

Fernand Didier
Jacques Gispert
Dominique Proudhon
Robert Rolland
Patrick Soubeyrand

**MATHÉMATIQUES EN
LIAISON AVEC DES
PROBLÈMES CONCRETS
TOME II**

Fernand Didier

E-mail : didier@irem.univ-mrs.fr

Jacques Gispert

E-mail : Jacques.Gispert@lidil.univ-mrs.fr

Dominique Proudhon

E-mail : dproudhon@wanadoo.fr

Robert Rolland

E-mail : rolland@iml.univ-mrs.fr

Url : <http://iml.univ-mrs.fr/~rolland>

Patrick Soubeyrand

E-mail : soubeyrand.patrick@free.fr,

IREM d'Aix-Marseille, Luminy Case 901, F13288 Marseille CEDEX 9

.

**MATHÉMATIQUES EN LIAISON AVEC
DES PROBLÈMES CONCRETS
TOME II**

**Fernand Didier, Jacques Gispert,
Dominique Proudhon, Robert Rolland,
Patrick Soubeyrand**

AVERTISSEMENT

Cette brochure, réalisée par l'équipe **liaison Lycée-Université** de l'IREM d'Aix-Marseille, constitue le tome 2 d'un travail que nous menons depuis quelques années. Comme dans le tome 1, nous donnons des exemples d'interventions des outils mathématiques dans des problèmes concrets issus des sciences ou des techniques.

Les problèmes exposés ont des énoncés simples. Par exemple : comment exprimer l'évolution de la hauteur d'eau lors d'une marée ? Comment a-t-on calculé il y a fort longtemps le rayon de la terre ? Quel temps moyen met un photon pour sortir du soleil ? Quant aux solutions mathématiques et aux développements qui s'en suivent, ce sont parfois des questions difficiles. On peut alors, pour s'adapter au niveau, n'aborder qu'une partie plus ou moins large de ces questions, ou encore aborder certaines d'entre elles sous leur aspect technique mathématique et d'autres sous un aspect de vulgarisation scientifique.

Redisons ici que si on veut bien considérer que le rôle de l'enseignement des mathématiques est de rendre compte d'une activité scientifique centrale au cours de l'histoire et, au-delà des techniques de la discipline, de dispenser une culture, alors les textes qui suivent pourront, nous l'espérons, se révéler utiles.

TABLE DES MATIÈRES

Avertissement	v
1. Les pieds dans l'eau	1
1.1. Présentation du problème.....	1
1.2. Montée sinusoïdale et règle des douzièmes.....	2
1.3. Interpolation par un polynôme.....	4
1.4. Qualité des approximations.....	7
1.5. Approximation de la fonction réciproque.....	12
2. Ça part en vrille	15
2.1. Présentation du problème.....	15
2.2. Utilisation du calcul différentiel.....	16
2.3. Méthode géométrique.....	19
3. La tête au soleil	23
3.1. Présentation.....	23
3.2. Marche aléatoire discrète.....	25
3.3. Application.....	27
3.4. Du côté de chez Brown.....	27
3.5. ... et à la Bourse!.....	28
3.6. ... ou chez les fourmis.....	29
3.7. Enfin, parmi les comètes.....	29
4. Ça ne tourne pas rond	31
5. ἀστρονόμογεομέτρης	39
5.1. Mesure du rayon de la Terre.....	39
5.2. Distance de la Lune (Aristarque de Samos).....	40

5.3. Calcul de la distance de Vénus au Soleil.....	41
6. L'art d'arrondir les angles.....	47
6.1. Position du problème.....	47
6.2. Première approche.....	48
6.3. Raccord circulaire.....	53
6.4. Troisième type de raccord : spline cubique.....	55
6.5. Comparaison des aires perdues (raccord parabolique , circulaire et spline cubique).....	56
6.6. Comparaison des énergies de flexion.....	57
6.7. Les notations.....	58
6.8. Raccord tangent par arc de cercle aux points I et J	59
6.9. Raccord tangent par arc de parabole aux points I et J	61
6.10. Raccord par une spline cubique.....	62
6.11. Conclusion.....	63
7. Errare humanum est.....	65
7.1. Présentation du problème.....	65
7.2. Les erreurs possibles.....	66
7.3. Comparons deux méthodes proches.....	67
7.4. Est-ce possible?.....	68
7.5. Commençons par $n = 2$	68
7.6. Passage du cas $n = 2$ au cas $n \geq 2$	76
7.7. Une construction particulière.....	76
7.8. Conclusion.....	77
Bibliographie.....	79

CHAPITRE 1

LES PIEDS DANS L'EAU

1.1. Présentation du problème

Nous nous intéressons à la variation de hauteur d'eau due à la marée. C'est un problème important en navigation, puisqu'il s'agit de savoir quelle sera la profondeur en une position donnée et à un instant donné et donc de répondre à la question vitale : le navire peut-il passer ou non ? Avant de formaliser ce problème, donnons la terminologie en usage. **Pleine mer** (la mer est montée et atteint la pleine mer avant de redescendre), **basse mer** (la mer est descendue et atteint la basse mer avant de remonter), **flot** (temps pendant lequel la mer monte), **flux** (courant du flot), **jusant** (temps pendant lequel la mer descend), **reflux** (courant du jusant), **marée de vive eau** (grande marée), **marée de morte eau** (petite marée). Le **coefficient de marée** (20-120) mesure si on est vers une marée de vive eau ou non. Définissons aussi le **marnage** (différence des hauteurs de la pleine mer avec la basse mer), la **profondeur** (distance de la surface de la mer au fond, à l'instant et au lieu considérés), la **hauteur** (distance, à l'instant considéré et dans la zone considérée, de la surface au zéro des cartes, qui est le point le plus bas atteint par l'eau lors des plus faibles marées), la **sonde** (distance du fond au zéro des cartes, la sonde peut être négative pour un rocher découvrant). Nous avons évidemment la relation suivante :

$$\mathbf{Profondeur = Hauteur + Sonde.}$$

Lorsqu'un navire doit passer à un instant donné en un point donné, il faut évidemment que la profondeur soit supérieure au tirant d'eau

du navire, auquel on rajoute une marge de sécurité appelée le **pied du pilote** :

$$\text{Tirant d'eau} + \text{Pied du pilote} < \text{Profondeur}.$$

La sonde est indiquée sur les cartes. Il s'agit donc pour déterminer la profondeur de calculer la hauteur.

Nous allons dans la suite considérer que nous partons d'une situation de basse mer et que la marée monte. Le cas d'une marée descendante se traiterait de la même manière.

Les annuaires des marées donnent pour un lieu donné et une date donnée les heures de basse mer et de pleine mer, ainsi que les hauteurs d'eau correspondantes. Nous noterons T_0 l'heure de basse mer que nous considérons, T_1 l'heure de pleine mer suivante, H_0 et H_1 les hauteurs d'eau respectivement en T_0 et T_1 . Le temps $T_1 - T_0$ est proche de $6h$, mais en diffère suivant les dates de façon qu'on ne peut négliger. Nous appellerons **heure marée** la quantité :

$$\frac{T_1 - T_0}{6}.$$

Le marnage $H_1 - H_0$, pour des raisons de calcul que nous allons voir, est divisé en douze. La quantité :

$$\frac{H_1 - H_0}{12}$$

est appelée le **douzième**.

1.2. Montée sinusoïdale et règle des douzièmes

On peut supposer que l'accroissement de la hauteur d'eau pendant une marée est sinusoïdal. Pour avoir une formule qui soit toujours valable, quel que soit le marnage, quelle que soit la durée de la marée, nous exprimons la hauteur d'eau en douzième et le temps en heure marée. Dans ce cas la variation en douzième y de la hauteur s'écrit en fonction de l'heure marée x sous la forme :

$$(1) \quad y = f(x) = 6 \left(\sin \left(\frac{\pi(x-3)}{6} \right) + 1 \right).$$

Nous représentons sur la figure 1 cette variation.

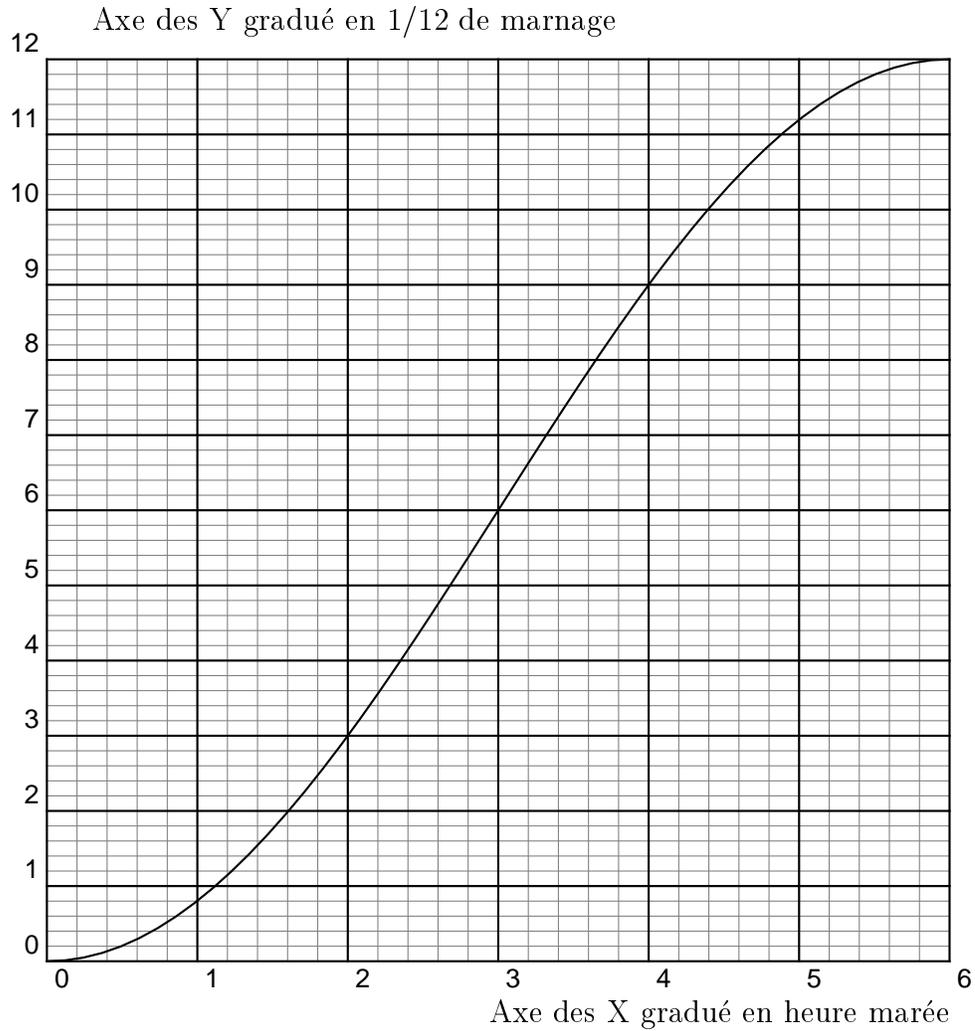


FIGURE 1. Montée sinusoidale

Une méthode très répandue, tout au moins chez les navigateurs amateurs, et qui évite l'usage des fonctions trigonométriques, consiste à approcher la fonction sinus par une fonction affine par morceau bien choisie et simple à retenir : l'accroissement de la hauteur de la mer est calculée par la règle des douzièmes.

La règle des douzièmes dit que la première heure marée la variation de la hauteur est de $1/12^e$ du marnage, la deuxième heure marée de $2/12^e$ du marnage, la troisième heure marée de $3/12^e$ du marnage, la quatrième heure marée de $3/12^e$ du marnage, la cinquième heure marée de $2/12^e$ du marnage et la sixième heure marée de $1/12^e$ du marnage. On représente le graphe de la fonction g affine par morceau ainsi obtenue sur la figure 2.

Nous comparons ensuite (voir figure 3) les deux graphiques obtenus (règle des douzièmes et fonction sinus), ce qui nous donne une idée de la qualité de l'approximation. Nous étudierons plus en détail dans la suite une évaluation de la différence entre les deux fonctions introduites.

Remarque : Si nous voulons la hauteur H en mètre en fonction du temps T , exprimé en heure, écoulé depuis le début de la marée (donc $T \in [0, T_1 - T_0]$), il suffit de faire un changement de variable qui nous donne la formule suivante :

$$(2) \quad H = \frac{H_1 + H_0}{2} + \frac{H_1 - H_0}{2} \sin\left(\frac{\pi}{2} \frac{2T + T_0 - T_1}{T_1 - T_0}\right)$$

1.3. Interpolation par un polynôme

On considère la fonction f définie sur l'intervalle $[0, 6]$ par l'équation (1).

Nous allons chercher un polynôme qui approche cette fonction sinus sur cet intervalle. Le point d'inflexion nous donne à penser qu'il faut tenter une cubique pour être "dans la forme".

Nous allons donc chercher le polynôme d'interpolation P de degré ≤ 3 tel que :

- $P(0)=f(0)=0$;
- $P(3)=f(3)=6$;
- $P(6)=f(6)=12$;
- $P'(0)=f'(0)=0$.

Les conditions $P(0) = 0$ et $P'(0) = 0$ imposent que :

$$P(x) = x^2(ax + b).$$

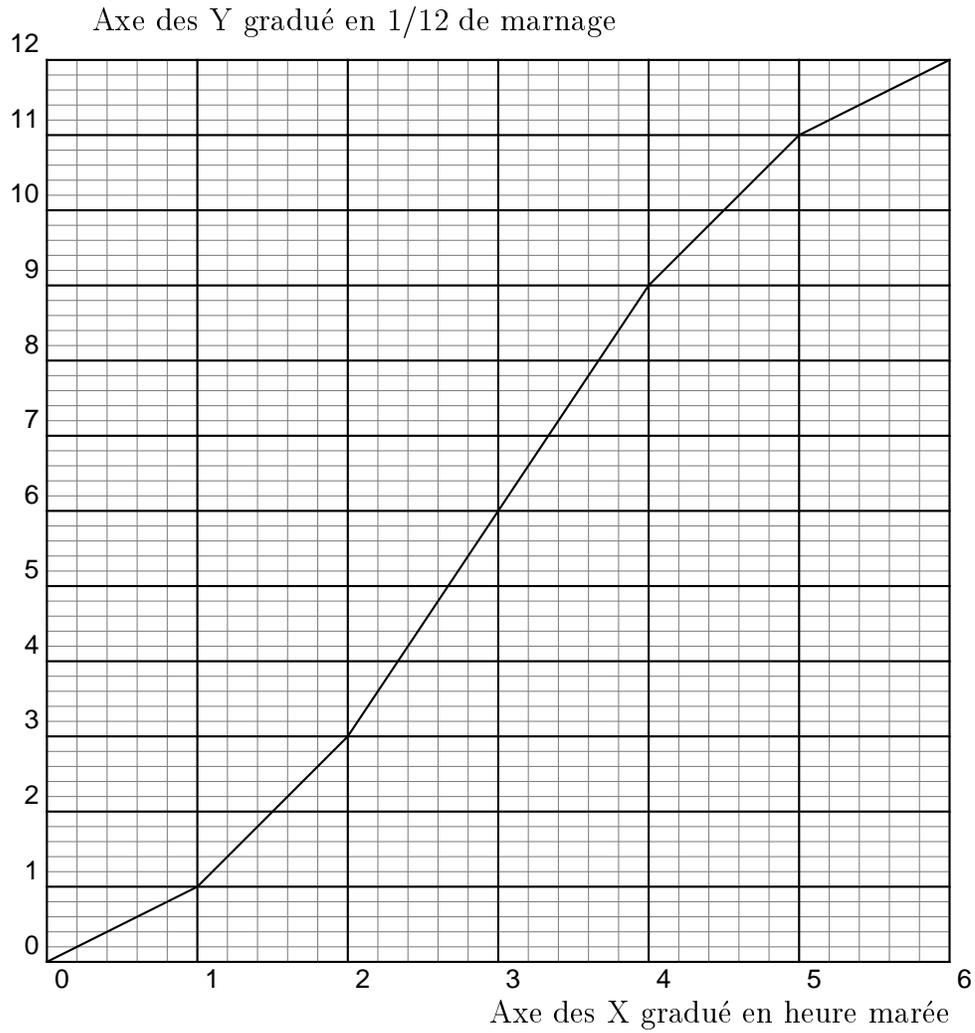


FIGURE 2. La règle des douzièmes

Les deux autres conditions donnent respectivement :

$$9a + 3b = 2,$$

$$18a + 3b = 1,$$

d'où :

$$\begin{cases} a = -\frac{1}{9} \\ b = 1 \end{cases}$$

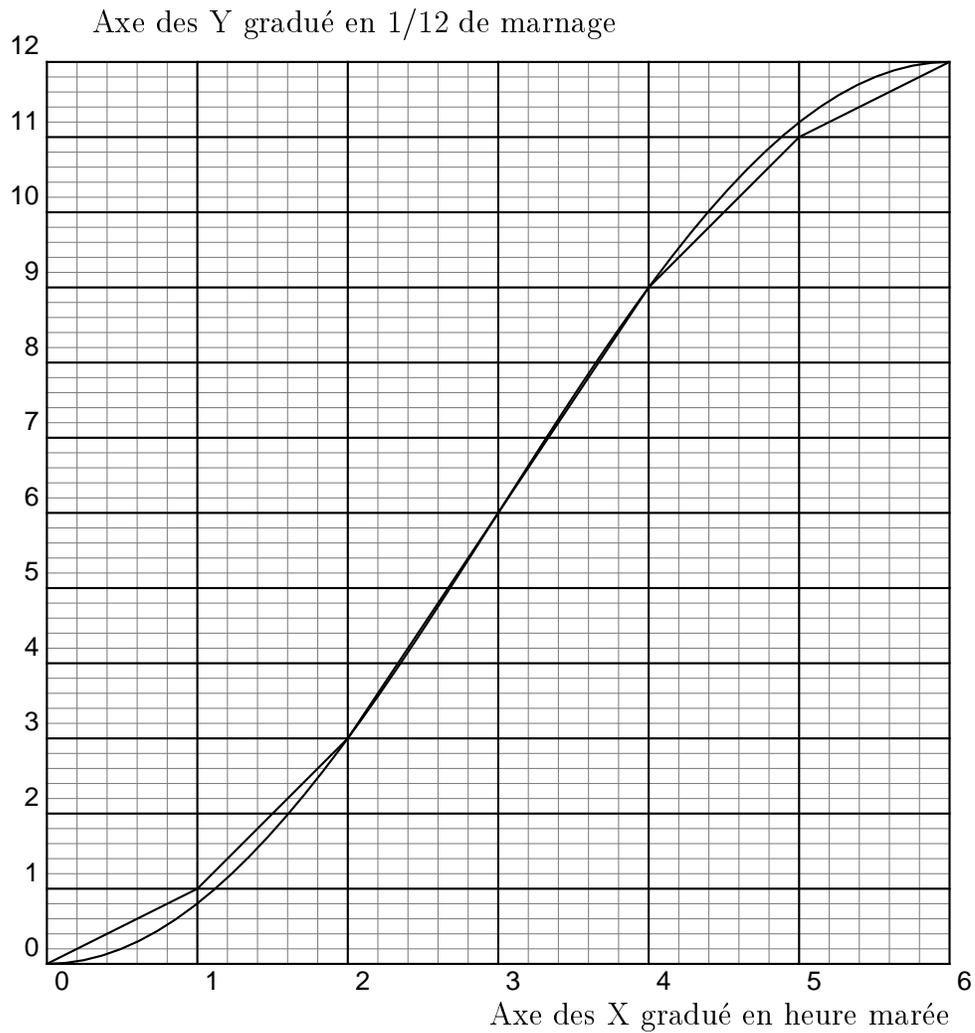


FIGURE 3. Comparaison

Le polynôme cherché est donc :

$$P(x) = -\frac{1}{9}x^3 + x^2.$$

Nous avons représenté le graphe de P sur la figure 4.

