = a_0/a_2.$$

Généralement :

Théorème. Soit P un polynôme de degré d à coefficients dans $\mathbf{C}$. $P(X) = a_d X^d + ... + a_0$ ($a_d \neq 0$). Soit $P(X) = a_d \Pi_{i=1}^d (X - x_i)$ la factorisation de P. On a, pour $k = 1, ..., d$:

$$a_{d-k}/a_d = (-1)^k \sum_K x_K,$$

la somme portant sur les sous-ensembles de $\{1, ..., d\}$ à k éléments, et x_K désignant le produit $\Pi_{i \in K} x_i$.

Preuve. On a :

$$P(X)/a_d = X^d + a_{d-1}/a_d X^{d-1} + ... + a_0/a_d = \Pi_{i=1}^d (X - x_i).$$

Pour obtenir dans le membre de droite un terme en X^{d-k}, il faut prendre $d - k$ fois X, donc choisir k fois l'opposé d'une racine x_i.

Exemples. $d = 3$, a_2 pour un polynôme de degré 4 (ordonner les termes dans l'ordre lexicographique), a_0.

Remarque. Les quantités : $\sum_K x_K$ ne dépendent pas de l'ordre selon lequel on a numéroté les x_i. C'est de plus un polynôme en les x_i. On dit que l'on a un polynôme symétrique en les racines. On peut prouver que tout polynôme symétrique en les racines s'exprime en fonctions des coefficients.

Exemple. $d = 3$. $x_1^2 + x_2^2 + x_3^2 = (x_1 + x_2 + x_3)^2 - 2(x_1 x_2 + x_1 x_3 + x_2 x_3) = (a_2/a_3)^2 - 2a_1/a_3$.

1.4. Factorisation des polynômes à coefficients réels.

Théorème. Soit P un polynôme à coefficients réels de degré $d \geq 1$. On suppose d impair. Alors, P a une racine réelle.

Preuve. On se ramène au cas où P est unitaire. On a $\lim_{\to +\infty} P(x) = +\infty$, donc il existe a tel que pour $x \geq a$, on a $P(x) \geq 1$. Donc $P(a) > 0$. De même, $\lim_{\to -\infty} P(x) = -\infty$, donc il existe a' tel que pour $x \leq a'$, on a $P(x) \leq -1$. Donc $P(a') < 0$ (et $a' < a$). Il existe x dans l'intervalle $[a', a]$ tel que $P(x) = 0$ (théorème des valeurs intermédiaires).

Proposition. Soit P un polynôme à coefficients réels de degré ≥ 1. Soit $x \in \mathbf{C}$, $x \notin \mathbf{R}$ une racine de P. Alors $\overline{x}$ est racine de P, avec la même multiplicité que x.

On a $x \neq \overline{x}$ puisque $x \notin \mathbf{R}$. On a $P(\overline{x}) = 0$, donc $\overline{x}$ est racine de P.

Pour prouver que $m(P, x) = m(P, \overline{x})$, on raisonne par récurrence sur le degré de P. On a forcément, deg(P) ≥ 2.

Si deg(P) $= 2$, on a $m(P, x) = m(P, \overline{x}) = 1$.

Supposons deg(P) ≥ 3. Comme x et $\overline{x}$ sont deux racine distinctes de P, P est divisible par $B(X) = (X - x)(X - \overline{x})$, $P = BQ$, Q à priori à coefficients dans $\mathbf{C}$.

$B(X) = (X - x)(X - \overline{x})$ est un polynôme à coefficients réels :

$$B(X) = X^2 - 2\mathrm{re(x)X} + \| \mathrm{x} \|^2 .$$

La division de P par B donne $P = BQ$ avec Q à coefficients réels. On applique l'hypothèse de récurrence à Q. Cela prouve la proposition.

On peut donc mettre la factorisation de P sous la forme :

$$P(X) = \Pi_{i=1}^{r_1}(X - x_i) \times \Pi_{j=1}^{r_2} Q_j(X),$$

x_i décrivant les racines réelles de P, $Q_j(X)$ de la forme $(X - x)(X - \overline{x})$, x racine de P, $x \in \mathbf{C}$, $x \notin \mathbf{R}$. On a $\deg(\mathrm{P}) = \mathrm{r}_1 + 2\mathrm{r}_2$.