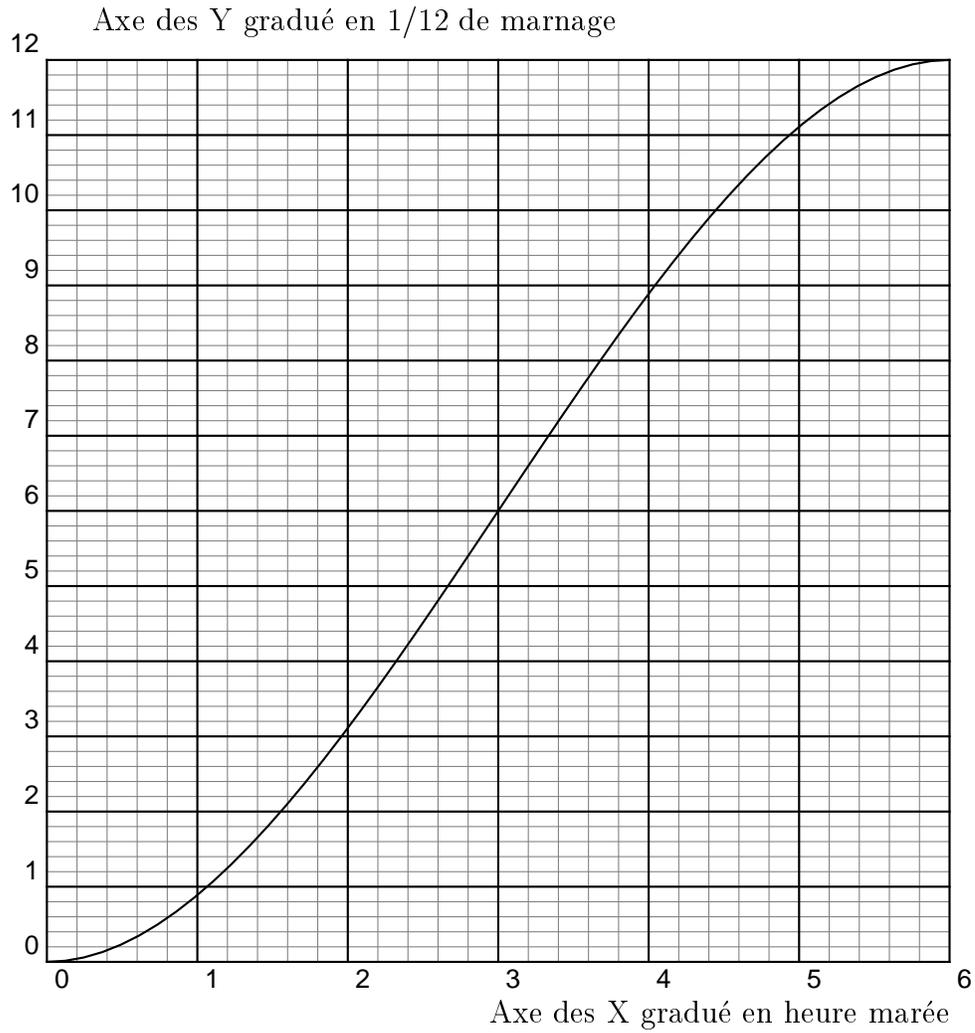


FIGURE 4. Approximation cubique

1.4. Qualité des approximations

1.4.1. Les problèmes à résoudre. — Afin d'évaluer la précision des deux approximations $g(x)$ et $P(x)$ de la fonction $f(x)$, nous allons majorer les quantités :

$$\sup_{x \in [0,6]} |f(x) - g(x)|$$

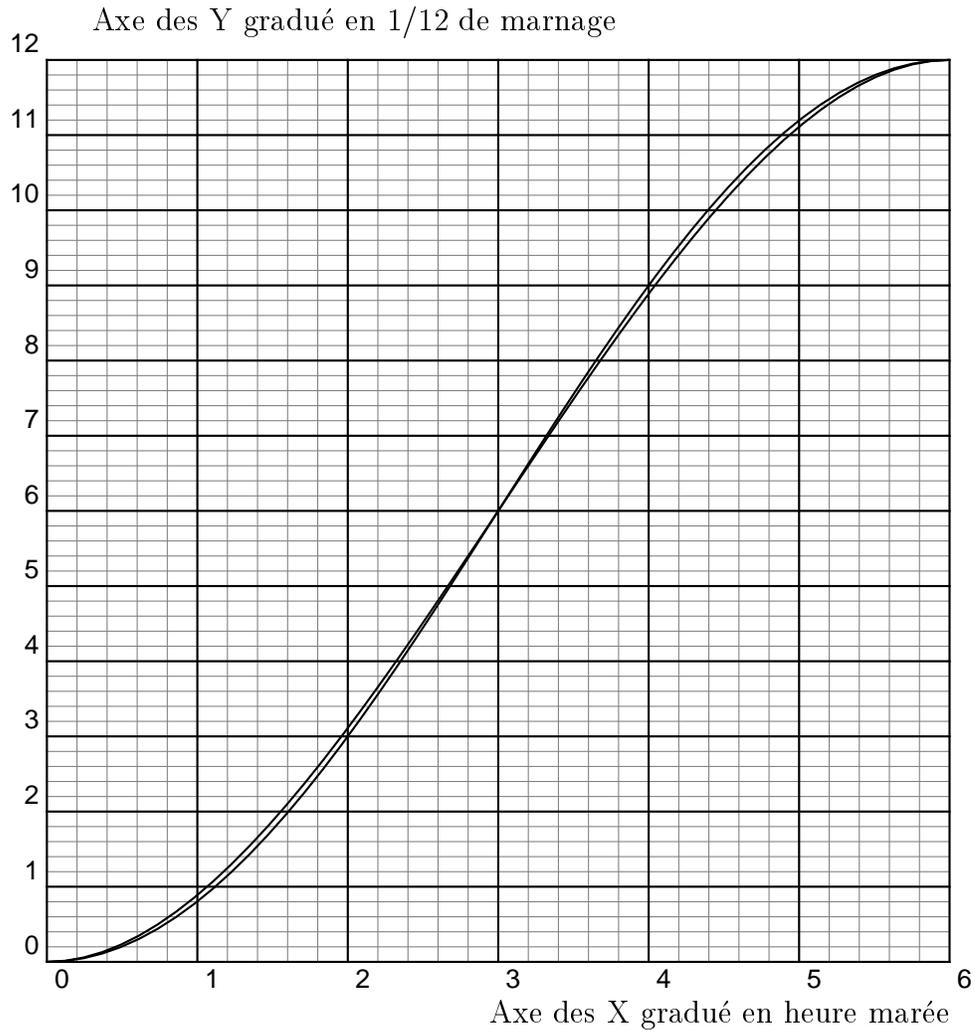


FIGURE 5. Comparaison entre le sinus et la cubique

et

$$\sup_{x \in [0,6]} |f(x) - P(x)|,$$

c'est-à-dire les normes uniformes $\|f - g\|_\infty$ et $\|f - P\|_\infty$ sur l'intervalle $[0, 6]$. (Les meilleures majorations seront primées!)

1.4.2. Un outil fondamental : le théorème de division des fonctions différentiables. —

Théorème 1.4.1. — Soit f une fonction réelle définie sur \mathbb{R} de classe C^{p+1} , où p est un entier naturel. On suppose que f s'annule en un point a de \mathbb{R} . Alors il existe une unique fonction continue $g(x)$ telle que :

$$f(x) = (x - a)g(x).$$

Cette fonction g est de classe C^p et pour tout $0 \leq q \leq p$:

$$(3) \quad |g^{(q)}(x)| \leq \frac{1}{q+1} \sup_{t \in [a, x]} |f^{(q+1)}(t)|.$$

Démonstration. — La fonction g est nécessairement définie par :

$$(4) \quad g(x) = \begin{cases} \frac{f(x)}{x-a} & \text{si } x \neq a, \\ f'(a) & \text{si } x = a. \end{cases}$$

On constate en distinguant le cas où $x = a$ de celui où $x \neq a$ que :

$$g(x) = \int_0^1 f'(a + (x - a)u) du.$$

Sous cette dernière forme, d'après le théorème de dérivation sous le signe intégrale, on voit que la fonction $g(x)$ est de classe C^p et que pour tout $0 \leq q \leq p$

$$g^{(q)}(x) = \int_0^1 u^q f^{(q+1)}(a + (x - a)u) du,$$

ce qui nous donne la formule (3). □

1.4.3. Majoration de l'erreur dans une interpolation. — Soit f une fonction de classe C^{n+1} , P le polynôme d'interpolation de Lagrange qui prend les mêmes valeurs que f aux points x_0, x_1, \dots, x_n et I un intervalle compact contenant x, x_0, x_1, \dots, x_n . Appliquons alors le théorème 1.4.1 à $f(x) - P(x)$. On obtient

$$f(x) - P(x) = (x - x_0)g_0(x)$$

avec

$$|g_0^{(n)}(x)| \leq \frac{1}{n+1} \sup_{t \in I} |f^{(n+1)}(t)|$$

(ne pas oublier que $P^{(n+1)}(x) = 0$), puis

$$g_0(x) = (x - x_1)g_1(x)$$

avec

$$|g_1^{(n-1)}(x)| \leq \frac{1}{n} \sup_{t \in I} |g_0^{(n)}(t)|,$$

et ainsi de suite. Si bien que :

$$(5) \quad |f(x) - P(x)| \leq \frac{1}{(n+1)!} |(x - x_0)(x - x_1) \dots (x - x_n)| \sup_{t \in I} |f^{(n+1)}(t)|.$$

Remarque 1.4.2. — Cette démonstration permet d'établir de la même façon une majoration dans le cas d'une interpolation de Lagrange-Sylvester.

1.4.4. Les majorations. —

1.4.4.1. *Cas de l'approximation par $P(x)$.* — Si on ne regarde pas de plus près, on pourrait croire que nous avons fait une interpolation de Lagrange-Sylvester par un polynôme de degré 3 sous les conditions d'interpolation :

$$P(0) = f(0) \quad P(3) = f(3) \quad P(6) = f(6) \quad P'(0) = f'(0).$$

Mais en fait on constate qu'avec ce même polynôme de degré 3 on a aussi $P'(6) = f'(6)$. Donc on a effectué en fait une interpolation de degré 4, dont le coefficient du terme de plus haut degré est nul. On peut donc appliquer la majoration (5) et la remarque 1.4.2 à cet ordre et on obtient :

$$|f(x) - P(x)| \leq \frac{1}{5!} |x^2(x-3)(x-6)^2| \sup_{t \in [0,6]} |f^{(5)}(t)|.$$

Ceci nous donne :

$$|f(x) - P(x)| \leq \frac{1}{120} \times 6 \times \left(\frac{\pi}{6}\right)^5 |x^2(x-3)(x-6)^2|,$$

$$|f(x) - P(x)| \leq \frac{1}{120} \times 6 \times \frac{1}{25} |x^2(x-3)(x-6)^2|.$$

Pour étudier la borne supérieure de la fonction $|x^2(x-3)(x-6)^2|$ qui est symétrique par rapport à $x = 3$, il suffit de chercher son maximum sur $[0, 3]$. Sur cet intervalle cette fonction est $x^2(3-x)(x-6)^2$ et sa dérivée

s'annule pour 0 et $\frac{15-3\sqrt{5}}{5}$. Le maximum est atteint en $\frac{15-3\sqrt{5}}{5}$ et est majoré par 70. En conséquence :

$$|f(x) - P(x)| \leq \frac{1}{120} \times 6 \times \frac{1}{25} \times 70,$$

$$|f(x) - P(x)| \leq 0.14$$

Remarque 1.4.3. — Un calcul à la machine montre qu'il semble que le maximum soit proche de 0.12 (pour $x \approx 1.7$).

1.4.4.2. *Cas de l'approximation par $g(x)$.* — Commençons par approcher f par la fonction affine par morceau h qui prend les mêmes valeurs que f aux points 0, 1, 2, 3, 4, 5, 6. La fonction h est affine sur tous les intervalles $[j, j+1]$ ($0 \leq j \leq 5$) et telle que :

$$h(j) = f(j) \text{ pour } 0 \leq j \leq 6.$$

Sur chaque intervalle $[j, j+1]$ on peut écrire en vertu de la majoration (5) :

$$|f(x) - h(x)| \leq \frac{1}{2!} |(x-j)(x-j-1)| \sup_{t \in [j, j+1]} |f''(t)|.$$

Donc :

$$|f(x) - h(x)| \leq \frac{1}{2} \times \frac{1}{4} \times \frac{\pi^2}{6},$$

d'où :

$$|f(x) - h(x)| \leq 0.21.$$

Nous allons évaluer maintenant $|h(x) - g(x)|$.

x	0	1	2	3	4	5	6
$f(x)$	0	0.8	3	6	9	11.2	12
$g(x)$	0	1	3	6	9	11	12
$h(x)$	0	0.8	3	6	9	11.2	12

Comme $h(x)$ et $g(x)$ sont des fonctions affines par morceau sur les mêmes points de partage 0, 1, 2, \dots , 6, qu'il y a une symétrie par rapport à $x = 3$ et que $h(x)$ et $g(x)$ coïncident en 0, en 2 et en 3, alors :

$$|h(x) - g(x)| \leq |g(1) - h(1)|.$$

(Le maximum de la valeur absolue de la différence de deux fonctions affines définies sur le même intervalle est atteint à une borne de l'intervalle.)

Or :

$$g(1) = 1 \text{ et } h(1) = f(1) \geq 0.8,$$

donc

$$\sup_{x \in [0,6]} |h(x) - g(x)| \leq 0.20.$$

En conséquence on a une majoration :

$$\sup_{x \in [0,6]} |f(x) - g(x)| \leq 0.41.$$

Cette majoration n'est certainement pas très bonne. En effet l'observation de la figure 3 montre qu'on doit avoir quelque chose comme :

$$\sup_{x \in [0,6]} |f(x) - g(x)| \approx 0.3.$$

Remarque 1.4.4. — Il est certainement plus judicieux dans ce cas d'étudier directement le maximum de la fonction $g(x) - f(x)$ sur l'intervalle $[0, 1]$.

1.5. Approximation de la fonction réciproque

Nous avons utilisé pour approcher l'accroissement de la hauteur en fonction du temps la fonction cubique :

$$P(x) = -\frac{1}{9}x^3 + x^2.$$

On souhaiterait avoir une formule (simple si possible) polynomiale pour trouver le temps en fonction de la hauteur. Bien entendu la fonction réciproque de $P(x)$ n'est pas polynomiale. On va donc chercher à l'interpoler par un polynôme de degré 3. On va chercher $Q(u)$ tel que $Q(0) = 0$, $Q(6) = 3$ et $Q(12) = 6$ plus une autre condition. Comme $P'(0) = P'(6) = 0$, il n'est pas raisonnable de donner une condition sur $Q'(0)$ ou $Q'(12)$. En revanche on peut imposer :

$$Q'(6) = \frac{1}{P'(3)} = \frac{1}{3}.$$

Le polynôme $Q(u)$ obtenu est alors :

$$Q(u) = \frac{1}{216}u^3 - \frac{1}{12}u^2 + \frac{5}{6}u.$$

Cette fonction est représentée sur la figure 6.

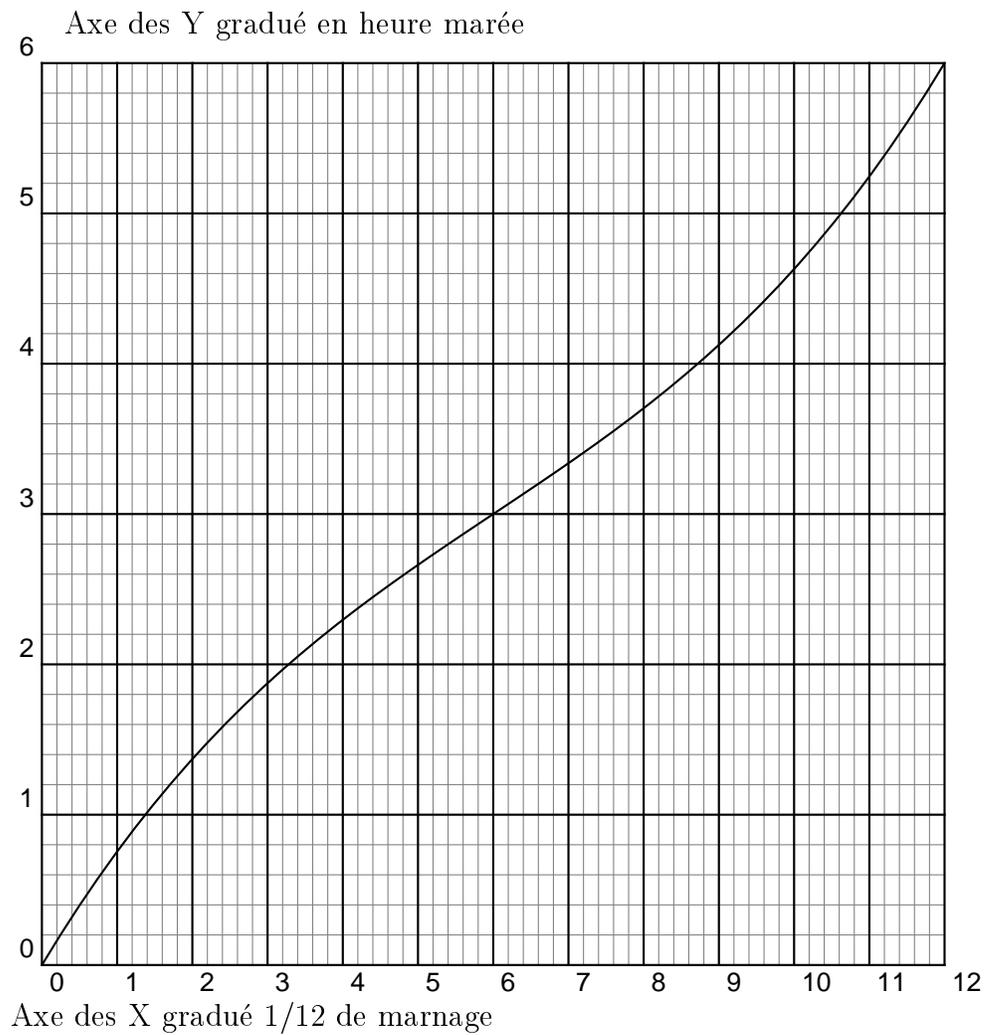


FIGURE 6. La fonction $Q(u)$

On peut aussi au lieu de la condition sur la dérivée, imposer plutôt que la valeur prise en 3 soit 2. Notons alors $R(x)$ le polynôme obtenu :

$$R(u) = \frac{1}{162}u^3 - \frac{1}{9}u^2 + \frac{17}{18}u.$$

Cette fonction est représentée sur la figure 7.

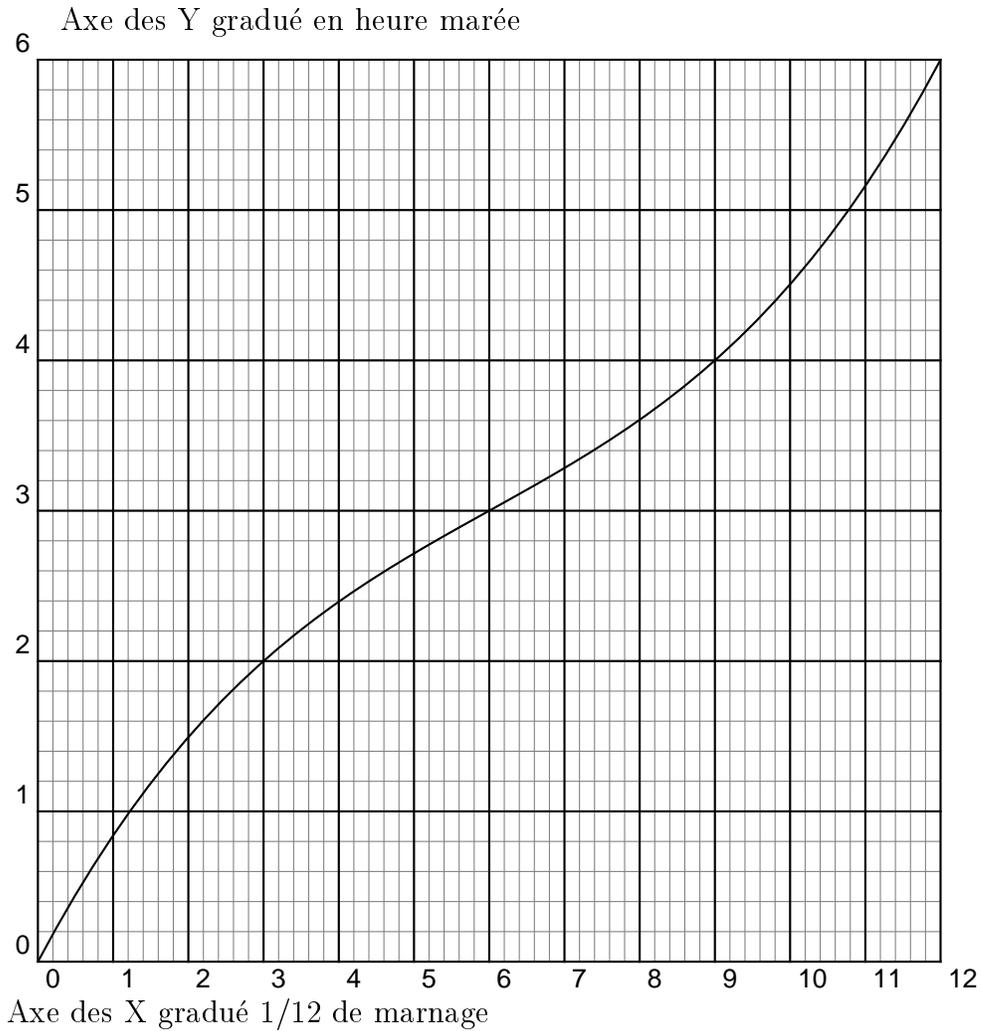


FIGURE 7. La fonction $R(u)$

CHAPITRE 2

ÇA PART EN VRILLE

2.1. Présentation du problème

Nous présentons ici un aspect de la projection de Mercator utilisée pour représenter des portions de la terre sur une carte et en particulier largement utilisée pour les cartes marines. Pour une étude didactique plus globale, nous renvoyons à l'excellente brochure [idBcglgc05].

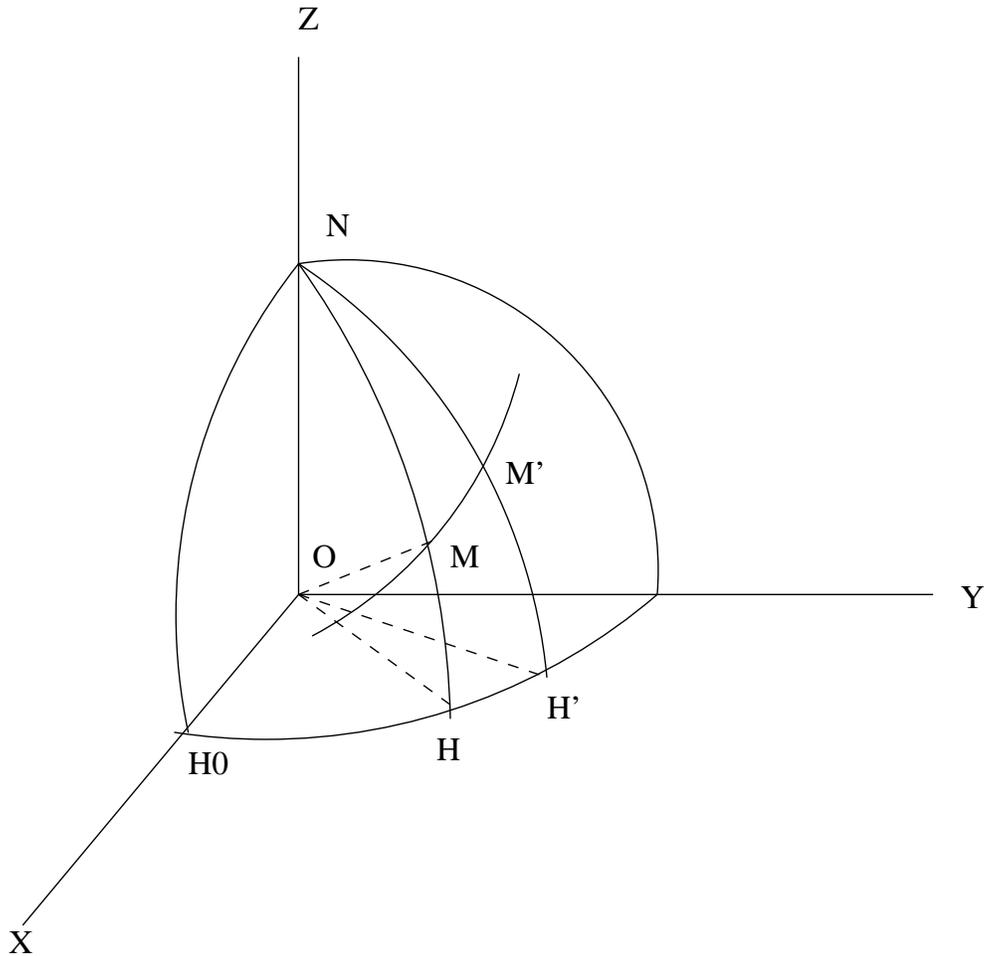


Voici un billet de banque avec le portrait de Mercator.

Gerardus Mercator (1512-1594), de son vrai nom Gerhard Kremer, est un mathématicien et géographe flamand, né à Rupelmonde (Belgique) le 5 Mars 1512. Il crée en 1559 la représentation qui porte son nom et publie un atlas de cartes.

Les marins ayant comme instrument de mesure de la direction un **compas** (c'est-à-dire une boussole), il est commode pour la navigation d'avoir des cartes marines sur lesquelles les trajectoires **à cap constant** (c'est-à-dire qui font toujours le même angle avec le nord) sont des droites. De plus on souhaite évidemment pouvoir mesurer les divers caps suivis directement sur la carte avec un rapporteur (règle Crass par exemple). Pour construire une carte marine il faut donc si possible une transformation qui conserve les angles, c'est-à-dire une transformation conforme.

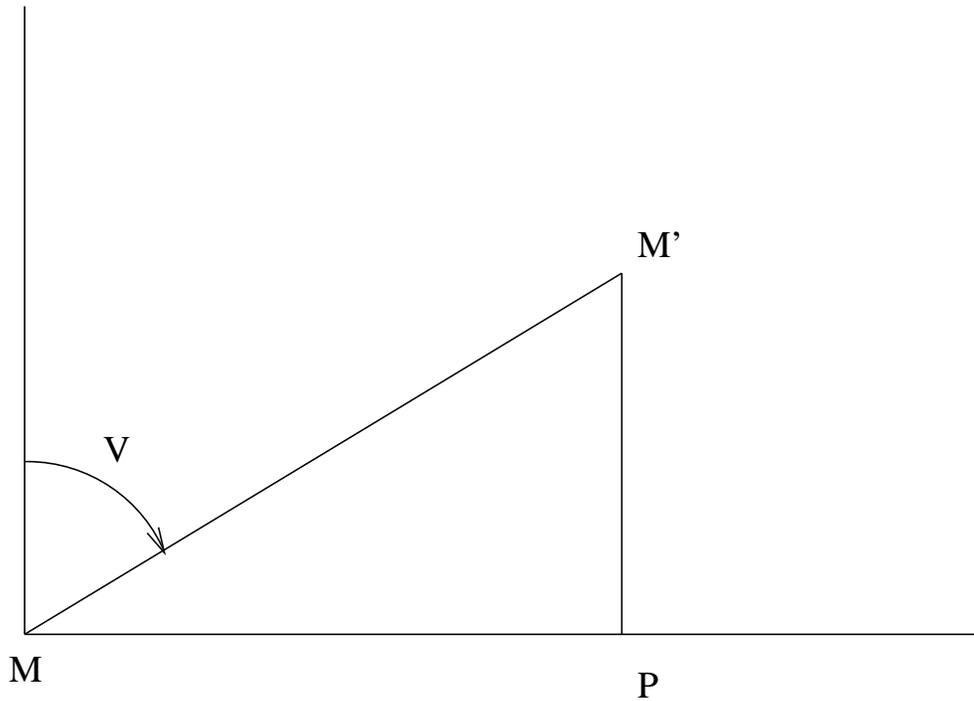
La terre sera assimilée à une sphère \mathcal{S} de centre O et de rayon R . Les pôles nord et sud seront notés N et S . Soit H_0 l'intersection du méridien origine (méridien de Greenwich) avec l'équateur.



2.2. Utilisation du calcul différentiel

Un point M est repéré par sa longitude G et sa latitude ϕ . Le point M décrit une trajectoire à cap V constant (loxodromie). Soit M' un point proche de M sur la trajectoire loxodromique décrite par M . On peut écrire les coordonnées de M et de M' :

$$M \begin{cases} G \\ \phi \end{cases}$$

FIGURE 1. Triangle différentiel au point M

$$M' \begin{cases} G' = G + \Delta G \\ \phi' = \phi + \Delta \phi \end{cases}$$

Introduisons alors le point P intersection du parallèle passant par M avec le méridien passant par M' . Le triangle sphérique MPM' sera assimilé à un triangle plan (cf. figure 1).

L'arc MP (assimilé au segment MP) est un arc de parallèle situé à la latitude ϕ , en conséquence :

$$MP = \Delta G \cos(\phi).$$

La longueur $M'P$ est mesurée par la variation de latitude :

$$M'P = \Delta \phi.$$

Les relations trigonométriques dans le triangle MPM' nous permettent d'exprimer MP en fonction de $M'P$:

$$MP = M'P \tan(V),$$

ce qui donne grâce aux relations précédentes :

$$\Delta G \cos(\phi) = \Delta \phi \tan(V),$$

puis :

$$\Delta G = \tan(V) \frac{\Delta \phi}{\cos(\phi)}.$$

Ceci nous incite à introduire la notion de **latitude croissante**. Considérons la primitive de la fonction :

$$\frac{1}{\cos(\phi)}$$

qui s'annule pour $\phi = 0$, c'est-à-dire la fonction de Gudermann :

$$Gud(\phi) = \ln \left(\tan \left(\frac{\phi}{2} + \frac{\pi}{4} \right) \right).$$

Avec cette notation, si on va d'un point A à un point B par une loxodromie de cap V , alors :

$$G_B - G_A = \tan(V) (Gud(\phi_B) - Gud(\phi_A)),$$

ce qui prouve que sur une carte plane, si l'axe des x (qui mesure les longitudes G) est gradué de manière équidistante, tandis que l'axe des y (qui mesure les latitudes ϕ) est gradué par une échelle qui suit la fonction de Gudermann, alors tout arc de loxodromie est représenté par une droite, et le cap suivi par cette loxodromie est respecté sur la carte.

Remarquons que si les longitudes G_A et G_B sont exprimées en **mille** au lieu d'être exprimées en radian (un mille correspond à la longueur d'un arc d'une minute sur un grand cercle de la terre) alors :

$$(G_B - G_A)_{mille} = \frac{180 * 60}{\pi} \tan(V) (Gud(\phi_B) - Gud(\phi_A)).$$

Cette dernière formule nous permet de construire un canevas de carte marine suivant la représentation appelée **projection de Mercator**. On définit alors la fonction latitude croissante par :

$$\phi_c(\phi) = \frac{180 * 60}{\pi} Gud(\phi),$$

ce qui nous donne :

$$(G_B - G_A)_{mille} = \tan(V) (\phi_c(\phi_B) - \phi_c(\phi_A)).$$

2.3. Méthode géométrique

De nombreux livres de navigation, pour faire comprendre les cartes de Mercator, essaient de présenter la transformation conforme utilisée en donnant une analogie plus ou moins lointaine avec une projection cylindrique. Malheureusement, il n'y a pas d'interprétation géométrique sous cette forme. Il existe cependant une interprétation géométrique mais celle-ci est relativement cachée et utilise l'inversion.

2.3.1. Loxodromie et spirale logarithmique. — Pour bien comprendre l'idée développée dans la suite, rappelons rapidement qu'une spirale logarithmique de point asymptote O est caractérisée par le fait que l'angle formé par le vecteur tangent et le rayon vecteur est constant.

Soit \mathcal{I} l'inversion de pôle S (pôle Sud) qui transforme la sphère \mathcal{S} en le plan équatorial. Le pôle Nord N est transformé en O et les méridiens (privés de S) en les demi-droites issues de O . Comme l'inversion conserve les angles, les loxodromies autres que les parallèles sont transformées en des spirales logarithmiques de point asymptote O , les parallèles sont transformés en des cercles de centre O . L'équateur est invariant.

Soit M un point de longitude G et latitude ϕ de la loxodromie de cap V passant par un point H de longitude G_0 situé sur l'équateur. Soit $M_1 = \mathcal{I}(M)$ le transformé de M par l'inversion \mathcal{I} . Notons $\rho(M_1)$ la distance de M_1 à O . Nous savons que le point M_1 décrit une spirale logarithmique d'équation :

$$\rho(M_1) = R e^{-\frac{1}{\tan(V)}(G-G_0)}.$$

2.3.2. Déroutons la spirale. — Donnons la mesure 2α à l'angle au centre \widehat{MON} . Nous avons alors :

$$\tan(\alpha) = \frac{\rho(M_1)}{R} = e^{-\frac{1}{\tan(V)}(G-G_0)},$$

avec :

$$\phi + 2\alpha = \frac{\pi}{2}.$$

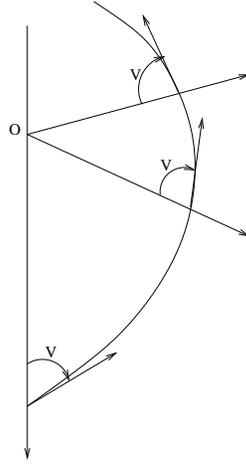


FIGURE 2. Transformée d'une loxodromie

On en conclut que :

$$\alpha = \frac{\pi}{4} - \frac{\phi}{2},$$

et donc :

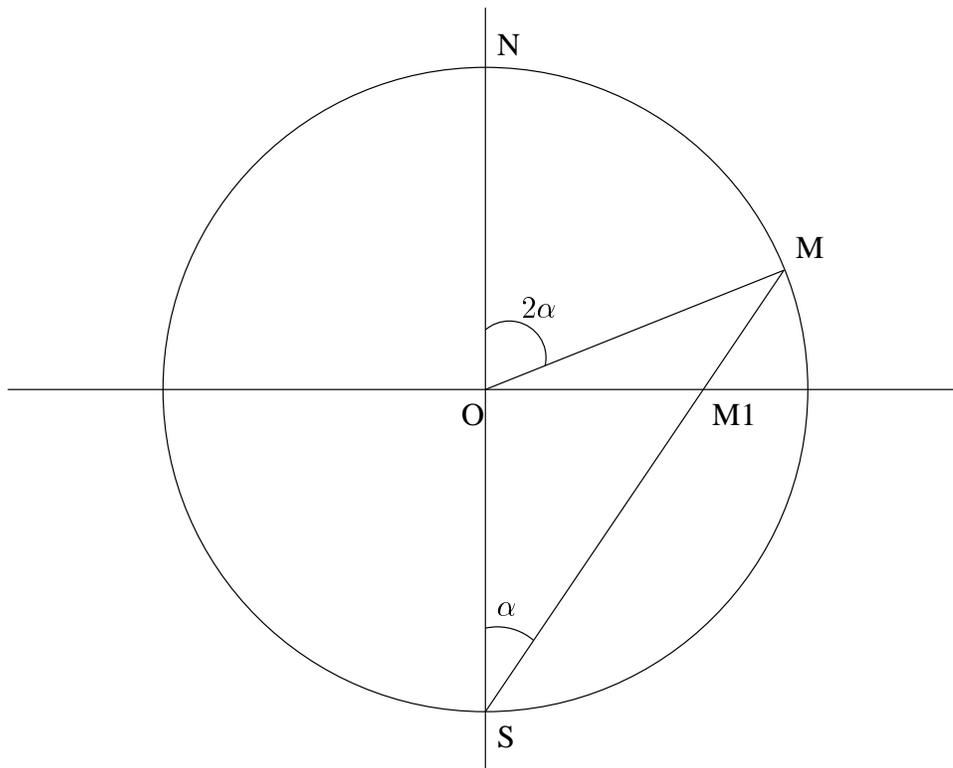
$$\tan\left(\frac{\pi}{4} - \frac{\phi}{2}\right) = e^{-\frac{1}{\tan(V)}(G-G_0)},$$

ou encore :

$$\tan\left(\frac{\pi}{4} + \frac{\phi}{2}\right) = e^{\frac{1}{\tan(V)}(G-G_0)}.$$

On retrouve la relation du paragraphe précédent :

$$G - G_0 = \tan(V) \ln\left(\tan\left(\frac{\pi}{4} + \frac{\phi}{2}\right)\right).$$

FIGURE 3. Plan méridien passant par M

CHAPITRE 3

LA TÊTE AU SOLEIL

Les trois chapitres qui suivent présentent des techniques mathématiques simples, ayant souvent un aspect historique, et relatives à l'astronomie. Ils offrent des pistes permettant de construire des exercices plus complexes.

3.1. Présentation

L'énergie des étoiles est produite par des réactions nucléaires dans le cœur. Lors d'une réaction, une partie de l'énergie produite est évacuée sous la forme d'un photon. La densité près du centre d'une étoile est telle que ce photon n'a aucune chance de survivre : il rencontre rapidement un atome qui l'absorbe ; son énergie est transférée à l'atome, qui se trouve dans un état excité. Au bout d'un certain temps très bref, l'atome se désexcite spontanément, en réémettant un photon (plusieurs photons se partageant l'énergie du photon exciteur, le photon réémis a une longueur d'onde plus grande que celle qu'avait le photon incident).

On appelle *libre parcours moyen* la distance qu'un photon caractéristique peut parcourir avant d'être ainsi absorbé. Dans le Soleil, cette distance est sub-millimétrique. Lorsqu'un photon est absorbé, puis réémis, ce n'est généralement pas dans la même direction. En effet, il est absorbé dans la direction d'où il vient, mais sa réémission se fait dans une direction totalement aléatoire. Le problème qu'on se pose est de savoir si un photon produit au centre du Soleil a une chance d'en sortir un jour !

Considérons un atome qui a été excité par un photon. Il va réémettre un photon, dans une direction quelconque. Pour simplifier le problème, nous allons le traiter à deux dimensions. Le photon est émis selon un angle θ_1 . Le libre parcours moyen sera noté d . Prenons deux axes de coordonnées rectangulaires.

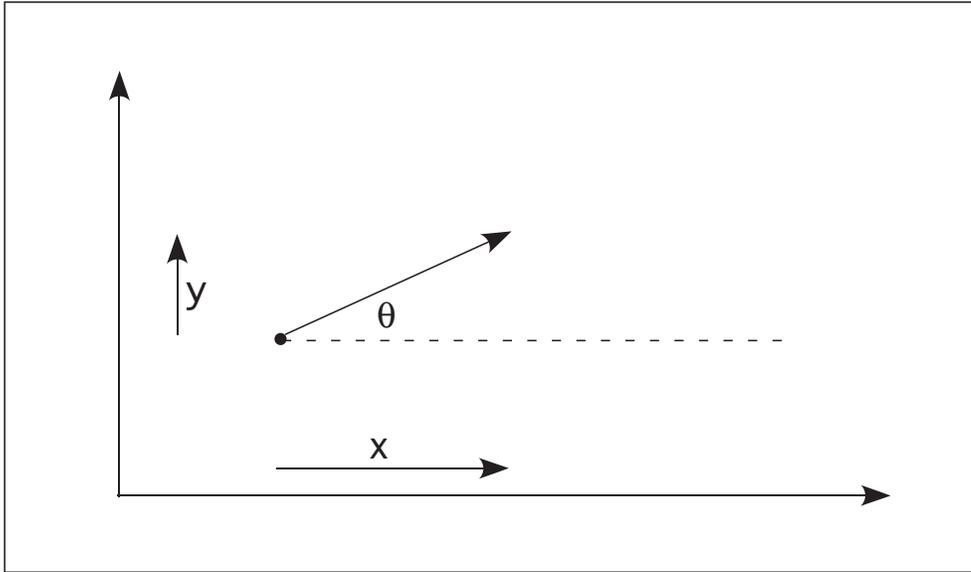


FIGURE 1. Angle de réémission d'un photon

L'angle θ_1 sera calculé par rapport à l'axe des x .

Les projections du déplacement selon les deux axes sont :

$$\begin{aligned}x &= d \cos \theta_1 \\y &= d \sin \theta_1\end{aligned}$$

Après ce parcours, le photon est absorbé, puis réémis dans une nouvelle direction aléatoire θ_2 . Après n parcours élémentaires, sa position sera la somme vectorielle des parcours élémentaires. Ses coordonnées seront donc :

$$x = \sum_{i=1}^n d \cos \theta_i$$

$$y = \sum_{i=1}^n d \sin \theta_i$$

La figure 2 montre un parcours en 4 étapes. A la fin du parcours, la particule s'est déplacée de x horizontalement, et de y verticalement. Ces composantes sont les projections de la somme vectorielle des déplacements élémentaires.

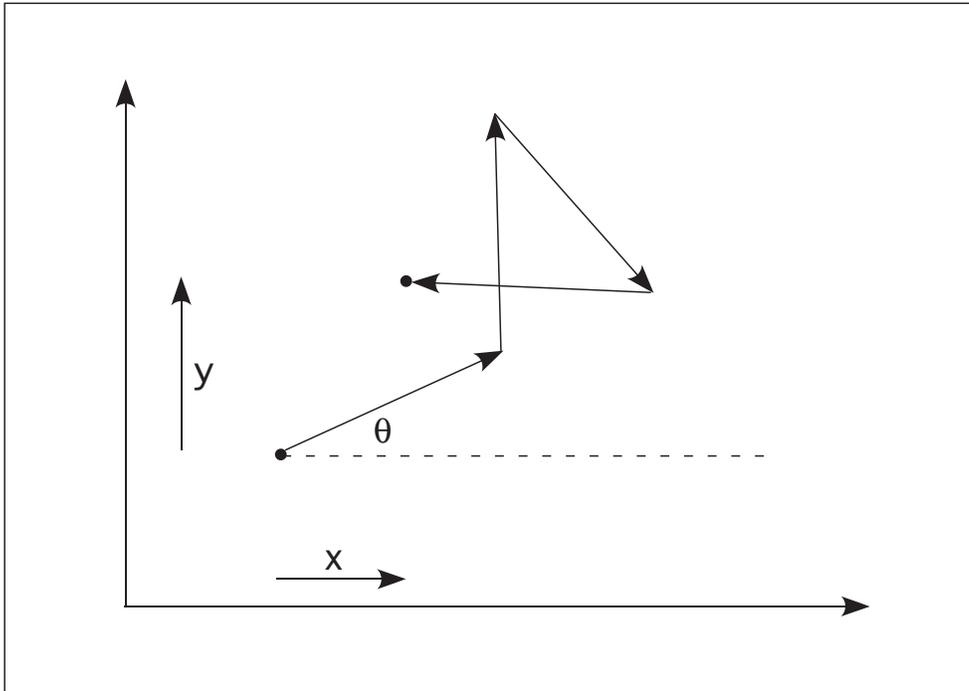


FIGURE 2. Parcours d'un photon

3.2. Marche aléatoire discrète

Dans ce modèle plan simplifié, nous supposons que le photon se déplace d'une distance d dans une certaine direction, après quoi il est réémis dans une autre direction, dans laquelle il se déplace aussi de la distance d et ainsi de suite. On suppose qu'à l'instant initial il est à l'origine $(0, 0)$. Dans la suite on prend d comme unité de longueur. Il est légitime dans un premier temps de considérer que d est fixe, car en pratique la dispersion

de d est toujours très faible. Il s'agit de regarder où est le photon après n étapes ; ses coordonnées sont alors :

$$X = \cos(\theta_1) + \cos(\theta_2) + \dots + \cos(\theta_n)$$

$$Y = \sin(\theta_1) + \sin(\theta_2) + \dots + \sin(\theta_n).$$

Autrement dit :

$$X = X_1 + X_2 + \dots + X_n$$

$$Y = Y_1 + Y_2 + \dots + Y_n$$

où X_1, X_2, \dots, X_n (resp. Y_1, Y_2, \dots, Y_n) sont des variables aléatoires ayant la même loi de probabilité : chacune est $\cos(\theta)$ (resp. $\sin(\theta)$) où θ est uniformément réparti sur $(0, 2\pi)$.