Quels sont les polynômes Q ?

Proposition. Soit $P = X^2 + a_1 X + a_0$ un polynôme à coefficients réels. Soit $\Delta = (a_1)^2 - 4a_0$ le discriminant. Alors, si $\Delta > 0$, P a deux racines réelles distinctes. Si $\Delta = 0$, P a une racine réelle de multiplicité 2. Si $\Delta < 0$, P a une deux racines complexes non réelles conjuguées : $P(X) = (X - x)(X - \overline{x})$, $x \in \mathbf{C}$, $x \notin \mathbf{R}$. Réciproquement, si $x \in \mathbf{C}$, $x \notin \mathbf{R}$, $P(X) = (X - x)(X - \overline{x})$ est un polynôme à coefficients réels de discriminant < 0.

Preuve que le discriminant de P est < 0. Sinon P aurait une racine réelle. On peut aussi dire que $\Delta = (x - \overline{x})^2 = -4b^2$ si $x = a + ib$.

P polynôme unitaire à coefficients réels de degré 3. Soit $P(X) = (X - x_1)(X - x_2)(X - x_3)$, x_1, x_2 et x_3 réels ($r_1 = 3$, $r_2 = 0$), soit $P(X) = (X - x)Q(X)$, x réel et Q unitaire de degré 2 à discriminant < 0 ($r_1 = 1$, $r_2 = 1$).

Comment distinguer les deux cas ?

Exemple : $P(X) = X^3 + pX + q$. On a $P'(X) = 3X^2 + p$. Posons $\delta = 4p^3 + 27q^2$.

Si $p \geq 0$, la fonction f de $\mathbf{R}$ dans $\mathbf{R}$ $x \mapsto P(x)$ est strictement croissante, et P n'a qu'une racine réelle (triple si $p = q = 0$). Pour $p \geq 0$, si $\delta > 0$, on a $r_1 = 1$ $r_2 = 1$, pas de racine multiple ; si $\delta = 0$, $p = q = 0$ et 0 racine triple : $r_1 = 3$ $r_2 = 0$.

Si $p < 0$, f est croissante dans $]-\infty, -\sqrt{-p/3}]$, et $[\sqrt{-p/3}, \infty[$, décroissante dans $[-\sqrt{-p/3}, \sqrt{-p/3}]$. On a $\delta = f(\sqrt{-p/3})f(-\sqrt{-p/3})$. Si $\delta < 0$, on a 3 racines réelles distinctes ($r_1 = 3$ $r_2 = 0$). Si $\delta > 0$, on a une seule racine réelle simple ($r_1 = 1$ $r_2 = 1$). Si $\delta = 0$, on a une racine réelle de multiplicité 2 ($r_1 = 3$ $r_2 = 0$).

Finalement :

- $\delta > 0$, une seule racine réelle ($r_1 = 1$ $r_2 = 1$), pas de racine multiple ;
- $\delta = 0$, une racine de multiplicité ≥ 2 et $r_1 = 3$ $r_2 = 0$;
- $\delta < 0$, $r_1 = 3$ $r_2 = 0$ pas de racine multiple.

Algorithme rudimentaire pour trouver une valeur approchée d'une racine réelle.

Soient $a < b$ deux réels et $f : [a, b] \to \mathbf{R}$ une application continue. On suppose que $f(a)$ et $f(b)$ sont de signes contraires : $f(a)f(b) \leq 0$. Le théorème des valeurs intermédiaires dit que f s'annule dans $[a, b]$.

En fait, on peut construire deux suites (a_n) et (b_n) qui tendent vers l avec $f(l) = 0$. De plus (a_n) est croissante, (b_n) décroissante et $a_n \leq b_n$. On pose $a_0 = a$ et $b_0 = b$.

On suppose que $f(a) \leq 0$ et $f(b) \geq 0$ (on peut s'y ramener en changeant f en $-f$). On définit a_n et b_n par récurrence de la façon suivante. On suppose que $f(a_n) \leq 0$ et $f(b_n) \geq 0$. Soit $m_n = (a_n + b_n)/2$. Si $f(m_n) \leq 0$, on pose $a_{n+1} = m_n$ et $b_{n+1} = b_n$. Si $f(m_n) > 0$, on pose $a_{n+1} = a_n$ et $b_{n+1} = m_n$. On a bien $f(a_{n+1}) \leq 0$ et $f(b_{n+1}) \geq 0$ La suite (a_n) est croissante, la suite (b_n) décroissante, $a_n \leq b_n$ et $b_n - a_n = (b-a)/2^n$ a pour limite vers 0 lorsque n tend vers ∞. Les deux suites (a_n) et (b_n) ont donc une même limite l.