Le théorème central limite que nous rappelons ici s'applique alors à chacune des deux sommes X et Y .

Théorème 3.2.1. — *Soient $X_1, X_2, \dots, X_n, \dots$ des variables aléatoires indépendantes de même loi de répartition de probabilité, de moyenne m et d'écart type s . Soit $S_n = X_1 + X_2 + \dots + X_n$.*

*Alors la répartition de probabilité de $(S_n - nm)/(s * \sqrt{n})$ converge vers la loi normale centrée réduite.*

Ici $m = 0$ (calculer l'intégrale de S_n sur $(0, 2\pi)$) et $s = \sqrt{2}/2 = 0.7$. Donc on peut estimer que $Z_n = S_n/(s * \sqrt{n})$ suit une loi normale réduite.

En conséquence la probabilité pour que :

$$-1.4 * \sqrt{n} \leq S_n \leq 1.4 * \sqrt{n}$$

est de 0.95.

En revanche la probabilité pour que S_n reste bornée tend vers 0 avec n . On peut montrer que S_n tend vers l'infini (en probabilité) en \sqrt{n} . En effet, il suffit de trouver dans la table de la loi normale réduite centrée une constante C telle que la probabilité pour que $-C < Z_n < C$ soit $< 5/100$, et dans ce cas la proba pour que $|S_n| \geq 0.7 * C * \sqrt{n}$ est 95/100.

$$r = d\sqrt{n}$$

Après n cycles absorption-réémission, le photon a parcouru la distance $d\sqrt{n}$.

3.3. Application

Dans le Soleil, dont le rayon est $700000 \text{ km} = 710^{11} \text{ mm}$ (représentant la distance à parcourir par le photon), le libre parcours moyen est de l'ordre de 0.1 mm . Le nombre de cycles absorption-réémission est :

$$n = \frac{r^2}{d^2} = \frac{(7 \cdot 10^{11})^2}{0.1^2} = \frac{49 \cdot 10^{22}}{0.01} = 4.9 \cdot 10^{25}$$

La distance parcourue par le photon est donc :

$$d = 0.1 \text{ mm} \times 4.9 \cdot 10^{25} = 4.9 \cdot 10^{24} \text{ mm} = 4.9 \cdot 10^{18} \text{ km}$$

A la vitesse de la lumière, le photon quittera le Soleil au bout de :

$$t = \frac{4.9 \cdot 10^{18} \text{ km}}{3 \cdot 10^5 \text{ km s}^{-1}} = 1.63 \cdot 10^{13} \text{ s} = 5.17 \cdot 10^5 \text{ ans}$$

Ce calcul approché donne un ordre de grandeur. Il suppose en particulier que le photon est réémis instantanément. Un calcul plus précis donne un temps compris entre 1 et 10 millions d'années. Le temps passé par le photon à l'intérieur du Soleil lui permettrait d'atteindre, dans l'espace libre, quelques unes des galaxies les plus proches.

La marche aléatoire se retrouve dans de nombreux phénomènes naturels ou artificiels. Il s'agit d'un processus de Markov, car en chaque point, le point suivant ne dépend que des probabilités locales, non du passé de la particule.

3.4. Du côté de chez Brown...

Le mouvement brownien est un autre exemple en physique. Il s'agit d'un mouvement aléatoire de fines particules en suspension dans un milieu. Il a été observé pour la première fois par Robert Brown en 1827, sur des grains de pollen en suspension dans l'eau. A la loupe, on voit les petits grains se déplacer, puis brusquement changer de direction, et ainsi de suite.

L'explication de ce mouvement a été difficile à trouver. Les grains de pollen sont baignés dans les molécules d'eau (dont on ne connaissait pas l'existence avec certitude). L'agitation thermique des molécules d'eau déplace les grains. Mais il est facile de constater que l'énergie individuelle d'une molécule est insuffisante pour déplacer un objet aussi gros qu'un

grain de pollen. Aussi, il faut considérer que plusieurs molécules s'allient aléatoirement pour pousser un grain. La théorie du mouvement brownien a été faite par Einstein.

Une autre façon de présenter le mouvement brownien consiste à dire que le mouvement quadratique moyen est proportionnel au temps. Soit $x(t)$ la distance de la particule à l'origine (son point de départ), à l'instant t . La moyenne quadratique de cette distance est :

$$\langle X^2(t) \rangle = \frac{1}{t} \int_0^t x^2(\tau) d\tau.$$

Cette distance moyenne étant proportionnelle au temps, on a :

$$\langle X^2(t) \rangle = 2aDt$$

où D est le coefficient de diffusion, a est la dimension du mouvement, linéaire, planaire ou spatial. L'expression de D , donnée par la mécanique statistique, est :

$$D = \frac{RT}{6\pi\eta Nr}$$

où R est la constante des gaz parfaits, T la température, η la viscosité du fluide dans lequel baignent les particules, N le nombre d'Avogadro, et r le rayon de la particule.

Einstein en a tiré le nombre d'Avogadro, fonction de la moyenne quadratique. La mesure de cette moyenne a donné enfin la valeur du nombre d'Avogadro.

3.5. ... et à la Bourse !

La marche aléatoire est aussi utilisée pour modéliser l'évolution d'un cours de bourse, dans un marché financier concurrentiel. Cette méthode a été introduite en 1863 par Jules Regnault. Chaque opérateur attribue implicitement une probabilité de hausse à un titre donné. Selon cette probabilité, il va vendre ou acheter, modifiant ainsi le cours du titre. Dans leur évaluation, les opérateurs font des erreurs, mais celles-ci suivent la loi classique des erreurs, la loi normale. Il existe ainsi deux

groupes d'opérateurs, dits haussiers et baissiers, qui sont équirépartis autour de la moyenne (cours inchangé). Alors, un opérateur passe à chaque instant d'un état haussier ou baissier, à un nouvel état haussier ou baissier. On obtient donc une marche aléatoire avec deux états possibles équiprobables. Il est équivalent d'acheter ou de vendre ! Regnault a de plus montré expérimentalement l'indépendance des mouvements des cours de bourse, ce qui en fait bien une marche aléatoire... Enfin, par l'analyse passée des cours d'un titre particulier, il a montré que l'écart entre le cours initial et le cours final est bien proportionnel à la racine carrée du temps, ce qui achève de justifier la solution.

3.6. ... ou chez les fourmis

La marche aléatoire a été aussi invoquée pour expliquer comment les fourmis construisent des tas. Une telle activité pourrait faire penser à une intelligence collective de ces insectes, mais un comportement indépendant et simple, par une marche aléatoire, suffit à expliquer la formation de tas.

Ces recherches ont débouché sur la définition de l'intelligence répartie, ou intelligence collective : un ensemble de petits acteurs, ayant chacun des possibilités rudimentaires, parvient à réaliser des tâches qu'on croyait intelligentes. Cette approche semble extrêmement intéressante pour l'exploration future des planètes, faite aujourd'hui à l'aide de sondes très coûteuses, mais toutefois limitées dans leurs mouvements et leurs capacités. Lorsqu'on voudra faire des recherches systématiques sur Mars par exemple, il sera peut-être bien plus économique d'envoyer un escadron de petits explorateurs rudimentaires, mais qui pourront quadriller le sol. On envisage de faire communiquer entre eux ces petits robots, pour les rendre plus performants.

3.7. Enfin, parmi les comètes

Dans les confins du système solaire se trouve un immense nuage de comètes, qui tournent autour du Soleil selon des orbites grossièrement circulaires. On estime qu'il doit y en avoir des milliards. Les plus lointaines se trouvent à presque une année-lumière du Soleil, c'est-à-dire à

peine 5 fois plus près du Soleil que des étoiles voisines. Dans ces conditions, bien qu'appartenant vraiment à notre système, ces comètes sont parfois perturbées par les autres étoiles, avec un temps caractéristique de l'ordre de 100.000 *ans*.

Les astres perturbateurs, bien qu'entraînés ensemble dans la rotation de la Galaxie, ont par rapport au Soleil une marche aléatoire en direction et en vitesse. Aussi, leurs perturbations sont-elles d'intensité quelconque, certaines accélérant une comète donnée, d'autres la ralentissant. A chaque pas (disons à chaque orbite, lorsqu'elle passe à son aphélie), la vitesse de la comète subira un incrément ou un décrement au hasard. Il s'agit donc d'une marche aléatoire. Par conséquent, les perturbations n'agissent que selon la racine carrée du temps, et ceci explique la stabilité du nuage de Oort : il s'est formé en même temps que le système solaire, il y a 5 milliards d'années ; si l'éjection d'une comète était proportionnelle au temps, il y a longtemps que le nuage de Oort aurait disparu (les perturbations auraient produit un phénomène de résonance).

CHAPITRE 4

ÇA NE TOURNE PAS ROND

Considérons les planètes qui tournent autour du Soleil. On appelle *révolution sidérale* le temps que met la planète, repérée par rapport aux étoiles, pour faire un tour complet autour du Soleil. Comme deux coureurs qui n'iraient pas à la même vitesse sur la cendrée, la plus proche du Soleil double périodiquement la plus lointaine. Combien de temps s'écoule entre deux rencontres ? Autrement dit, combien de temps s'écoule pour que le coureur A revoie le coureur B à côté de lui ?

On appelle *révolution synodique* le temps au bout duquel le mouvement apparent d'une planète se reproduit. Nous le définirons selon l'alignement de la planète et du Soleil par rapport à la Terre. Ces positions particulières sont les *oppositions* pour les *planètes supérieures* (plus lointaines que la Terre), et les *conjonctions inférieures* pour les *planètes inférieures* (plus proches du Soleil).

La révolution synodique est donc une conséquence des deux mouvements de la Terre et de la planète. Soient T_{sid} et T'_{sid} les périodes de révolution sidérale de la Terre et de la planète.

A chaque instant, la planète se déplace donc d'un angle $2\pi/T'_{sid}$. Le mouvement apparent d'une planète est la différence entre le mouvement de la Terre et celui de la planète :

$$\frac{2\pi}{T_{sid}} - \frac{2\pi}{T'_{sid}}.$$

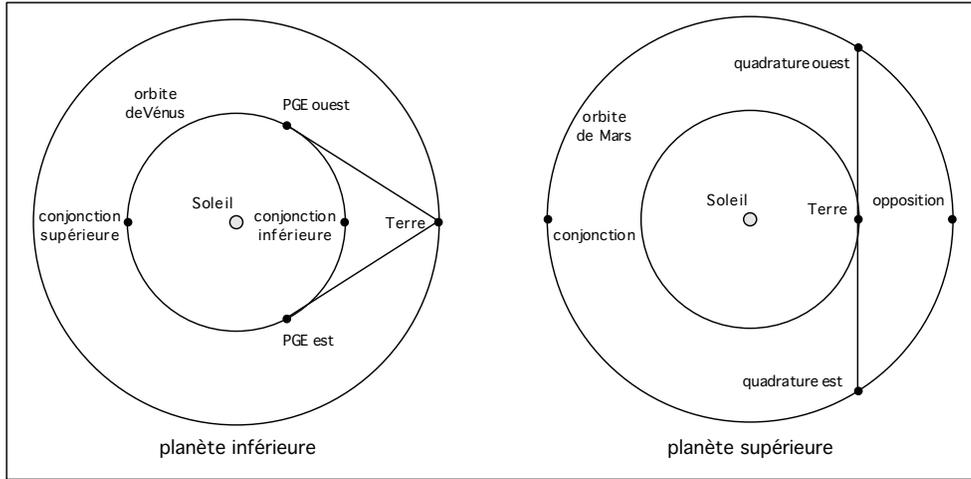


FIGURE 1. Alignements de planètes

Cette formule est valable pour les planètes supérieures. Pour Mercure et Vénus, il convient de prendre l'opposé :

$$\frac{2\pi}{T'_{sid}} - \frac{2\pi}{T_{sid}}$$

Soit θ la période du mouvement apparent. Par unité de temps, le mouvement apparent évolue de l'angle $\frac{2\pi}{\theta}$ et donc :

$$\frac{2\pi}{\theta} = \frac{2\pi}{T_{sid}} - \frac{2\pi}{T'_{sid}}$$

ou encore :

$$\frac{1}{\theta} = \frac{1}{T_{sid}} - \frac{1}{T'_{sid}}$$

Exemple :

prenons le cas de Mars :

$$T_{sid} \approx 365 j \quad T'_{sid} \approx 1 an \quad 321 j = 686 j$$

$$\frac{1}{\theta} = \frac{1}{T_{sid}} - \frac{1}{T'_{sid}} = \frac{1}{365} - \frac{1}{686} = 0,0027397 - 0,0014577 = 0,0012820$$

$\theta = 780$ jours, soit deux ans et 50 jours.

Cette durée est intéressante, car c'est le temps qui s'écoule entre deux fenêtres d'observation de Mars, ou entre deux tirs de fusée vers la planète.

On remarquera que, si T'_{sid} croît, $1/T'_{sid}$ décroît. Donc, $1/\theta$ tend vers $1/T_{sid}$ lorsque T'_{sid} tend vers l'infini, et θ tend vers T_{sid} . Par conséquent, si on considère une planète lointaine, sa période synodique s'approche d'autant plus de l'année terrestre qu'elle est plus lointaine. Ainsi, la période synodique de Pluton est très voisine de l'année terrestre. C'est le même effet de perspective que nous observons sur les arbres proches et lointains vus de la fenêtre d'un train.

On pourra calculer les périodes synodiques des différentes planètes, à partir du tableau suivant qui donne leur période sidérale :

planète	T_{sid}	p. syn.	%	planète	T_{sid}	p. syn.	%
Mercure	88 j			Saturne	29 a 167 j		
Vénus	224 j			Uranus	84 a 7 j		
Mars	1 a 321 j			Neptune	164 a 280 j		
Jupiter	11 a 314 j			Pluton	248 a 157 j		

Comparer les valeurs obtenues aux révolutions sidérales, selon la distance de la planète au Soleil. Pour cela, on pourra les exprimer en pourcentages.

Cycle de Méton

La Lune a eu, dans le passé, une très grande importance, parce qu'elle était la seule lumière nocturne (à part quelques fumeuses lampes à huile), et le meilleur moyen de mesurer le temps. Elle marque le rythme du temps plus aisément que les insaisissables saisons... Le cycle de Méton (IV^{ème} siècle avant JC) a permis la prévision des phases. Il est totalement empirique, et constate que les phases de la Lune se reproduisent à l'identique (presque) au bout d'un certain temps.

Un cycle est une période raisonnable de k années contenant un nombre entier p de mois lunaires. Nous allons retrouver le cycle de Méton en utilisant des valeurs proches de celles connues à l'époque.

année solaire de 365,25 jours, et mois lunaire de 29,53 jours

On doit vérifier :

$$365,25 k \approx 29,53 p \text{ avec } k \text{ et } p \text{ entiers}$$

Divisant tout par 29,53 on obtient : $p \approx 365,25 k / 29,53 = 12,3688 k$

Donc $p \approx 12,3688 k = (12 + 0,3688) k = 12 k + 0,3688 k$

k étant un entier, ainsi que p : $0,3688 k$ doit être entier.

On construit le tableau des multiples :

$k = 1$	2	3	4	5	6	7	8	9	10
0,368	0,738	1,106	1,475	1,844	2,213	2,582	2,950	3,319	3,688
$k = 11$	12	13	14	15	16	17	18	19	20
4,057	4,426	4,794	5,163	5,532	5,901	6,270	6,638	7,007	7,376

Dans ce tableau, il faut rechercher les multiples qui sont pratiquement des entiers.

- $k = 8$; $p \approx 12,3688 \times 8 = 98,950$, donc $p = 99$. 8 ans comptent 99 mois ; C'est l'Octaétéride des Grecs : (mois de 29 et 30 j alternés), les années 3, 5 et 8 du cycle comportant un mois supplémentaire de 30 j. La moyenne est de 365,25 jours. Cette durée semble connue depuis -775.
- $k = 11$; $p = 136$. Gain très faible par rapport à l'Octaétéride. Le système n'a pas été employé.
- $k = 19$; valeur entière approchée à 7 millièmes près ! Trouvée par Méton, elle est la base du cycle portant son nom. $p \approx 235,0072$ donc $p = 235$ mois. L'erreur est de $6939.75 - 6939.55 = 0,20 j$, ou un peu moins de 6 heures. Les éclipses se reproduisent donc, d'un cycle à l'autre, avec un décalage de six heures. Pour les éclipses totales de Soleil, ceci revient à les reporter $1/3$ de tour plus loin sur la planète. L'homologue d'une éclipse totale se reproduira donc $120i\frac{1}{2}$ plus loin en longitude.

Si on note précisément les dates et heures des éclipses pendant 19 ans, on retrouvera les mêmes pendant les 19 années suivantes, avec un léger décalage temporel. A $k = 19$ correspond $p = 235$. La différence entre $365,25 k$ et $29,53 p$ vaut : $365,25 \times 19 - 29,53 \times 235 = 6939.75 - 6939.55 = 0,20 j$

D'un cycle à l'autre, les éclipses se reproduisent donc avec une avance de 5 heures.

En utilisant cette technique, Hipparque a obtenu une lunaison moyenne de 29,5305851 j (29 jours 12 h 44 min 2 s), ce qui représente moins

d'une seconde d'erreur!! Ceci vers 130 avant J.C.... et malgré les fortes variations de la lunaison vraie par rapport à la lunaison moyenne.

Etablissement d'un calendrier

Le calendrier est basé sur l'année tropique. Celle-ci est l'intervalle de temps qui s'écoule entre deux équinoxes de printemps successifs. Sa valeur exacte est de 365,2422 jours. On écrit : $365,2422 = 365 + a/b$ avec a et b entiers.

Cette écriture signifie qu'il faut construire une année de base de 365 jours, et ajouter a jours dans une période de b années. Par exemple, $365 + 7/29$ signifie qu'il faut rajouter $7/29$ de jour par an, ou bien 7 jours en 29 ans.

On cherche des approximations.

1. $a = 0$; année de 365 jours, utilisée par de nombreux calendriers anciens ;
2. fixons $a = 1$. On cherche donc à résoudre $365,2422 = 365 + 1/b$. Il vient $b = 1/(365,2422 - 365) = 4,12882$

$$365,2422 = 365 + 1/4,12882$$

Il faudrait ajouter 1 jour tous les 4,12882 ans ; ce n'est pas très pratique !

On prend $b = 4$: c'est l'année julienne de $365j1/4$.

3. On applique le même procédé au nombre qu'on vient d'approcher : $4,12882 = 4 + 1/b_1$ on obtient $b_1 = 7,76282$, d'où année

$$a = 365 + \frac{1}{4 + \frac{1}{7,76282}}$$

on conserve la seule partie entière :

$$a = 365 + \frac{1}{4 + \frac{1}{7}} = 365 + \frac{7}{28}$$

Ce qui correspond à une année moyenne de 365,24138 j. L'erreur est de $365,2422 - 365,24138$ jours = 0,00082 j, ce qui ne représente que 1 min 11 s.

4. On continue d'appliquer le même procédé : $7,76282 = 7 + 1/b_2$ d'où $b_2 = 1,3109$

$$a = 365 + \frac{1}{4 + \frac{1}{7 + \frac{1}{1,3109}}}$$

et on ignore la partie décimale :

$$a = 365 + \frac{1}{4 + \frac{1}{7 + \frac{1}{1}}} = 365 + \frac{8}{33}$$

C'est le calendrier persan ! $8/33 = 0,2424242424$ L'erreur n'est que de $0,2424242424 - 0,2422 = 0,000224$ j = 19 secondes... La règle qui consiste à ajouter 8 jours bissextils dans toute période de 33 ans est plus simple que les règles grégoriennes de notre calendrier.

On reconnaît dans cette méthode le développement en fractions continues. Le calcul peut se poursuivre, et les résultats sont donnés par le tableau suivant :

coefficients											p	q	p/q	validite
365											0	1	0	4
365	4										1	4	0,25	128
365	4	7									7	29	0,2413793103	1.218
365	4	7	1								8	33	0,24242424	4.459
365	4	7	1	3							31	128	0,2421875	80.000
365	4	7	1	3	4						132	545	0,2422018348	545.000
365	4	7	1	3	4	1					163	673	0,2421991085	1.121.667
365	4	7	1	3	4	1	1				295	1218	0,2422003284	3.045.000
365	4	7	1	3	4	1	1	1			458	1891	0,2421998946	9.454.998
365	4	7	1	3	4	1	1	1	1		753	3109	0,2422000640	15.545.006
365	4	7	1	3	4	1	1	1	1	1	1211	5000	0,2422	∞

La dernière valeur est évidente : $2.422 = 0,2422 \times 10.000 = 0,2422 \times 2 \times 5.000$. Donc $0,2422 = \frac{2.422}{2 \times 5.000} = \frac{1.211}{5.000}$.