On a $f(l) = \lim f(a_n) \leq 0$ (on utilise ici que f est continue) et $f(l) = \lim f(b_n) \geq 0$, donc $f(l) = 0$. C'est une preuve du théorème des valeurs intermédiaires.

Pour que cela donne un algorithme pour trouver une valeur approchée d'une racine d'un polynôme P de degré impair à coefficients réels, on détermine un $A > 0$ tel que les racines (réelles) de P sont de module $< A$ (et donc $P(A) > 0$ et $P(-A) < 0$).

On a :

Proposition. Soit $P(X) = X^d + a_{d-1}X^{d-1} + ... + a_0$ un polynôme unitaire de degré $d \geq 1$ à coefficients dans $\mathbf{C}$. Soit $M = \max_{0 \leq i \leq d-1}(a_i)$. Alors, si $x \in \mathbf{C}$ est racine de P, on a : $\| x \| < 1 + M$.

Preuve. Si $M = 0$, c'est clair. Supposons $M \neq 0$.

Il s'agit de prouver que si z vérifie $\| z \| \geq 1 + M$, on a $P(z) \neq 0$. On a :

$$P(z) = z^d(1 + a_{d-1}z^{-1} + ... + a_0 z^{-d}).$$

Il suffit de prouver que :

$$(1) \ : \| a_{d-1}z^{-1} + ... + a_0 z^{-d} \| < 1.$$

On a :

$$\| a_{d-1}z^{-1} + ... + a_0 z^{-d} \| \leq M \ \ \| z \|^{-1} \ \ (1 + \| z \|^{-1} + ... + \| z \|^{-d+1}).$$

Comme $\| z \|^{-1} \leq 1/(1+M) < 1$, on en déduit :

$$\| a_{d-1}z^{-1} + ... + a_0 z^{-d} \| < M \ \ \| z \|^{-1} \ \ \Big(\frac{1}{1 - \| z \|^{-1}}\Big),$$

et donc :

$$\| a_{d-1}z^{-1} + ... + a_0 z^{-d} \| < 1.$$

Supposons les a_i réels. Prenons z réel. On déduit de (1) que, pour $| z | \geq 1 + M$, $P(z)$ est du signe de z^d. Lorsque d est impair, on a donc $P(z) > 0$ pour $z \geq 1 + M$ et $P(z) < 0$ lorsue $z \leq -(1 + M)$. On peut prendre $A = 1 + M$.

2. Suites définies par itération d'une fonction. Méthode de Newton pour la recherche numérique des zéros d'une fonction.

2.1. Itération : exemples.

Soit I un intervalle de $\mathbf{R}$. Les extrémités a et b de I, $a < b$, peuvent être des réels, ou bien $a = -\infty$, $b = +\infty$. I est dit *borné* si a et b sont des réels. Il est dit *fermé* si ses extrémités finies appartiennent à I, *ouvert* si ses extrémités finies n'appartiennent pas à I. $]-\infty, +\infty[$ est à la fois ouvert et fermé ; $[1, 2[$ n'est ni ouvert ni fermé.

Soit φ une fonction de I dans I. Soit $x \in I$. On définit la suite $(x_n)_{n\in\mathbf{N}}$ par $x_0 = x$, $x_1 = \varphi(x_0)$ et $x_{n+1} = \varphi(x_n)$. On dit que la suite $(x_n)_{n\in\mathbf{N}}$ est obtenue par itération de la fonction φ (la suite $(x_n)_{n\in\mathbf{N}}$ dépend bien sûr de x_0). Attention $\varphi(I) \subset I$ est indispensable pour la définir ! On a $x_n \in I$ pour tout n.

La suite (x_n) peut avoir une limite ou pas lorsque n tend vers $+\infty$.

Exemple. $I = \mathbf{R}$, $\varphi(x) = \lambda x$.

Si $|\lambda| < 1$, on a $\lim x_n = 0$ pour tout x_0.