Année grégorienne

Alors que l'année julienne, simple, s'obtient très bien par ce calcul, l'année grégorienne qui lui a succédé en 1582 n'est pas basée sur le même principe. Elle n'a pas été obtenue directement, par un calcul d'approximation plus poussé, mais par un ajustement de l'année julienne.

Ceci peut s'expliquer pour des raisons de commodité, la modification légère (sauf sur un point qui a posé beaucoup de problèmes sociaux) est passée pratiquement inaperçue.

La différence entre l'année tropique ($365,2422$ j) et l'année julienne ($365,25$ j) appelait la réforme, il est facile de le montrer :

l'erreur est donc de $365,25j - 365,2422j = 0,0078j$ par an, ou $0,78j$ par siècle. Ceci est très proche de $0,75j = 3/4$ j. Donc en 4 siècles, l'erreur est de 3 jours en trop.

La réforme grégorienne a fixé des règles simples pour les supprimer :

- Les années séculaires ne sont bissextiles que si leur millésime est divisible par 400
- Les autres suivent la règle julienne (millésime divisible par 4)

4 siècles juliens = $400 \times 365,25$ j = 146.100 j.

4 siècles grégoriens = $146.100 - 3 = 146.097$ j.

La durée moyenne de l'année grégorienne est donc de $146.097/400 = 365,2425$ j. L'erreur par rapport à l'année tropique est de $0,2425 - 0,2422 = 0,0003$ j qui correspond à 26 secondes par an.

Il est remarquable que les Perses aient obtenu une valeur un peu meilleure bien avant !

Nous connaissons aujourd'hui la durée précise de l'année tropique ! Elle nous a permis de faire ce calcul. Historiquement, les choses se sont passées dans l'ordre inverse : c'est l'observation des erreurs du calendrier sur de très longues périodes qui déterminé la valeur moyenne de l'année tropique.

Remarque : Tous les pays ne sont pas passés au calendrier grégorien à la même époque. Par exemple en Espagne et en France, le calendrier a été réformé très tôt (dès 1582). Il n'en est pas de même en Angleterre par exemple où le calendrier grégorien n'a été utilisé qu'à partir de 1752.

CHAPITRE 5

ἌΣΤΡΟΝΟΜΟΓΕΟΜΕΤΡΗΣ

Géométrie signifie mesure de la Terre. L'origine se trouve dans la crue annuelle du Nil : l'inondation des terres par le Nil effaçait toute trace du cadastre. Aussi, chaque année il fallait refaire les bornages des champs. L'art de la géométrie a été poussé très loin par les Grecs. Euclide a achevé l'œuvre en définissant les axiomes de la Géométrie. La seule, celle qui décrit le monde...

La trigonométrie repose sur la similitude des triangles. Deux triangles semblables ont les mêmes proportions. Ces proportions constituent les rapports trigonométriques. Depuis ses origines, la trigonométrie s'est constituée par tabulation des rapports, étude des relations qu'ils ont entre eux, puis nouvelles définitions...

5.1. Mesure du rayon de la Terre

Cette mesure a été imaginée et réalisée par Eratosthène. Au solstice d'été, le Soleil est exactement à la verticale de Syène. Ceci n'est pas dû au hasard, mais tout simplement au fait que la ville est construite exactement sur le tropique du Cancer. Les puits étant généralement creusés à la verticale, le fond d'un puits dans cette ville est brièvement éclairé par le Soleil le jour du solstice d'été. Cette constatation prouve que le Soleil est bien à la verticale du lieu.

Le même jour, on mesure l'ombre d'un obélisque à Alexandrie. les deux villes se trouvant à peu près sur le même méridien, cet angle est

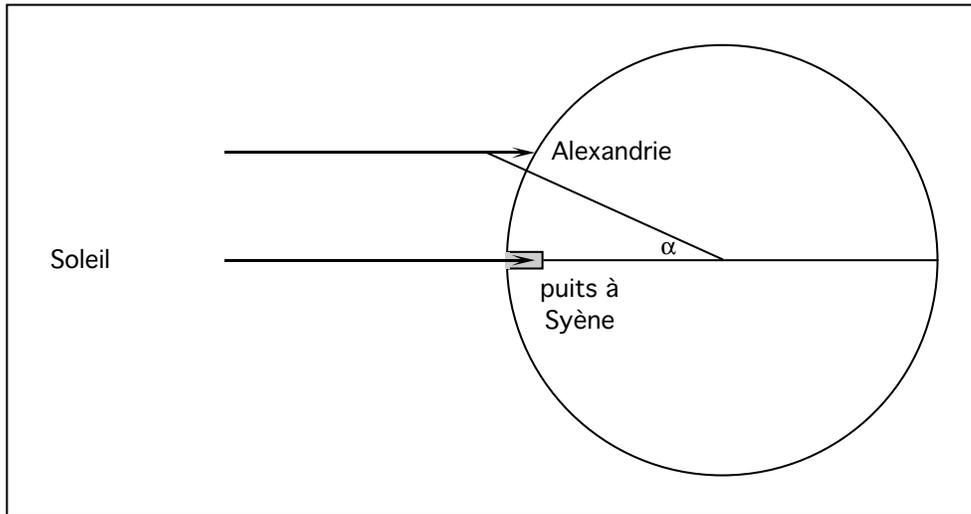


FIGURE 1. Mesure du rayon de la Terre

égal à leur différence de latitude. La distance entre les deux villes est mesurée par le pas des chameaux. Peut-être un peu moins précise qu'une mesure moderne, la distance obtenue est tout de même très fiable, car les Egyptiens de l'époque avaient une grande habitude de ce genre de mesure. Soient L la circonférence de la Terre, d la distance entre les deux villes, et α l'angle mesuré.

Eratosthène a trouvé 252.000 stades, soit 39.564.000 m ou 39.564 km. Cette valeur est vraiment excellente. Une seule incertitude subsiste sur cet exploit : il y avait à l'époque plusieurs stades différents ! Et nous ignorons lequel a été utilisé. Celui qui a servi ici est le plus probable historiquement, mais si on en utilise un autre, la valeur obtenue serait un peu moins bonne. Quoi qu'il en soit, la méthode utilisée est excellente.

5.2. Distance de la Lune (Aristarque de Samos)

On suppose le Soleil très loin. Dans ces conditions, l'ombre de la Terre, qui est un cône, peut être considérée comme cylindrique. Au niveau de la Lune, elle a donc le même diamètre que la Terre.

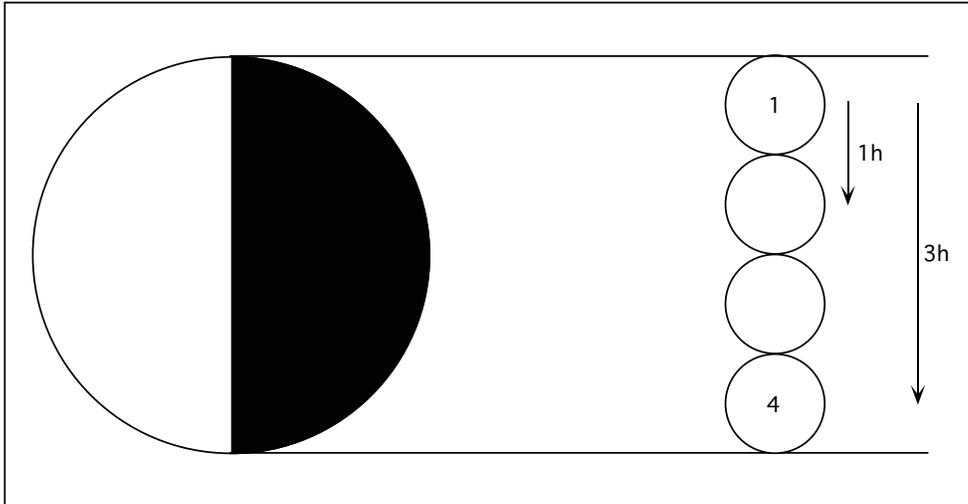


FIGURE 2. La Lune dans l'ombre de la Terre

Le temps t_1 écoulé entre le début de l'entrée dans l'ombre et le début de la totalité est proportionnel au diamètre de la lune. Le temps t_2 passé par la lune dans l'ombre de la Terre est proportionnel au diamètre de la Terre. Donc, le rapport t_1/t_2 est égal au rapport d/D . Ce rapport est proche de 4. La Lune est donc quatre fois plus petite que la Terre : $d = D / 4$. On peut déduire la distance de la Terre à la Lune. On mesure un diamètre apparent de la Lune de $30'$, alors que son diamètre linéaire est $D / 4$.

On construit un triangle rectangle d'angle au sommet égal à $30'$ (figure 3). On mesure ses côtés a et b . Ce triangle est semblable au triangle formé par l'observateur et la Lune. Alors, $TL / d = b / a = k$ $TL = k d = k D / 4 = k/4 D = k/2 R$ Les premières estimations étaient $TL = 80 R$; du temps de Ptolémée, le rapport était ramené à $60 R$, ce qui constitue une excellente mesure.

5.3. Calcul de la distance de Vénus au Soleil

Vénus est une planète intérieure. A l'élongation maximale, le triangle que forment les trois astres est rectangle au sommet Vénus (figure 4).

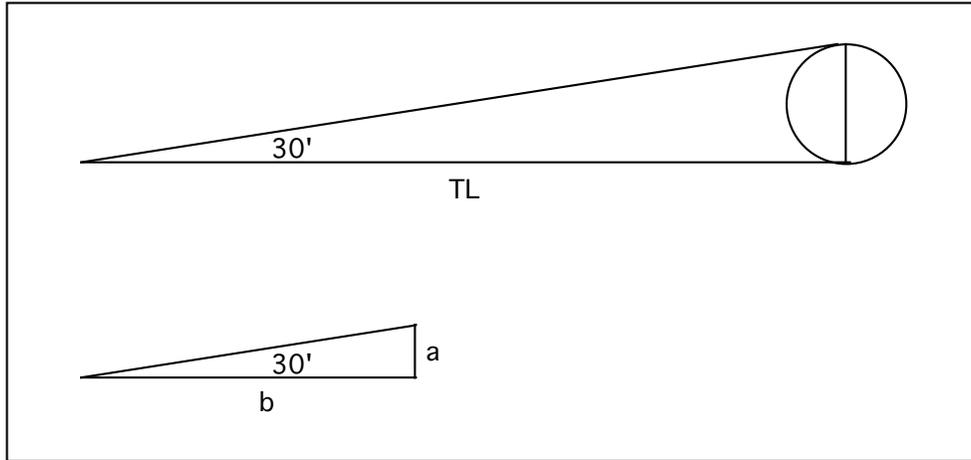


FIGURE 3. Résolution du triangle

On notera VS le segment Vénus-Soleil, TS le segment Terre-Soleil. Alors : $VS = TS \sin \alpha$. On mesure α très facilement à l'aide d'une montre ! Le principe est très simple : on note l'instant du coucher du Soleil (le moment où le centre du Soleil passe en dessous de l'horizon) ; puis on regarde Vénus apparaître dans le ciel, en descendre vers l'horizon. On note l'instant de son coucher. Pour que l'observation soit correcte, il faut que l'horizon soit assez plat, que le Soleil et la planète se couchent à une même hauteur. La différence de temps entre les deux couchers est une mesure de la distance angulaire des deux astres.

En 24 heures, chacun tourne ainsi de 360° (à leur mouvement propre près). Donc l'angle mesuré, rapporté à 24 heures, donne l'angle rapporté à 360° . Supposons que Vénus se couche deux heures après le Soleil : 2 heures correspondent à $\frac{1}{12}$ lorsque 24 heures correspondent à 360° . On en déduit que Vénus est à $360^\circ/12 = 30^\circ$ du Soleil. Pendant les quelques heures séparant les deux couchers, on peut négliger les mouvements propres des deux astres pour la précision que nous souhaitons atteindre.

Plusieurs observations, de soir en soir, donnent l'angle maximum entre les deux astres. Cet angle correspond au triangle rectangle. On trouve une valeur proche de 45° . Son sinus vaut 0.707. On vient donc de déterminer que $VS = 0.707 TS$. Dans ces conditions, si on prend TS pour unité, on

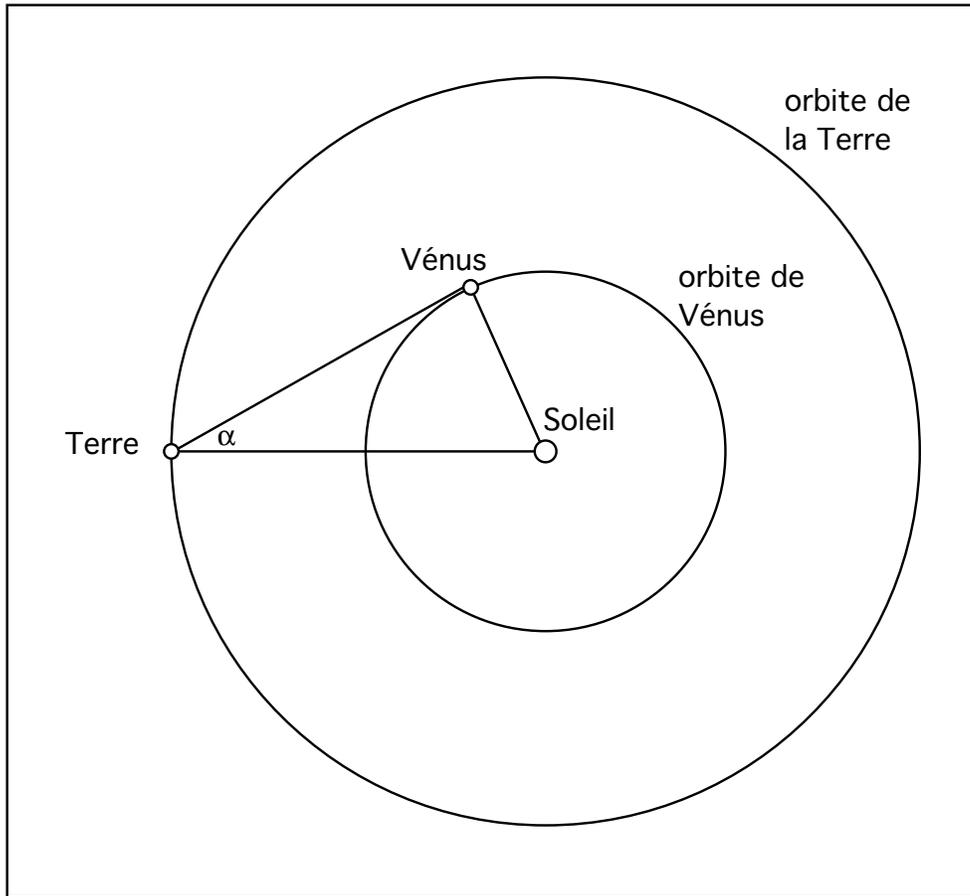


FIGURE 4. Distance de Vénus au Soleil

a $VS = 0.707$. C'est ce qu'ont fait les astronomes, et c'est l'origine de l'unité astronomique (distance moyenne de la Terre au Soleil).

Il est beaucoup plus difficile de rattacher l'unité astronomique aux unités terrestres (km). Un principe totalement différent doit être utilisé pour cela, et c'est la parallaxe qui est à son origine. Le principe est d'observer le passage d'une planète intérieure, Mercure ou Vénus, devant le Soleil, de deux endroits les plus éloignés possible sur Terre. La distance entre ces lieux sera suffisante pour que la planète ne se projette pas au même endroit du Soleil, et que le temps du passage soit différent.

Une mesure précise permettra, après quelques calculs, de déterminer la distance du Soleil.

La première mesure a été effectuée lors d'un passage de Mercure. Une plus grande précision est obtenue avec les passages de Vénus, mais ils sont beaucoup plus rares. Les deux derniers sont ceux des 6 décembre 1882 et 8 juin 2004 ; les deux prochains auront lieu les 6 juin 2012 et 11 décembre 2117. Comme on peut le voir, nous avons beaucoup de chance d'avoir deux passages visibles en peu de temps (8 ans). La périodicité des passages de Vénus est de 8 ans, 121,5 ans, 8 ans, et 105,5 ans. Après quoi le cycle recommence.

Maintenant, les distances entre les planètes sont mesurées beaucoup plus précisément par radar.

La trigonométrie sphérique

La trigonométrie sphérique sert pour calculer les positions sur la Terre, et les distances entre deux points. Elle est donc indispensable pour calculer précisément les passages de Vénus...

Géométrie + trigonométrie

Mouvement elliptique :

Le Soleil est au foyer S de l'ellipse (figure 5). A est le périhélie (du grec *peri* = proche, et *helios* = Soleil). L'angle ASP est nommé anomalie vraie, et noté v . L'angle AOP' est nommé anomalie excentrique, et noté u . Dans ce qui suit, la fonction \mathcal{S} représente la surface de la figure désignée en paramètre. L'anomalie vraie et l'anomalie excentrique sont liées par une relation trigonométrique simple :

$$\operatorname{tg}\left(\frac{v}{2}\right) = \sqrt{\frac{1+e}{1-e}} \operatorname{tg}\left(\frac{u}{2}\right).$$

Détermination de l'équation de Kepler :

$$\mathcal{S}(OSP') = \frac{OS.HP'}{2} = \frac{c.HP'}{2}$$

$$\mathcal{S}(OAP') = \frac{a^2 u}{2}$$

$$\mathcal{S}(SAP') = \mathcal{S}(OAP') - \mathcal{S}(OSP')$$

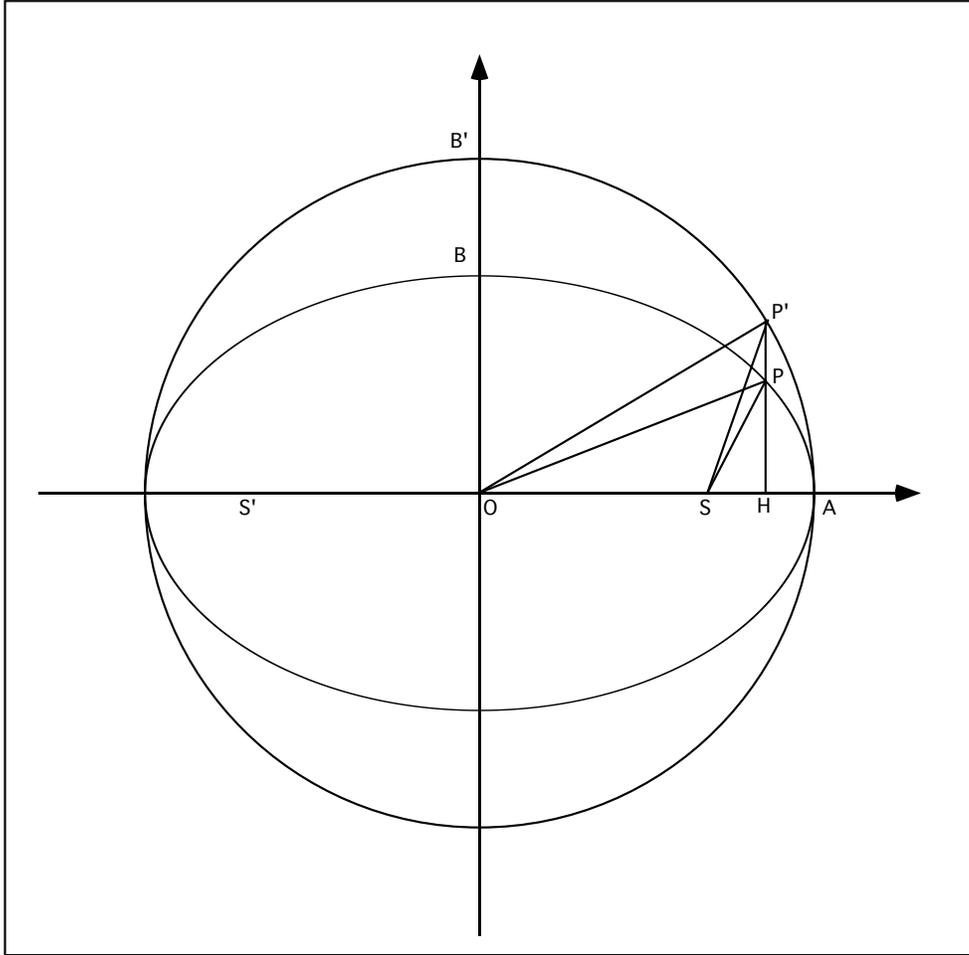


FIGURE 5. Orbite Képlérienne

$$\mathcal{S}(SAP') = \frac{a^2 u}{2} - \frac{c \cdot HP'}{2}$$

$$HP' = OP' \sin u = a \sin u$$

$$\mathcal{S}(SAP') = \frac{a^2 u}{2} - \frac{c a \sin u}{2}$$

$$\mathcal{S}(SAP) = \frac{b}{a} \mathcal{S}(SAP') = \frac{b a u}{2} - \frac{b c \sin u}{2}$$

$$\mathcal{S}(SAP) = \frac{b}{2}(a u - c \sin u) = \frac{b}{2}(a u - a e \sin u) = \frac{a b}{2}(u - e \sin u) = k t$$

Soit s la surface de l'ellipse :

$$s = \pi a b \quad \Rightarrow \quad a b = \frac{s}{\pi}$$

$$\frac{a b}{2}(u - e \sin u) = k t = \frac{s}{2 \pi}(u - e \sin u)$$

$$u - e \sin u = \frac{2 \pi k}{s} t$$

Soit $T = \frac{s}{k}$ et $M = \frac{2\pi}{T}$

Il vient enfin :

$$u - e \sin u = M t$$

C'est l'équation de Kepler. M est le *moyen mouvement*. C'est la vitesse qu'aurait une planète de même période circulant d'un mouvement uniforme sur le cercle circonscrit à l'ellipse. Pour connaître la position d'une planète à l'instant t , il faut tout d'abord résoudre l'équation de Kepler.