Si $|\lambda| > 1$, $|x_n|$ tend vers $+\infty$ pour $x_0 \neq 0$. 0 est point fixe.

Si $\lambda = 1$ tous les points sont fixes. Cas $\lambda = -1$: 0 est point fixe, $x \neq 0$ est périodique de période 2.

Définition. x est *fixe* si $\varphi(x) = x$.

Si x_0 est fixe, (x_n) est constante.

Proposition. On suppose que I est fermé et que φ est continue. On suppose que (x_n) a une limite l finie. Alors $l \in I$ et $\varphi(l) = l$, l est point fixe.

Preuve. $x_n \in I$ donc $l \in I$ (I contient ses extrémités finies). x_{n+1} tend vers l. $\varphi(x_n)$ tend vers $\varphi(l)$ car φ est continue. Donc $\varphi(l) = l$.

Remarque. Résoudre $f(x) = 0$ se ramène à $\varphi(x) = x$ si l'on pose $\varphi(x) = x + f(x)$. L'itération permet d'approcher numériquement les points fixes, du moins s'ils sont "attractifs".

Exemple : $I = \mathbf{R}$, $\varphi(x) = \mathrm{ch}(x) - 1$ ($\mathrm{ch}(x) = 1/2(e^x + e^{-x})$). φ est paire, croissante sur $[0, +\infty[$, a pour limite $+\infty$ lorsque x tend vers $+\infty$. Posons $f(x) = \varphi(x) - x$. Sa dérivée $\mathrm{sh}(x) - 1 = 1/2(e^x - e^{-x}) - 1$ est négative sur $[0, l_1]$ puis positive sur $[l_1, +\infty[$ pour un $l_1 > 0$. Comme $f(x)$ a pour limite $+\infty$ lorsque x tend vers $+\infty$, on voit que φ a deux points fixes : 0 et un $l > l_1$. Comme φ est croissante, on a, pour $x \in [0, l]$, $0 \leq \varphi(x) \leq \varphi(l) = l$. On a donc $\varphi([0, l]) \subset [0, l]$. Si $x \in [0, l]$, $x_n \in [0, l]$ pour tout n. De plus, comme pour $x \in [0, l]$, $\varphi(x) \leq x$, la suite x_n est décroissante. On en déduit, comme elle est minorée, qu'elle a une limite. Si $x \in [0, l[$, la limite ne peut-être que 0 puisque l est l'unique point fixe $< l$. De même, si $x > l$, (x_n) est croissante et a pour limite $+\infty$.

Proposition. a) Si φ est croissante, (x_n) est monotone.

b) Si $\varphi(x) \geq x$ pour tout $x \in I$, (x_n) est croissante.

c) Si $\varphi(x) \leq x$ pour tout $x \in I$, (x_n) est décroissante.

Preuve. a) Si $x_1 \geq x_0$, on a $x_2 = \varphi(x_1) \geq \varphi(x_0) = x_1$, ect...

b) $x_1 = \varphi(x_0) \leq x_0$, ect...

2.2. Théorème du point fixe.

Définition. Soit I un intervalle et φ une application de I dans $\mathbf{R}$. On dit que φ est

contractante s'il existe λ, $0 \leq \lambda < 1$ tel que pour tout x et $x' \in I$, on ait :

$$| \varphi(x) - \varphi(x') | \leq \lambda | x - x' | .$$

Théorème. Soit I un intervalle fermé et φ une application contractante de I dans I. Alors φ a un unique point fixe $l \in I$. Pour tout $x_0 \in I$, la suite $(x_n)_{n \in \mathbf{N}}$ définie par récurrence par $x_{n+1} = \varphi(x_n)$ converge vers l. Plus précisément, on a pour tout n :

$$| x_n - l | \leq \lambda^n | x_0 - l | .$$

Proposition. Soit I un intervalle et φ une application de I dans $\mathbf{R}$. Soit $\lambda \in \mathbf{R}_{\geq 0}$. On suppose que φ est dérivable et que pour tout $x \in I$ on a $| \varphi'(x) | \leq \lambda$. Alors, pour tout $x, x' \in I$, on a :

$$| \varphi(x') - \varphi(x) | \leq \lambda | x - x' | .$$

En particulier, si $\lambda < 1$, φ est contractante.

La proposition résulte de ce que si $\psi : I \to \mathbf{R}$ est dérivable et à dérivée ≥ 0, ψ est croissante. Ceci a sans doute été admis. Par exemple, pour prouver que pour $t \geq 0$, $x + t \in I$, on a :

$$\varphi(x + t) - \varphi(x) \geq -\lambda t,$$

on considère $\psi(t) = \varphi(x + t) - \varphi(x) + \lambda t$.

Dans le théorème du point fixe, il a au plus un point fixe. Pour φ contractante, on a :

$$| \varphi(x') - \varphi(x) | < | x - x' | .$$

Si l est point fixe :

$$| \varphi(x) - l | < | x - l |,$$

et donc $x \neq l$ n'est pas point fixe.

Si I est borné, l'existence d'un point fixe résulte de :

Proposition. Soient $a < b$ deux réels et φ une application continue de $[a, b]$ dans $[a, b]$. Alors φ a un point fixe.

Preuve. Posons $\psi(x) = x - \varphi(x)$. On a $\psi(a) \leq 0$ et $\psi(b) \geq 0$. La proposition résulte du théorème des valeurs intermédiaires.

Remarque. L'exemple $I = [0, 1]$ $\varphi(x) = x^2$ montre que l'hypothèse I fermé est nécessaire dans la proposition. L'exemple $I = \mathbf{R}_{\geq 0}$, $\varphi(x) = x + e^{-x}$ montre que I borné est nécessaire, et que dans le théorème du point fixe, on ne peut pas remplacer l'hypothèse φ contractante par $| \varphi(x') - \varphi(x) | < | x - x' |$ pour tout $x, x' \in I$.

Existence d'un point fixe (sous les hypothèses du théorème) dans le cas $I = [a, +\infty[$.

On a $\varphi(a) - a \geq 0$. Il suffit donc de prouver que $\varphi(x) - x$ tend vers $-\infty$ lorsque x tend vers $+\infty$ (théorème des valeurs intermédiaires). Or :

$$\varphi(x) \leq \varphi(a) + \lambda(x - a),$$

donc :

$$\varphi(x) - x \leq \varphi(a) - \lambda a - (1 - \lambda)x.$$

QED

Convergence de la suite (x_n) vers le point fixe.

On a :

$$| \varphi(x_n) - \varphi(l) | \leq \lambda | x_n - l |,$$

donc :

$$| x_{n+1} - l | \leq \lambda | x_n - l |,$$

et :

$$| x_n - l | \leq \lambda^n | x_0 - l | .$$

Comme $| \lambda | < 1$, λ^n tend vers 0 lorsque n tend vers $+\infty$ et (x_n) tend vers l.

2.3. Méthode de Newton.

Soient $a < b$ deux réels. Soit $f : [a, b] \to \mathbf{R}$ une application deux fois continûment dérivable. On suppose que

- f s'annule dans $[a, b]$,
- f' ne s'annule pas dans $[a, b]$,
- f'' ne s'annule pas dans $[a, b]$.

En particulier, f' et f'' gardent un signe constant dans $[a, b]$. f est strictement croissante ou décroissante. $f(x) = 0$ a une unique solution l dans $[a, b]$. On veut calculer des valeurs approchées de l.

On part de x_0. On définit x_n par itération de φ. $\varphi(x)$ est l'abscisse de l'intersection de la tangente en le point $(x, f(x))$ au graphe de f avec l'axe des x. Cette intersection existe car $f'(x) \neq 0$. L'équation de la tangente est

$$Y - f(x) = f'(x)(X - x).$$

On a donc :

$$\varphi(x) = x - \frac{f(x)}{f'(x)}.$$

φ a pour unique point fixe l dans $[a, b]$.

Attention : sous les hypothèses ci-dessus, $[a, b]$ n'est pas nécessairement stable par φ.

Supposons par exemple $f'(x)$ et $f''(x)$ positifs pour $x \in [a, b]$. Alors

Proposition. $I = [l, b]$ est stable par φ.

En effet :

$$\varphi'(x) = \frac{f(x)f''(x)}{f'(x)^2}.$$

Donc $\varphi'(x) \geq 0$ pour $x \in I$. On a $\varphi(l) = l$, donc $\varphi(x) \geq l$ pour $x \in I$. De plus $x - \varphi(x) = \frac{f(x)}{f'(x)}$. Donc $x \geq \varphi(x)$ pour $x \in I$. Par suite, $\varphi(x) \leq x \leq b$ pour $x \in I$.