Algèbre

L'algèbre est une invention arabe, comme son nom l'indique. L'algèbre est une abstraction de la représentation des nombres, et de leurs relations. Le formalisme concis que nous utilisons aujourd'hui est assez récent. Ce n'est pas un luxe pédant, il permet une excellente visualisation.

Résolution de l'équation de Kepler

$$u - e \sin u = M$$

On utilise une méthode d'approximations successives. Si u était petit, on aurait $\sin u \approx u$ et donc on utilise cette approximation :

$$u - eu = M \Rightarrow u(1 - e) = M \quad \text{et} \quad u_0 = \frac{M}{1-e}.$$

On utilise cette valeur pour calculer une meilleure approximation, en remplaçant $\sin u$ par $\sin u_0$: $u_1 = e \sin u_0 + M$. Et plus généralement, on calcule la suite $u_n = e \sin u_{n-1} + M$ jusqu'à ce que $|u_n - u_{n-1}| < \epsilon$. La dernière valeur calculée de u est la solution de l'équation de Kepler à ϵ près. C'est une méthode de point fixe, car on a trouvé une valeur telle que $u = f(u)$ avec $f(u) = e \sin u + M$. C'est la méthode de la tangente de Newton qui a été utilisée. Son application directe permet de montrer la convergence de la suite.

CHAPITRE 6

L'ART D'ARRONDIR LES ANGLES

6.1. Position du problème

On se propose de trouver le moyen d'arrondir un angle. Une fois données les équations des deux côtés de l'angle, il s'agit de trouver une fonction de raccordement suffisamment régulière, autrement dit au moins de classe C^1 , c'est à dire dérivable, et à dérivée continue. Voir figure 1.

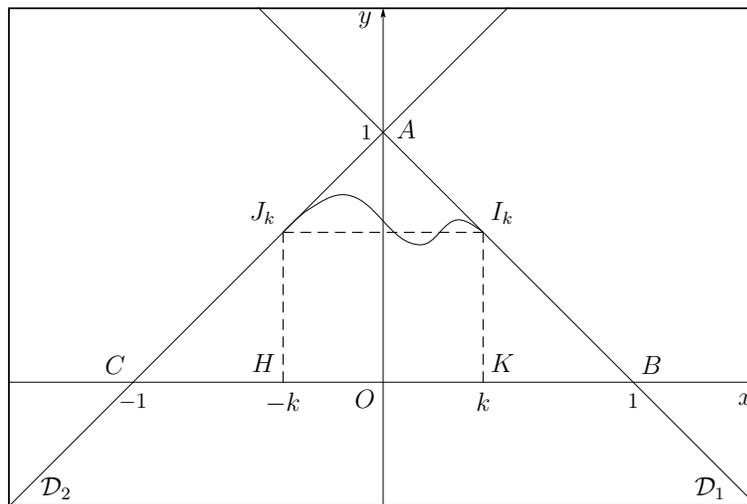


FIGURE 1. Schéma de départ

6.2. Première approche

Pour simplifier le problème, dans un premier temps, nous allons supposer :

- que l'angle en A est celui des droites :
 - (\mathcal{D}_1) passant par les points A et B de coordonnées respectives $(0, 1)$ et $(1, 0)$ dans le repère $\mathcal{R} = (0, x, y)$ orthonormé, d'équation $y = 1 - x$
 - (\mathcal{D}_2) passant par les points A et C , où C est le point de coordonnées $(-1, 0)$ dans le même repère, et d'équation $y = 1 + x$
- que le "raccord" se fait de façon dérivable aux points $I_k : (-k, 1 - k)$ de \mathcal{D}_2 et $J_k : (k, 1 - k)$ de \mathcal{D}_1 , où $k \in]0, 1[$
- que la restriction de f à l'intervalle $[-k, k]$ est une fonction polynomiale de degré 2.

Voir figure 2.

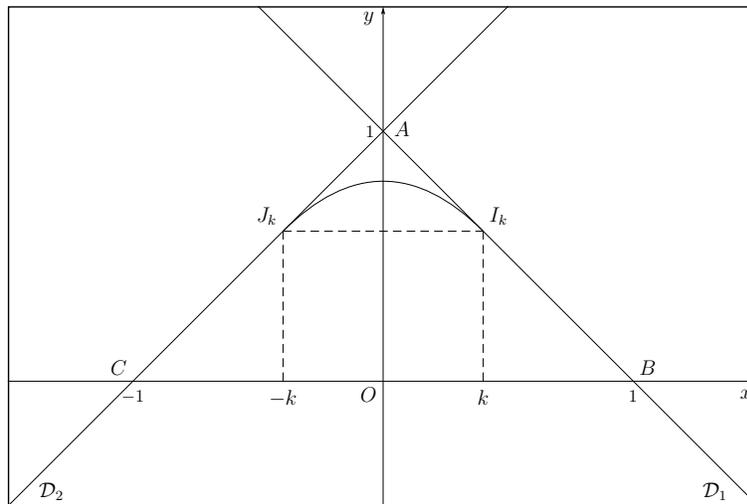


FIGURE 2. Raccord parabolique

6.2.1. Détermination du raccord parabolique. — On écrit le système des contraintes imposées :

- Les contraintes dues à la forme de f :
 - Il existe $(\alpha, \beta, \gamma) \in \mathbb{R}^3 / \forall x \in [-k, k], f(x) = \alpha x^2 + \beta x + \gamma$

- $\forall x \in [-1, -k], f(x) = x + 1$
- $\forall x \in [-k, k], f'(x) = 2\alpha x + \beta$
- $\forall x \in [k, 1], f(x) = -x + 1$
- Les contraintes dûes au raccordement :
 - En $I_k : f(k) = 1 - k$, et $f'(k) = -1$, d'où le système :

$$\alpha k^2 + \beta k + \gamma = 1 - k$$

$$2\alpha k + \beta = -1$$

- En $J_k : f(-k) = 1 - k$, et $f'(-k) = 1$, d'où le système :

$$\alpha k^2 - \beta k + \gamma = 1 - k$$

$$-2\alpha k + \beta = 1$$

On obtient ainsi :

$$\beta = 0$$

$$\alpha = -\frac{1}{2k}$$

$$\gamma = 1 - k - \alpha k^2 = 1 - \frac{k}{2}$$

Notons que $\beta = 0$ était prévisible vu la symétrie de la figure.

Conclusion : Dans cette première approche, la solution f est donnée par les expressions :

$$f(x) = x + 1, \quad \text{si } x \in [-1, -k]$$

$$f(x) = -\frac{1}{2k}x^2 + 1 - \frac{k}{2}, \quad \text{si } x \in [-k, k]$$

$$f(x) = -x + 1, \quad \text{si } x \in [k, 1]$$

6.2.2. Une autre idée. — Plutôt que de raisonner sur f , raisonnons plutôt sur f' . Avec les mêmes notations, les contraintes sur f' sont :

- $\forall x \in [-1, -k], f'(x) = 1$
- $\forall x \in [-k, k], f'(x) = 2\alpha x + \beta$
- $\forall x \in [k, 1], f'(x) = -1$

La continuité de f' en k et en $-k$ donne : $2\alpha k + \beta = -1$, et $-2\alpha k + \beta = 1$. On retrouve donc les mêmes valeurs $\alpha = -\frac{1}{2k}$ et $\beta = 0$ que précédemment.

Voir figure 3.

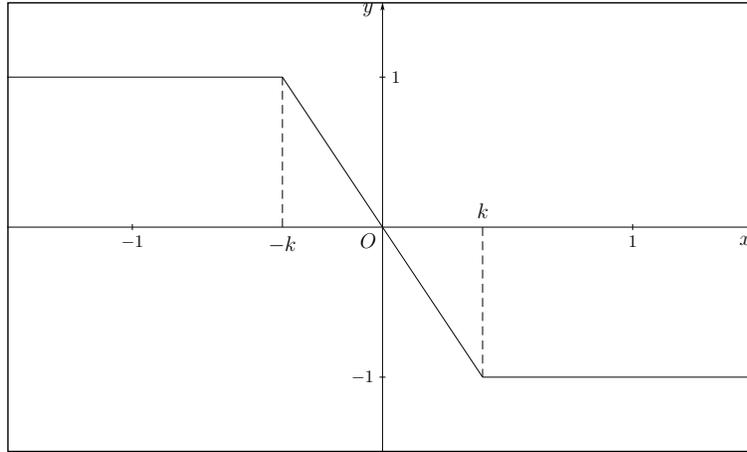


FIGURE 3. Représentation graphique de f'

En intégrant ces relations, puisque f' est continue, et en utilisant l'expression de f sur $[-1, -k]$ et sur $[k, 1]$, on obtient : $\forall x \in [-1, 1]$, $f(x) = \int_{-1}^x f(t)dt$, puisque finalement f est la primitive de f' qui s'annule en -1 . Voir figure 3.

On obtient donc :

$$\begin{aligned} \forall x \in [-1, -k], \quad f(x) &= x + 1 \\ \forall x \in [-k, k], \quad f(x) &= \int_{-1}^x f'(t)dt \\ &= \int_{-1}^{-k} f'(t)dt + \int_{-k}^x f'(t)dt \\ &= f(-k) + [\alpha x^2 + \beta x]_{-k}^x \\ &= 1 - k - \frac{1}{2k}(x^2) + \frac{k^2}{2k} \\ \forall x \in [k, 1], \quad f(x) &= 1 - x \end{aligned}$$

Finalement, on retrouve :

$$\begin{aligned} f(x) &= x + 1, & \text{si } x \in [-1, -k] \\ f(x) &= -\frac{1}{2k}x^2 + 1 - \frac{k}{2}, & \text{si } x \in [-k, k] \\ f(x) &= -x + 1, & \text{si } x \in [k, 1] \end{aligned}$$

Il est immédiat de vérifier que f est bien de classe C^1 (voir figure 3.)

6.2.3. Calcul de l'aire "perdue" lors du raccord parabolique.

— Cette aire \mathcal{A} , quadrillée dans la figure 4, est donnée par :

$$\begin{aligned} \mathcal{A} &= 2 \int_0^k (1 - x - f(x)) dx \\ &= 2 \int_0^k \left(1 - x - 1 + \frac{k}{2} + \frac{1}{2k}x^2 \right) dx \\ &= 2 \left(-\frac{k^2}{2} + \frac{k^2}{2} + \frac{k^2}{6} \right) \\ &= \frac{k^2}{3} \end{aligned}$$

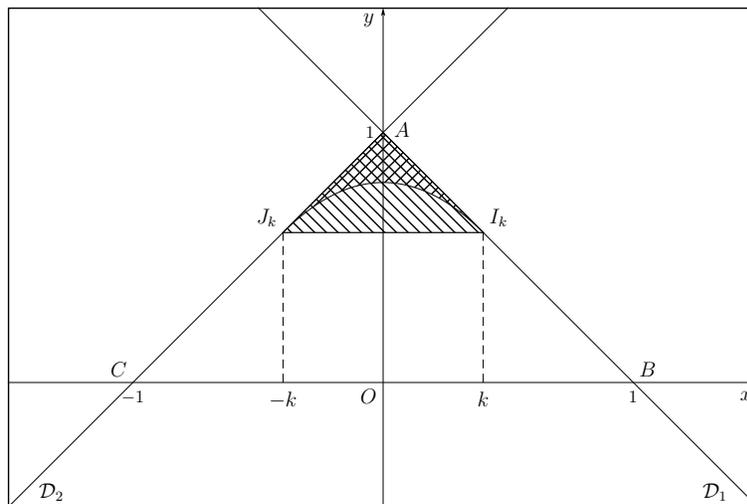


FIGURE 4. Aire perdue dans le cas du raccord parabolique

On peut remarquer que cette aire est aussi égale au tiers de l'aire AI_kJ_k . En effet, cette dernière vaut :

$$\mathcal{A}' = k(1 - (1 - k)) = k^2.$$

C'est une propriété générale des paraboles :

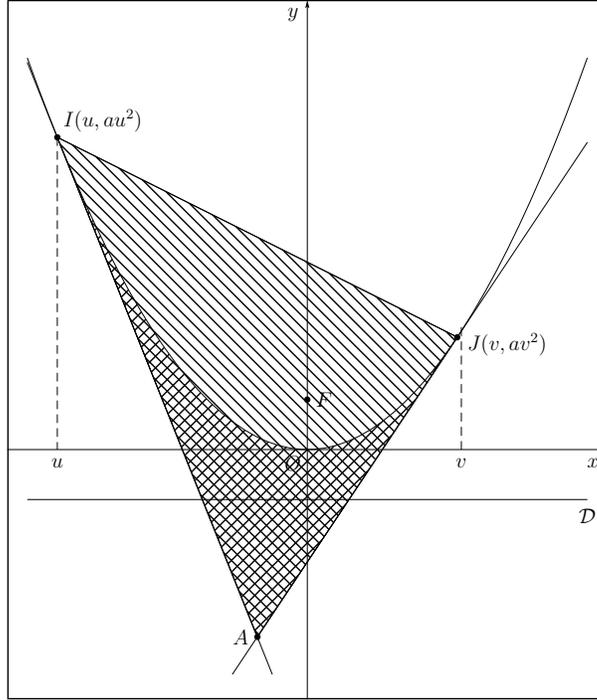


FIGURE 5. Propriété géométrique de la parabole

I et J étant deux points situés sur une parabole \mathcal{P} , les tangentes en I et en J à \mathcal{P} se coupent en A . Alors, le triangle AIJ a une aire triple de celle de la partie du triangle située “hors” de la parabole.

La démonstration analytique de ce résultat ne pose pas de problème.

On se place dans un repère orthonormé $(0, x, y)$ dans lequel la parabole a pour équation $y = ax^2$ avec $a > 0$, ce qui est toujours possible.

Voir figure 5.

6.2.4. Généralisation. — On peut faire une étude plus générale en translatant la figure, en modifiant la hauteur du triangle, en conservant

l'axe de symétrie du problème, et en gardant pour l'arrondi un polynôme de degré 2. La propriété relative à l'aire est conservée. Voir figure 6.

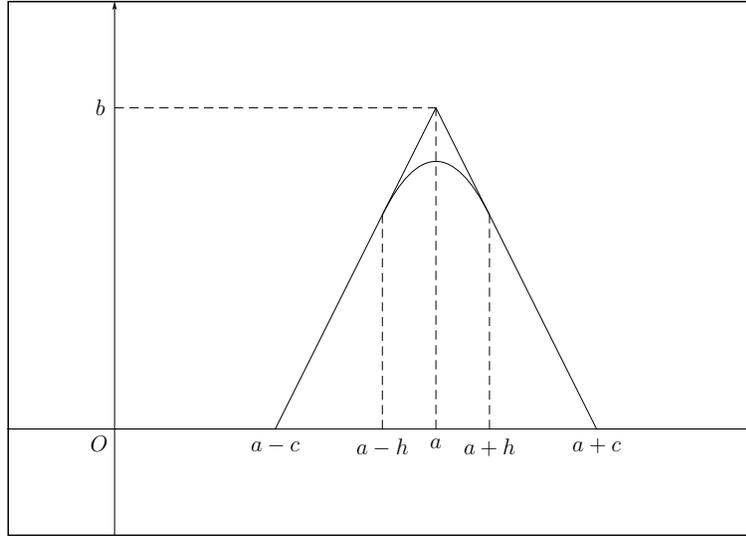


FIGURE 6. Généralisation

6.3. Raccord circulaire

6.3.1. Détermination du raccord circulaire. — On se propose ici résoudre le même type de problème, mais cette fois-ci avec un raccord circulaire, avec par ailleurs les mêmes notations.

La partie de la courbe représentative de f correspondant à l'intervalle $[-k, k]$ est donc une partie de cercle.

Voir figure 7.

On obtient facilement le centre $\Omega : (a, b)_{\mathcal{R}}$ du cercle en exprimant que le vecteur $\overrightarrow{\Omega I_k}$ (resp. $\overrightarrow{\Omega J_k}$) est orthogonal à \mathcal{D}_1 (resp. \mathcal{D}_2).

On obtient ainsi les équations :

$$(-k - a) + (1 - k - b) = 0$$

$$(k - a) - (1 - k - b) = 0$$

D'où : $a = 0$ et $b = 1 - 2k$

Comme on pouvait s'y attendre, le point Ω est sur l'axe Oy .

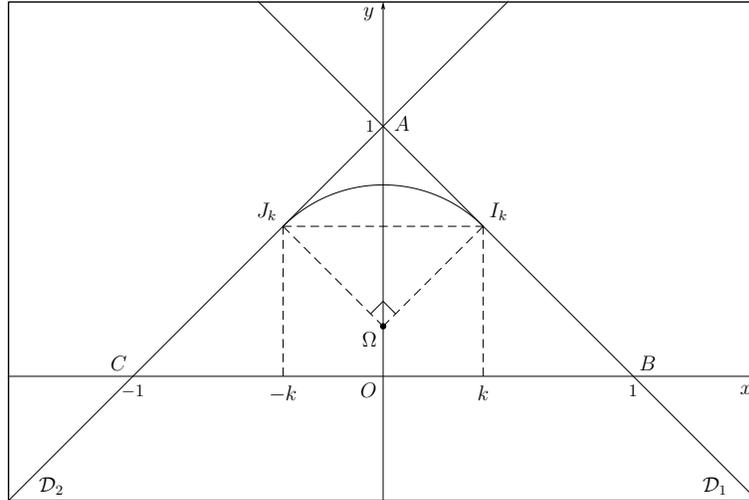


FIGURE 7. Raccord circulaire

Le cercle a pour rayon $\rho = k\sqrt{2}$

On peut aussi calculer l'expression de $f(x)$ dans $[-k, k]$:

$f(x) = 1 - 2k + \sqrt{2k^2 - x^2}$, mais celle-ci n'est pas indispensable pour le calcul qui suit.

Là encore, on peut vérifier que f est de classe C^1 .

6.3.2. Calcul de l'aire "perdue" lors du raccord circulaire. —

L'aire en question est égale à :

$$2 \int_0^k \left(1 - x - (1 - 2k + \sqrt{2k^2 - x^2}) \right) dx.$$

Ce calcul d'intégrale ne pose aucun problème, grâce au changement de variable $x = k\sqrt{2}\sin\theta$, mais il est beaucoup plus simple et rapide de raisonner géométriquement :

L'aire "perdue" est l'aire du carré $AI_k\Omega J_k$ (c'est bien un carré car tous les côtés sont égaux à $k\sqrt{2}$, vérification facile puisqu'on a les coordonnées de tous les points), moins l'aire \mathcal{A}' du secteur angulaire $\Omega I_k J_k$.

Cette dernière vaut : $\mathcal{A}' = \frac{\theta\rho^2}{2}$, avec $\theta = \frac{\pi}{2}$, et $\rho = k\sqrt{2}$ soit :

$$\mathcal{A}' = \frac{\pi k^2}{2}.$$

Finalement, $\mathcal{A} = 2k^2 - \frac{\pi k^2}{2} = \left(2 - \frac{\pi}{2}\right) k^2$

6.4. Troisième type de raccord : spline cubique

6.4.1. Détermination du raccord par spline cubique. — Maintenant, outre les raccordements dérivables en I_k et J_k , nous allons supposer :

- que la restriction de f à l'intervalle $[0, k]$ est une fonction polynomiale de degré 3.
- que f est paire
- que f prend la même valeur en zéro que dans le cas du raccord circulaire, soit : $1 - 2k + k\sqrt{2}$
- que f a une dérivée nulle en 0

Voir figure 8.

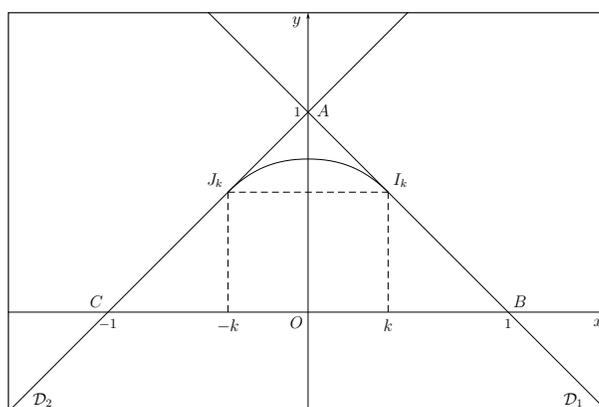


FIGURE 8. Raccord par spline cubique

On écrit les différentes contraintes imposées :

- Les contraintes dûes à la forme de f :
 - Il existe $(u, v, w, t) \in \mathbb{R}^4 / \forall x \in [0, k], f(x) = ux^3 + vx^2 + wx + t$
 - $\forall x \in [0, k], f'(x) = 3ux^2 + 2vx + w$
 - $\forall x \in [k, 1], f(x) = -x + 1$
 - $f(0) = t = 1 - 2k + k\sqrt{2}$
 - $f'(0) = w = 0$
- Les contraintes dûes au raccordement :
 - En I_k : $f(k) = 1 - k$, et $f'(k) = -1$, d'où les équations :

$$uk^3 + vk^2 + t = 1 - k$$

$$3uk^2 + 2vk = -1$$

On obtient ainsi :

$$\begin{aligned} t &= 1 - 2k + k\sqrt{2} \\ u &= \frac{-2 + k + 2t}{k^3} = \frac{2\sqrt{2} - 3}{k^2} \\ v &= \frac{3 - 2k - 3t}{k^2} = \frac{4 - 3\sqrt{2}}{k} = \sqrt{2}ku \end{aligned}$$

Conclusion : Ici, la solution f est donnée par les expressions :

$$\begin{aligned} f(x) &= x + 1, & \text{si } x \in [-1, -k], \\ f(x) &= \frac{2\sqrt{2} - 3}{k^2}x^3 + \frac{4 - 3\sqrt{2}}{k}x^2 + 1 - 2k + k\sqrt{2}, & \text{si } x \in [0, k], \\ f(x) &= -\frac{2\sqrt{2} - 3}{k^2}x^3 + \frac{4 - 3\sqrt{2}}{k}x^2 + 1 - 2k + k\sqrt{2}, & \text{si } x \in [-k, 0], \\ f(x) &= -x + 1, & \text{si } x \in [k, 1]. \end{aligned}$$

Et f est bien de classe C^1 .

6.4.2. Calcul de l'aire "perdue". — Cette aire \mathcal{A} est donnée par :

$$\begin{aligned} \mathcal{A} &= 2 \int_0^k (1 - x - f(x)) dx \\ &= 2 \int_0^k (1 - x - ux^3 - vx^2 - t) dx \\ &= 2k(1 - t) - k^2 - \frac{2uk^4}{4} - \frac{2vk^3}{3} \\ &= \left(\frac{11}{6} - \sqrt{2} \right) k^2 \end{aligned}$$

6.5. Comparaison des aires perdues (raccord parabolique , circulaire et spline cubique)

Si l'on reprend les trois résultats, on constate que dans le cas du raccord parabolique, l'aire "perdue" est égale à $k^2/3$, que pour le raccord circulaire, elle est égale à $(2 - \pi/2)k^2$, enfin que pour le raccord par spline cubique, elle vaut $(\frac{11}{6} - \sqrt{2})k^2$

Or, $(2 - \pi/2)$ a pour valeur approchée 0.429 à 0.001 près, tandis que $\frac{11}{6} - \sqrt{2}$ a pour valeur approchée 0.419 à 0.001 près.

L'aire "perdue" est donc supérieure, lors du raccord circulaire, à celle perdue lors du raccord par spline cubique, elle-même supérieure à celle perdue lors du raccord parabolique.

6.6. Comparaison des énergies de flexion

Dans la suite, nous allons essayer de comparer les énergies de flexion obtenues dans les trois cas de raccord envisagés : parabolique, circulaire, et par spline cubique.

La formule théorique de l'énergie de flexion avec les notations de la première partie est :

$$E = \int_{-k}^k \left(\frac{1}{R^2} ds \right) = 2 \int_0^k \left(\frac{(f'')^2}{(1 + f'^2)^{5/2}} \right),$$

R étant le rayon de courbure et s l'abscisse curviligne.

Rappelons que dans les trois cas envisagés, f est paire.

Toujours avec les mêmes notations que précédemment, on obtient :

$$E_c = \frac{\pi\sqrt{2}}{4k}$$

dans le cas du raccord circulaire,

$$E_p = \frac{5\sqrt{2}}{6k}$$

pour le cas parabolique,

et enfin,

$$E_s = 2 \int_0^k \left(\frac{(6ux + 2v)^2}{(1 + (3ux^2 + 2vx)^2)^{5/2}} \right)$$

pour la spline.

Pour pouvoir comparer les résultats des trois raccords, il nous faut rendre les hypothèses plus homogènes ; D'autre part, le calcul de E_s étant compliqué, nous allons nous placer dans un cas où nous pourrions légitimement négliger f'^2 devant 1, ce qui n'était pas possible jusqu'alors, puisque f' variait de 0 à -1 . Ensuite, nous ferons tendre X vers $+\infty$, ce qui nous permettra d'avoir des équivalents des différentes énergies.

Ces changements sont illustrés sur la figure 9.

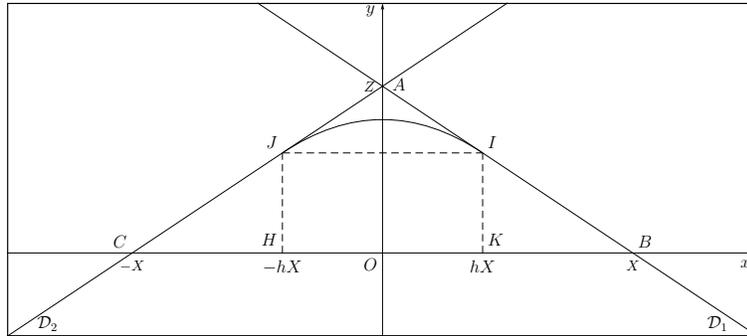


FIGURE 9. Nouvelles notations. Schéma de départ.

6.7. Les notations

Les points initiaux ($0 < h < 1$, $X > 0$, $Z > 0$) :

$$A = (0, Z) \quad B = (X, 0) \quad C = (-X, 0)$$

$$H = (-hX, 0) \quad K = (hX, 0)$$

Les droites initiales :

$$(A, B) : \quad y = -\frac{Z}{X}x + Z$$

$$(A, C) : \quad y = \frac{Z}{X}x + Z$$

Suite de constructions :

$$\text{points : } J = (-hX, Z(1-h)) \quad I = (hX, Z(1-h))$$

6.8. Raccord tangent par arc de cercle aux points I et J

6.8.1. Les éléments de base. — Nous appellerons Ω le centre du cercle, ρ son rayon et S l'intersection de l'arc de cercle avec l'axe des ordonnées.

$$\text{droite : } (J, \Omega) : y = -\frac{X}{Z}x + Z(1-h) - \frac{hX^2}{Z}$$

$$\text{point : } \Omega = \left(0, Z(1-h) - \frac{hX^2}{Z}\right)$$

$$\rho = \frac{hX^2}{Z} \sqrt{1 + \frac{Z^2}{X^2}}$$

$$\text{point : } S = \left(0, Z(1-h) - \frac{hX^2}{Z} + \frac{hX^2}{Z} \sqrt{1 + \frac{Z^2}{X^2}}\right)$$

6.8.2. La flexion. —*6.8.2.1. Calcul exact.* —

$$E_c = \int_{\widehat{(J,I)}} \frac{ds}{\rho^2}$$

Posons $\theta_1 = \text{Arctan}(Z/X)$

$$E_c = 2 \int_0^{\theta_1} \frac{d\theta}{\rho} = \frac{2Z}{hX^2 \sqrt{1 + \frac{Z^2}{X^2}}} \text{Arctan} \left(\frac{Z}{X} \right)$$

Cherchons un équivalent de E_c lorsque $X \rightarrow \infty$:

$$E_c \sim \frac{2Z^2}{hX^3}$$

On a aussi

$$E_c = \frac{2Z^2}{hX^3} - \frac{5Z^4}{3hX^5} + \frac{89Z^6}{60hX^7} + o\left(\frac{1}{X^7}\right)$$

6.8.2.2. *Calcul avec la formule approchée.* — On part de l'équation de la courbe entre $-hX$ et hX

$$y = y_\Omega + (\rho^2 - x^2)^{1/2}$$

et on calcule successivement

$$y' = -x(\rho^2 - x^2)^{-1/2}$$

$$y'' = -\rho^2(\rho^2 - x^2)^{-3/2}$$

$$(y'')^2 = \rho^{-2} \left(1 - \frac{x^2}{\rho^2}\right)^{-3}$$

et donc

$$E'_c = 2\rho^{-2} \int_0^{hX} \left(1 - \frac{x^2}{\rho^2}\right)^{-3} dx$$

ou encore en posant $u = x/\rho$

$$E'_c = \frac{2Z}{hX^2} \left(1 + \frac{Z^2}{X^2}\right)^{-1/2} \int_0^\beta (1 - u^2)^{-3} du$$

où

$$\beta = \frac{Z}{X} \left(1 + \frac{Z^2}{X^2}\right)^{-1/2}$$

On trouve

$$E'_c = \frac{2Z}{hX^2} \left(1 + \frac{Z^2}{X^2}\right)^{-1/2} \left[\frac{3}{16} \ln \left(\frac{1 + \beta}{1 - \beta}\right) + \frac{5\beta - 3\beta^3}{8(1 - u^2)^2} \right]$$

On a donc, lorsque X tend vers $+\infty$,

$$E'_c \sim \frac{2Z^2}{hX^3}$$

et aussi le développement limité :

$$E'_c = \frac{2Z^2}{hX^3} + \frac{2Z^6}{5hX^7} + o\left(\frac{1}{X^7}\right)$$

On peut refaire ce calcul d'une autre façon. Si on appelle M le point courant de l'arc de cercle impliqué, on introduit θ , l'angle de ΩM avec l'axe des ordonnées. Ainsi :

$$\begin{aligned} x &= \rho \sin(\theta) & y &= y_\Omega + \rho \cos(\theta) \\ dx &= \rho \cos(\theta) d\theta & y &= -\rho \sin(\theta) d\theta \end{aligned}$$

$$\begin{aligned}\frac{dy}{dx} &= -\tan(\theta) \\ \frac{d^2y}{dx d\theta} &= -\frac{1}{\cos^2(\theta)} \\ \frac{d^2y}{dx^2} &= -\frac{1}{\rho \cos^3(\theta)}\end{aligned}$$

d'où

$$E'_c = \frac{2}{\rho} \int_0^{\text{Arctan}(\frac{Z}{X})} \frac{d\theta}{\cos^5(\theta)}$$

Le calcul est difficile à partir de cette formule, mais en revanche on obtient aisément un développement limité. On retombe bien entendu sur le résultat précédent (ouf!).

6.9. Raccord tangent par arc de parabole aux points I et J

6.9.1. Les éléments de base. — Sur l'intervalle $[-hX, hX]$ l'équation de l'arc de parabole est

$$y = \left(-\frac{Z}{2hX^2}\right)x^2 + Z\left(1 - \frac{h}{2}\right)$$

Soit S_1 le sommet de la parabole

$$\begin{aligned}S_1 &= \left(0, Z\left(1 - \frac{h}{2}\right)\right) \\ y' &= -\frac{Z}{hX^2}x \quad y'' = -\frac{Z}{hX^2}\end{aligned}$$

6.9.2. Flexion. —

6.9.2.1. Calcul exact. —

$$E_p = \frac{2Z^2}{3hX^3} \left(\frac{\frac{2Z^2}{X^2} + 3}{\left(1 + \frac{Z^2}{X^2}\right)^2} \right) \sqrt{1 + \frac{Z^2}{X^2}}$$

ou encore

$$E_p = \frac{2Z^2}{3hX^3} \left(\frac{3 + 2\left(\frac{Z}{X}\right)^2}{\left(1 + \left(\frac{Z}{X}\right)^2\right)^{3/2}} \right)$$

D'où

$$E_p \sim \frac{2Z^2}{hX^3}$$

et donc $E_p \sim E_c$. On a aussi

$$E_p = \frac{2Z^2}{hX^3} - \frac{5Z^4}{3hX^5} + \frac{21Z^6}{12hX^7} + o\left(\frac{1}{X^7}\right)$$

6.9.2.2. *Calcul avec la formule approchée.* —

$$E'_p = \int_{-hX}^{hX} (y''(t))^2 dt$$

$$E'_p = \frac{2Z^2}{hX^3}$$

6.10. Raccord par une spline cubique

6.10.1. Les éléments de base. — On va prendre pour raccord l'arc de cubique qui sur $[0, hX]$ vérifie : (la courbe passe par S et J a une tangente horizontale en S et une tangente de pente $-Z/X$ en I)

$$f(0) = Z(1-h) - h\frac{X^2}{Z} + hX\sqrt{1 + \frac{X^2}{Z^2}}, \quad f(hX) = Z(1-h)$$

$$f'(0) = 0, \quad f'(hX) = -\frac{Z}{X}$$

On a sur $[0, hX]$

$$f(x) = ax^3 + bx^2 + d$$

avec

$$d = Z(1-h) - h\frac{X^2}{Z} + hX\sqrt{1 + \frac{X^2}{Z^2}}$$

ou encore :

$$d = Z(1-h) - h\frac{X^2}{Z} + \frac{hX^2}{Z}\sqrt{1 + \frac{Z^2}{X^2}}$$

$$a = \frac{1}{h^2} \left(-\frac{2}{XZ} - \frac{Z}{X^3} + \frac{2}{XZ}\sqrt{1 + \frac{Z^2}{X^2}} \right)$$

$$b = \frac{1}{h} \left(\frac{3}{Z} + \frac{Z}{X^2} - \frac{3}{Z}\sqrt{1 + \frac{Z^2}{X^2}} \right)$$

Remarquons que sur $[-hX, 0]$ l'arc de cubique correspondant est donné par l'équation

$$y = -ax^3 + bx^2 + d$$

6.10.2. Flexion. —

6.10.2.1. *Calcul exact.* — Ici le calcul avec la formule complète est inextricable.

6.10.2.2. *Calcul avec la formule approchée.* —

$$E'_s = 8(3a^2h^3X^3 + 3abh^2X^2 + b^2hX)$$

dont on va chercher un équivalent lorsque $X \rightarrow +\infty$. On a :

$$a \sim -\frac{Z^3}{4h^2X^5}$$

$$b \sim -\frac{Z}{2hX^2}$$

Donc a^2X^3 est en $1/X^7$, abX^2 est en $1/X^5$ et b^2X est en $1/X^3$. Le terme principal est $8b^2hX$, c'est-à-dire

$$8hX \frac{Z^2}{4h^2X^4}$$

ce qui donne

$$E'_s \sim \frac{2Z^2}{hX^3}$$

et on trouve encore le même résultat. On peut aussi donner un développement limité

$$E'_s = \frac{2Z^2}{hX^3} + \frac{3Z^6}{8hX^7}$$

6.11. Conclusion

Les trois énergies de flexion sont équivalentes lorsque Z et h restent fixes et $X \rightarrow +\infty$.

On sait de manière théorique que si on prend la formule simplifiée (donc si on calcule E'_c, E'_p, E'_s et non E_c, E_p, E_s) alors

$$E'_p \leq E'_s \leq E'_c.$$

Notons (c) le cercle (p) la parabole et (s) la spline constituée de 2 arcs de cubiques, passant par aussi par S . Commençons à regarder le cas des contraintes : raccord dérivable en I et J et courbe de classe C^2 que réalisent les 3 courbes. On sait que le minimum de E' est atteint pour la spline cubique en un seul arc de cubique. Mais ici cette cubique est dégénérée en la conique (p) . Rajoutons maintenant une contrainte supplémentaire, passer par le point S en plus de I et J , contrainte qui n'est pas réalisée par (p) . On impose toujours bien sûr à la courbe d'être globalement C^2 sur l'intervalle $[-hX, hX]$ (pas sur tout \mathbb{R}). On sait que le minimum sous ces contraintes est atteint par la spline en deux arcs de cubiques (s) .

Quant-à-classer E_c, E_p, E_s c'est une autre affaire ! Peut-être peut-on classer facilement E_c et E_p , pour l'autre c'est moins clair mais on peut essayer.

CHAPITRE 7

ERRARE HUMANUM EST

7.1. Présentation du problème

Dans de nombreuses circonstances nous sommes amenés à attribuer des numéros à des objets, des produits, des comptes, des services de la vie courante : numéros de sécurité sociale, numéros de compte bancaire, numéros de cartes de paiement, numéros de billets de banque, code des produits de consommation, etc. Ces numéros doivent parfois être retranscrits manuellement, transmis par téléphone ou lus par des lecteurs. Lors de ces transcriptions des erreurs peuvent être commises. Un premier problème est de détecter ces erreurs éventuelles. Bien entendu il existe des moyens performants, les **codes correcteurs d'erreurs**, qui non seulement détectent les erreurs de transmission, mais aussi arrivent à corriger la plupart d'entre elles. Cependant ces méthodes performantes demandent des allongements importants des messages à transmettre et sont peu adaptés aux numéros courants utilisés par le public. Nous nous focalisons donc ici sur des méthodes simples à mettre en œuvre, et qui de ce fait se limitent à la détection des erreurs commises lors d'une opération de recopie. C'est ce qu'on appelle des **codes détecteurs d'erreurs**. Ces méthodes consistent en général à rajouter au numéro, une clé calculée astucieusement en fonction du numéro. Quelques uns de ces codes détecteurs sont décrits dans [idMgl99], [Rol01] et [Rol02]. Nous nous intéresserons ici aux codes qui n'utilisent que les chiffres $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, et qui n'utilisent qu'un chiffre pour la clé. En outre, si les numéros (sans la clé) ont $n - 1$ chiffres, nous souhaitons pouvoir utiliser les 10^{n-1} numéros

possibles. Tout ceci élimine le cas des numéros de sécurité sociale et des numéros de comptes bancaires qui ont une clé constituée de deux chiffres. Cela élimine aussi le code ISBN, utilisé pour les livres, en raison d'une clé qui peut être, en plus des dix chiffres, le symbole X .

7.2. Les erreurs possibles

Si on analyse de plus près les erreurs commises il apparaît que certaines d'entre elles sont plus probables que d'autres. Nous distinguerons en particulier les types disjoints suivants.

- **Erreur unique**

Le mot :

$$a_0 a_1 \cdots a_i \cdots a_{n-1}$$

est transformé en :

$$a_0 a_1 \cdots b_i \cdots a_{n-1},$$

où $a_i \neq b_i$.

- **Transposition de chiffres consécutifs**

Le mot :

$$a_0 a_1 \cdots a_i a_{i+1} \cdots a_{n-1}$$

est transformé en :

$$a_0 a_1 \cdots a_{i+1} a_i \cdots a_{n-1},$$

où $a_i \neq a_{i+1}$.

On dispose en fait d'une classification des erreurs plus fine que celle donnée ici. Cependant l'étude des fréquences relatives des divers types d'erreurs fait apparaître une majorité importante pour ces deux types d'erreurs.

Type de l'erreur	Fréquence relative
Erreur unique	0.791
Transposition	0.102

Nous considérerons, bien que ce ne soit pas tout à fait le cas, que les autres erreurs sont totalement aléatoires et se comportent comme si on avait tiré au sort un nombre (y compris la clé) distinct du nombre original parmi les $10^n - 1$ possibilités restantes.

Remarque 7.2.1. — Le cumul d'une erreur de type *erreur unique* avec une transposition est classé dans les erreurs aléatoires et non pas dans les deux premiers types.

7.3. Comparons deux méthodes proches

7.3.1. Codes de type UPC (Universal Product Code) ou EAN (European Article Number). — Soit :

$$a_n a_{n-1} \cdots a_1 a_0$$

un mot de longueur $n + 1$, dont la clé est a_0 . On calcule a_0 de telle sorte que :

$$a_0 + 3a_1 + a_2 + 3a_3 + \cdots + a_{2k} + 3a_{2k+1} + \cdots \equiv 0 \quad (10).$$

a) Ce code détecte-t-il toutes les erreurs uniques? Sachant qu'une erreur de ce type s'est produite, quelle est la probabilité de la détecter?

b) Ce code détecte-t-il toutes les transpositions de chiffres consécutifs? Sachant qu'une erreur de ce type s'est produite, quelle est la probabilité de la détecter?

d) Lorsqu'une erreur qui n'est pas d'un des deux types précédents se produit on admettra que la probabilité de la détecter est 0.9. Comment peut-on justifier mathématiquement (approximativement) cette probabilité?

e) Quand une erreur se produit, quelle est la probabilité de la détecter?

7.3.2. Code IBM ou règle de Luhn. — Soit

$$a_n a_{n-1} \cdots a_1 a_0$$

un mot de longueur $n+1$, dont la clé est a_0 . Pour tout nombre a représenté par un seul chiffre, on définit

$$m(a) = \begin{cases} 2 * a \bmod 9 & \text{si } 0 \leq a < 9 \\ 9 & \text{si } a = 9. \end{cases}$$

On calcule a_0 de telle sorte que :

$$a_0 + m(a_1) + a_2 + m(a_3) + \cdots + a_{2k} + m(a_{2k+1}) + \cdots \equiv 0 \quad (10).$$

a) Ce code détecte-t-il toutes les erreurs uniques? Sachant qu'une erreur de ce type s'est produite, quelle est la probabilité de la détecter?

b) Ce code détecte-t-il toutes les transpositions de chiffres consécutifs? Sachant qu'une erreur de ce type s'est produite, quelle est la probabilité de la détecter?

d) Lorsqu'une erreur qui n'est pas d'un des deux types précédents se produit on admettra que la probabilité de la détecter est 0.9. Comment peut-on justifier mathématiquement (approximativement) cette probabilité?

e) Quand une erreur se produit, quelle est la probabilité de la détecter?