On choisit $x_0 \in I$ et on définit x_n par $x_{n+1} = \varphi(x_n)$. C'est possible car I est stable par φ.

Proposition. (x_n) est décroissante et a pour limite l.

En effet, on a vu que pour $x \in I$, on a $\varphi(x) \leq x$. Donc (x_n) est décroissante. Elle est minorée par l, donc elle a une limite. Cette limite est un point fixe, c'est donc l.

On a $\varphi'(l) = 0$. Ceci entraîne que la suite (x_n) tend très vite vers l (ou au moins finit par tendre très vite vers l).

Proposition. On suppose f'' continûment dérivable. Il existe n_0 et C tels que

$$| x_{n+n_0} - l | \leq \frac{C}{10^{2^n}}.$$

A chaque itération, on double le nombre de décimales.

Preuve.

Lemme. Soit ψ deux fois continûment dérivable $[c, d] \to \mathbf{R}$. On suppose donné $z \in [c, d]$ tel que $\psi'(z) = 0$. Soit $M = \sup_{x \in [c,d]}(| \psi''(x) |)$.

Alors, pour $x \in [c, d]$:

$$| \psi(x) - \psi(z) | \leq M \frac{(x - z)^2}{2}.$$

Prouvons la proposition. On applique le lemme avec φ, $c = l$, $d = b$, $z = l$:

$$| x_{n+1} - l | \leq M/2 \, | x_n - l |^2 .$$

On prend $C = 2/M$ et n_0 tel que $| x_{n_0} - l | \leq C/10$.

Appendice.

Soient n et k deux entiers, $n \geq 1$ et $0 \leq k \leq n$.

Définition. $\binom{n}{k} = C_n^k$ est le nombre de sous-ensembles à k éléments choisis dans un ensemble à n éléments.

Exemples. $k = 0$ ou n, $\binom{n}{k} = 1$; $\binom{n}{1} = n$.

Remarque. Choisir un sous-ensemble, c'est choisir son complémentaire, donc $\binom{n}{k} = \binom{n}{n-k}$. On voit que $\binom{n}{n-1} = n$.

Proposition.

$$\binom{n}{k} = \frac{n \times (n-1) \times ... \times (n-k+1)}{k\ !} = \frac{n!}{k! \times (n-k)!}.$$

Exemple. $\binom{n}{2} = n(n-1)/2$.

Soit X_n un ensemble à n éléments. Il y a $n \times (n-1) \times ... \times (n-k+1)$ façons de choisir une suite $x_1, x_2, ..., x_k$ d'éléments de X_n. L'ensemble $Y = \{x_1, x_2, ..., x_k\}$ étant donné, il y a de même $k!$ façons d'ordonner les éléments de Y.

Proposition (formule du binôme).

$$(U+V)^n = \sum_{k=0}^{n} \binom{n}{k} U^k V^{n-k}.$$

Remarque. C'est une formule dans les polynômes en les deux variables U et V. On peut substituer à U et V deux polynômes à coefficients dans $\mathbf{C}$, ou bien deux nombres complexes. Si U et V sont des matrices qui ne commutent pas, on n'a pas la formule pour $n = 2$.

Preuve. On développe $(U+V)(U+V)...(U+V)$, les facteurs $(U+V)$ étant numérotés de 1 à n. A un terme en $U^k V^{n-k}$, on associe le sous-ensemble de $\{1, ..., n\}$ formé des indices des facteurs où l'on a choisi U.

Proposition. Pour $k \leq n-1$, on a : $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$.

Preuve. Soit X_{n+1} un ensemble à $n+1$ éléments. Soit $x_0 \in X_{n+1}$. Il y a $\binom{n}{k}$ sous-ensembles de X_{n+1} à $k+1$ éléments qui contiennent x_0 et $\binom{n}{k+1}$ sous-ensembles de X_{n+1} à $k+1$ éléments qui ne contiennent pas x_0.

Exercice. Déduire la proposition de la formule du binôme. La déduire aussi du calcul de $\binom{n}{k}$.

Triangle de Pascal.