7.4. Est-ce possible?

Les deux exemples précédents, très utilisés en pratique, souffrent du même manque : ils ne détectent pas tous les cas de transposition de deux symboles consécutifs. Le problème est donc posé : existe-t-il un code détecteur tel que :

- les symboles utilisés sont $0, 1, \dots, 9$;
- le code est constitué d'un numéro ayant n symboles $a_1 a_2 \dots a_n$ et d'une clé $a_{n+1} = f(a_1, a_2, \dots, a_n)$ calculée en fonction du numéro ;
- les numéros admissibles sont les 10^n numéros possibles constitués avec les 10 symboles. Autrement dit la fonction f doit être définie sur $\{0 \dots 9\}^n$ et à valeurs dans $\{0 \dots 9\}$;
- le code détecte toute erreur unique ;
- le code détecte toute erreur de type transposition de deux symboles consécutifs, y compris si la clé est impliquée.

7.5. Commençons par $n = 2$

7.5.1. introduction d'une opération et d'un code associé. —

Dans ce cas le numéro est constitué de deux digits décimaux $x_1 x_2$ et la clé est calculée par une formule du type :

$$x_3 = f(x_1, x_2),$$

le tout donnant un mot de code valide $x_1x_2x_3$. Nous noterons C_1 ce code, c'est à dire l'ensemble des mots $x_1x_2x_3$ valides. Dans ce cas la fonction f peut être définie par un tableau F de taille 10×10 , qui contient dans la case située à la ligne i et à la colonne j la valeur $f(i, j)$. Ceci nous incite à écrire f sous forme d'opération, c'est-à-dire :

$$x_3 = f(x_1, x_2) = x_1 \star x_2.$$

On se rend compte que pour que ce code détecte toute erreur unique il faut et il suffit que :

- (1) les éléments d'une même ligne soient tous différents, autrement dit, chaque ligne donne une permutation de $\{0 \cdots 9\}$;
- (2) les éléments d'une même colonne soient tous différents, autrement dit, chaque colonne donne une permutation de $\{0 \cdots 9\}$.

On peut exprimer ceci en disant que :

Théorème 7.5.1. — *Le code C_1 construit précédemment détecte toute erreur unique si et seulement si le tableau T est un carré latin.*

Pour que ce code détecte une erreur de transposition de deux digits consécutifs il faut et il suffit que :

- (3) $i \star j \neq j \star i$ pour tout $i \neq j$; on dit dans ce cas que la loi \star est **anti-commutative** ou que le tableau T est anti-commutatif ;
- (4) si $i \star j = k$ alors $i \star k \neq j$ pour tout $j \neq k$.

En effet, si $x_1x_2x_3$ est un mot valide, on détecte grâce à (3) la transposition de x_1 avec x_2 pourvu bien sûr que $x_1 \neq x_2$. Grâce à (4) on détecte la transposition de x_2 avec x_3 quand $x_2 \neq x_3$. On peut ainsi énoncer :

Théorème 7.5.2. — *Le code C_1 construit précédemment détecte toute erreur unique et toute erreur de transposition de deux digits consécutifs si et seulement si le tableau T est un carré latin anti-commutatif qui vérifie la condition (4).*

7.5.2. Un autre code associé à la même opération. — Nous supposons maintenant que le tableau T définissant l'opération \star est un carré latin. De ce fait pour tout $x \in \{0, \dots, 9\}$ il existe un unique $y \in \{0, \dots, 9\}$ tel que :

$$x \star y = 0.$$

En conséquence l'équation :

$$(u_1 \star u_2) \star u_3 = 0,$$

définit une clé :

$$(6) \quad u_3 = g(u_1, u_2)$$

Remarquons que puisqu'on a défini $f(u_1, u_2) = u_1 \star u_2$, on a :

$$f(u_1, u_2) \star g(u_1, u_2) = 0.$$

Théorème 7.5.3. — *Soit \star une opération sur $\{0, \dots, 9\}$ dont la table T est un carré latin. Le code C définit par (6) détecte toute erreur de transposition de deux digits consécutifs si et seulement si T est anti-commutatif et :*

(4') *si $(i \star j) \star k = 0$ alors $(i \star k) \star j \neq 0$ pour tout $j \neq k$.*

Remarquons que la condition (4) n'est pas équivalente à la condition (4') et donc les deux codes associées à l'opération \star définies par f et g n'ont pas nécessairement les mêmes propriétés.

7.5.3. Essai avec des opérations issues de $\mathbb{Z}/10\mathbb{Z}$. — Dans cette section, toutes les opérations (addition, soustraction) sont faites dans $\mathbb{Z}/10\mathbb{Z}$, c'est-à-dire modulo 10. Nous n'écrivons pas le modulo. Essayons déjà de construire un carré latin anti-commutatif en définissant la clé x_3 à mettre dans la case située à la ligne x_1 et à la colonne x_2 par :

$$(7) \quad x_3 = \sigma_1(x_1) + \sigma_2(x_2),$$

où σ_1 et σ_2 sont des permutations de $\{0, \dots, 9\}$. Ceci est bien entendu une méthode simple pour définir certaines fonctions particulières f permettant un calcul de clé sous la forme $x_3 = f(x_1, x_2)$. On constate que les fonctions σ_1 et σ_2 étant bijectives le tableau ainsi construit est un carré latin, si bien que le code associé détecte toute erreur unique. Nous pouvons supposer sans perdre de généralité que σ_1 est l'identité, c'est-à-dire qu'on peut ne considérer que des fonctions définies par :

$$(8) \quad x_3 = x_1 + \sigma(x_2),$$

où σ est une permutation de $\{0, \dots, 9\}$ dans la mesure où nous avons :

Lemme 7.5.4. — *Il existe un carré latin anti-commutatif défini par une équation de type (7) si et seulement si il existe un carré latin anti-commutatif défini par une équation du type (8).*

Démonstration. — Comme une équation de type (8) est un cas particulier d'équation du type (7), il suffit de montrer que s'il existe un carré latin anti-commutatif défini par une équation (7), il existe un carré latin défini par une équation (8). Définissons un tableau en mettant dans la case qui se trouve à la ligne y_1 et à la colonne y_2 la clé y_3 définie par :

$$y_3 = y_1 + \sigma_2 (\sigma_1^{-1}(y_2)) .$$

Cette équation est bien du type (8) avec $\sigma = \sigma_2 (\sigma_1^{-1})$ qui est bien une permutation, ce qui donne bien un carré latin. Posons $x_1 = \sigma_1^{-1}(y_1)$ et $x_2 = \sigma_1^{-1}(y_2)$. Alors si $y_1 \neq y_2$, on a aussi $x_1 \neq x_2$ et :

$$y_2 + \sigma_2 (\sigma_1^{-1}(y_1)) = \sigma_1(x_2) + \sigma_2(x_1) \neq \sigma_1(x_1) + \sigma_2(x_2) = y_1 + \sigma_2 (\sigma_1^{-1}(y_2)) ,$$

ce qui prouve que le tableau est aussi anti-commutatif. \square

Lemme 7.5.5. — *Le carré latin T défini par (8) est anti-commutatif si et seulement si l'application $g(x) = x - \sigma(x)$ est une permutation de $\{0, \dots, 9\}$.*

Démonstration. — En effet, T est anti-commutatif si et seulement si pour tout $x_1 \neq x_2$ on a :

$$x_1 + \sigma(x_2) \neq x_2 + \sigma(x_1),$$

c'est-à-dire :

$$x_1 - \sigma(x_1) \neq x_2 - \sigma(x_2),$$

ou encore :

$$g(x_1) \neq g(x_2),$$

ce qui dans le cas d'une application d'un ensemble fini dans lui-même est équivalent à g bijective. \square

Lemme 7.5.6. — *Toute permutation σ de $\{0, \dots, 9\}$ vérifie :*

$$\sum_{i=0}^9 \sigma(i) \equiv 5 \quad (10).$$

Démonstration. — Puisque σ est une permutation :

$$\sum_{i=0}^9 \sigma(i) = \sum_{i=0}^9 i \equiv 5 \quad (10).$$

□

Théorème 7.5.7. — *Il n'existe aucun carré latin anti-commutatif construit grâce à une équation de type (7)*

Démonstration. — Il suffit de montrer qu'il n'y en a aucun construit grâce à une équation (8). Pour cela il suffit de constater que pour toute permutation σ on a :

$$\sum_{i=0}^9 (i - \sigma(i)) = \sum_{i=0}^9 i - \sum_{i=0}^9 \sigma(i) \equiv 0 \quad (10).$$

Donc $g(x) = x - \sigma(x)$ n'est pas une permutation. □

A fortiori, il n'exite pas de code construit de cette façon qui détecte toute erreur unique et toute transposition de deux digits consécutifs. Remarquons que les deux exemples que nous avons donnés (code EAN et loi de Luhn) sont de ce type.

7.5.4. Mais alors c'est possible! — Le seul espoir restant pour trouver un code répondant aux contraintes et qui détecte toute erreur unique et toute transposition de deux digits consécutifs réside dans le choix d'une bonne opération f plus compliquée que celles construites de la façon précédente. On ne va toutefois pas trop compliquer, on va choisir une méthode du type précédent, mais où l'addition modulo 10 sera remplacée par une autre loi de groupe, qui ne soit pas commutative (pour une loi commutative, les démonstrations précédentes s'appliquent).

7.5.4.1. Le groupe diédral d'ordre 10. — Considérons le groupe D_{10} des isométries qui laissent invariant un pentagone régulier. Supposons que les sommets du pentagone soient les points M_k d'affixe Z_k ($0 \leq k < 5$) :

$$Z_i = e^{\frac{2i\pi}{5}}.$$

Nous noterons \circ la loi de ce groupe, c'est-à-dire la composition des transformations. Ce groupe comporte les 5 rotations R_k ($0 \leq k < 5$), où R_k

est la rotation de centre O et d'angle $2k\pi/5$, ainsi que les 5 symétries S_k où S_k est la symétrie d'axe passant par O et par le sommet M_k . Ce groupe est le produit semi-direct :

$$D_{10} \simeq \mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}.$$

Plus précisément, notons R la rotation R_1 , si bien que pour $0 \leq k < 5$ on a $R_k = R^k$. Notons S la symétrie S_0 . Tout élément du groupe D_{10} s'écrit d'une façon et d'une seule sous la forme :

$$(9) \quad T = R^k \circ S^r,$$

où $0 \leq k < 5$ et $0 \leq r < 2$. Le groupe D_{10} est isomorphe au produit semi-direct $\mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ dont on notera l'opération grâce à l'application ϕ de $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ dans D_{10} définie par

$$\phi(k, r) = R^k \circ S^r.$$

Ainsi dans $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$:

$$(k_1, r_1) \cdot (k_2, r_2) = (k_1 + (-1)^{r_1} k_2, r_1 + r_2).$$

La somme et le produit utilisés dans le calcul $k_1 + (-1)^{r_1} k_2$ sont les opérations habituelles d'entiers modulo 5. Le groupe $\mathbb{Z}/2\mathbb{Z}$ agit sur $\mathbb{Z}/5\mathbb{Z}$ par produit par $(-1)^r$, où $r \in \mathbb{Z}/2\mathbb{Z}$, le résultat étant à prendre modulo 5.

Pour le groupe vu sous forme géométrique on a :

$$T_1 \circ T_2 = (R^{k_1} \circ S^{r_1}) \circ (R^{k_2} \circ S^{r_2}) = R^{k_1} \circ (S^{r_1} \circ R^{k_2} \circ S^{r_1}) \circ S^{r_1+r_2}.$$

Autrement dit :

$$T_1 \circ T_2 = \begin{cases} R^{k_1+k_2} \circ S^{r_2} & \text{si } r_1 = 0 \\ R^{k_1-k_2} \circ S^{1+r_2} & \text{si } r_1 = 1, \end{cases}$$

où les exposants de R sont à prendre modulo 5 et ceux de S modulo 2.

Numérotons alors de 0 à 9 les éléments du groupe D_{10} en attribuant à la transformation :

$$T = R^k \circ S^r$$

le numéro :

$$5r + k.$$

Si x est le numéro de T_1 et y le numéro de T_2 , nous ferons l'abus de notation consistant à écrire $x \circ y$ le numéro de la transformation composée $T_1 \circ T_2$.

7.5.5. Une bonne permutation. — Nous allons utiliser le même principe que dans le cas d'un groupe commutatif, c'est-à-dire que nous allons utiliser des fonctions f particulières pour calculer la clé :

$$(10) \quad x_3 = x_1 \circ \sigma(x_2),$$

où σ est une permutation de $\{0, \dots, 9\}$. Cette formule est tout à fait comparable à la formule (8). Tout en étant non-commutatif, le groupe diédral ne donne pas une loi anti-commutative, car les rotations commutent. Mais si on choisit bien la permutation σ la loi définie par (10) sera anti-commutative. Considérons la permutation σ définie par :

$$\sigma(x) = \begin{cases} 4 - x & \text{si } 0 \leq x \leq 4 \\ x & \text{si } 5 \leq x \leq 9. \end{cases}$$

Théorème 7.5.8. — *Pour tout x et tout y dans $\{0, \dots, 9\}$ tels que $x \neq y$ on a $x \circ \sigma(y) \neq y \circ \sigma(x)$.*

Démonstration. — Si $0 \leq x, y \leq 4$ avec $x \neq y$ alors :

$$x \circ \sigma(y) = x \circ (4 - y) = (x - 1 - y) \pmod{5}.$$

En revanche :

$$y \circ \sigma(x) = (y - 1 - x) \pmod{5}.$$

Donc :

$$x \circ \sigma(y) - y \circ \sigma(x) = 2(x - y) \pmod{5} \neq 0.$$

Si $0 \leq x \leq 4 < y \leq 9$ alors :

$$x \circ \sigma(y) = x \circ y = 5 + (x + y \pmod{5}).$$

En revanche :

$$y \circ \sigma(x) = y \circ (4 - x) = 5 + (x + y + 1 \pmod{5}).$$

Ce qui prouve qu'il n'y a pas égalité.

La démonstration dans la situation où $0 \leq y \leq 4 < x \leq 9$ est évidemment identique.

Si $5 \leq x, y \leq 9$ alors :

$$x \circ \sigma(y) = x \circ y = (x - y \pmod{5}).$$

En revanche :

$$y \circ \sigma(x) = y \circ x = (y - x \pmod{5}).$$

Donc :

$$x \circ \sigma(y) - y \circ \sigma(x) = 2(x - y) \pmod{5} \neq 0.$$

□

À partir de ce théorème on peut énoncer le corollaire :

Corollaire 7.5.9. — *La table de l'opération \star définie par :*

$$x \star y = x \circ \sigma(y),$$

est un carré latin anti-commutatif.

Le tableau T associé à la loi \star est donné par :

$$T = \begin{array}{c|cccccccccc} \star & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \hline 0 & 4 & 3 & 2 & 1 & 0 & 5 & 6 & 7 & 8 & 9 \\ \hline 1 & 0 & 4 & 3 & 2 & 1 & 6 & 7 & 8 & 9 & 5 \\ \hline 2 & 1 & 0 & 4 & 3 & 2 & 7 & 8 & 9 & 5 & 6 \\ \hline 3 & 2 & 1 & 0 & 4 & 3 & 8 & 9 & 5 & 6 & 7 \\ \hline 4 & 3 & 2 & 1 & 0 & 4 & 9 & 5 & 6 & 7 & 8 \\ \hline 5 & 6 & 7 & 8 & 9 & 5 & 0 & 4 & 3 & 2 & 1 \\ \hline 6 & 7 & 8 & 9 & 5 & 6 & 1 & 0 & 4 & 3 & 2 \\ \hline 7 & 8 & 9 & 5 & 6 & 7 & 2 & 1 & 0 & 4 & 3 \\ \hline 8 & 9 & 5 & 6 & 7 & 8 & 3 & 2 & 1 & 0 & 4 \\ \hline 9 & 5 & 6 & 7 & 8 & 9 & 4 & 3 & 2 & 1 & 0 \end{array}$$

7.5.5.1. La construction. — On va définir la clé sous la forme :

$$(11) \quad \sigma(x_1) \circ \sigma^2(x_2) \circ \sigma^3(x_3) = 0$$

plutôt que sous la forme $x_3 = f(x_1, x_2)$, car ensuite, l'extension au cas $n \geq 2$ est plus simple. Ainsi les mots de codes corrects sont de la forme $x_1 x_2 x_3$ de telle sorte que l'équation (11) soit réalisée. Remarquons que nous n'avons pas besoin de parenthèses, puisque \circ est une loi de groupe, donc associative. On laisse au lecteur le soin de vérifier que le code ainsi

construit détecte toute erreur unique et toute transposition de deux digits consécutifs (y compris si la clé est impliquée).

7.6. Passage du cas $n = 2$ au cas $n \geq 2$

Maintenant, expliquons comment calculer la clé dans le cas général. On calcule a_n en fonction de a_1, \dots, a_{n-1} de telle sorte que :

$$\sigma(a_1) \circ \sigma^2(a_2) \circ \dots \circ \sigma^{n-1}(a_{n-1}) \circ \sigma^n(a_n) = 0.$$

Ce code a bien les propriétés convoitées.

7.7. Une construction particulière

La construction suivante a été utilisée pour numéroter les billets de banque allemands. Elle ressemble à la construction précédente mais utilise une autre permutation et un calcul un peu différent de la clé.

On part de l'opération

$$(12) \quad x_3 = x_1 \circ \sigma(x_2),$$

où σ est la permutation de $\{0, \dots, 9\}$ définie par :

$$\sigma(0) = 1; \quad \sigma(1) = 5; \quad \sigma(2) = 7; \quad \sigma(3) = 6; \quad \sigma(4) = 2;$$

$$\sigma(5) = 8; \quad \sigma(6) = 3; \quad \sigma(7) = 0; \quad \sigma(8) = 9; \quad \sigma(9) = 4;$$

Théorème 7.7.1. — *La loi \star :*

$$x \star y = x \circ \sigma(y)$$

définit un carré latin anticommutatif.

Démonstration. — Il suffit d'écrire le tableau T de la loi \star pour constater qu'il a les propriétés attendues :

$$T = \begin{array}{c|cccccccccc} \star & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \hline 0 & 1 & 5 & 7 & 6 & 2 & 8 & 3 & 0 & 9 & 4 \\ \hline 1 & 2 & 6 & 8 & 7 & 3 & 9 & 4 & 1 & 5 & 0 \\ \hline 2 & 3 & 7 & 9 & 8 & 4 & 5 & 0 & 2 & 6 & 1 \\ \hline 3 & 4 & 8 & 5 & 9 & 0 & 6 & 1 & 3 & 7 & 2 \\ \hline 4 & 0 & 9 & 6 & 5 & 1 & 7 & 2 & 4 & 8 & 3 \\ \hline 5 & 9 & 0 & 3 & 4 & 8 & 2 & 7 & 5 & 1 & 6 \\ \hline 6 & 5 & 1 & 4 & 0 & 9 & 3 & 8 & 6 & 2 & 7 \\ \hline 7 & 6 & 2 & 0 & 1 & 5 & 4 & 9 & 7 & 3 & 8 \\ \hline 8 & 7 & 3 & 1 & 2 & 6 & 0 & 5 & 8 & 4 & 9 \\ \hline 9 & 8 & 4 & 2 & 3 & 7 & 1 & 6 & 9 & 5 & 0 \end{array}$$

□

On définit alors le code de longueur 11 où les mots $x_1x_2\cdots x_{11}$ vérifient :

$$\sigma(x_1) \circ \sigma^2(x_2) \circ \cdots \circ \sigma^{10}(x_{10}) \circ a_{11} = 0.$$

On laisse au lecteur le soin de vérifier que ce code détecte aussi toujours une erreur unique et toujours une transposition de deux digits consécutifs.

7.8. Conclusion

Perseverare diabolicum.

BIBLIOGRAPHIE

- [BRV05] P. BARTHÉLEMY, R. ROLLAND & P. VÉRON – *Cryptographie - principes et mises en œuvre*, Lavoisier, 2005.
- [COM97] COMAP – *Principles and practice of mathematics*, Springer-Verlag, 1997.
- [idBcglgc05] IREM DE BESANCON, GROUPE LYCÉE & GROUPE CARTOGRAPHIE – *De la sphère au plan*, Les Publications de l'IREM de Besançon, Presses Universitaires de Franche-Comté, 2005.
- [idMgl99] IREM DE MARSEILLE & GROUPE LYCÉE – *Cours et activités en arithmétique pour les classes de terminales (2^e éd.)*, irem de Marseille, 1999.
- [Rol01] R. ROLLAND – « Quelques activités arithmétiques liées aux codes correcteurs et à la cryptographie », *Bulletin de l'APMEP* **432** (2001), p. 81–94.
- [Rol02] _____, « Euro er math », *http://iml.univ-mrs.fr/rolland/* (2002).