Certificat S3

B. Helffer à partir de différents documents
(souvent préparés à partir de notes ou résumés de
P. Pansu, T. Ramond et Sylvie Ruette)
Département de Mathématiques
Université Paris-Sud

Version évolutive de Automne 2006

Table des matières

Chapitre 1

Equations différentielles

1.1 Introduction

La modélisation mathématique des phénomènes du monde réel passe presque toujours par l'écriture d'une équation différentielle, qui décrit les variations de la quantité que l'on veut étudier en fonction d'un paramètre. C'est encore une fois Isaac Newton qui a le premier écrit et étudié des équations différentielles. Son principe fondamental de la dynamique s'écrit par exemple

$$mx''(t) = F(x(t)),$$

où $t \mapsto x(t)$ décrit la trajectoire du centre de gravité d'un objet de masse m, soumis au champ de force $x \mapsto F(x)$. Il est d'ailleurs clair que pour connaître la position $x(t)$ de l'objet à l'instant t, il faut connaître non seulement la règle qui gouverne les variations de cette fonction, mais aussi la position et la vitesse initiale du centre de masse. Dans le cas d'un objet se déplaçant verticalement sous l'action de l'attraction terrestre, supposée constante dans la région où le mouvement a lieu, et compte tenu de la résistance de l'air, l'équation différentielle ci-dessus s'écrit

$$mx''(t) = -kx'(t) + mg,$$

où k, g sont des constantes. Un autre exemple célèbre est celui du pendule : une masse m est suspendue à l'extremité d'une corde de longueur ℓ dont l'autre extrémité est fixe. L'angle $\theta(t)$ que fait, à l'instant t, le fil avec la verticale vérifie la relation

$$\theta''(t) + \frac{g}{l}\sin(\theta(t)) = 0.$$

Cette équation n'a pas de solution que l'on puisse exprimer simplement avec des fonctions connues. Il faut avoir à l'esprit que c'est le cas de la plupart

des équations différentielles, même si les exercices proposés aux étudiants consistent souvent à trouver une solution explicite - c'est plus facile ! L'étude qualitative d'une équation différentielle consiste à décrire certaines propriétés des solutions sans les calculer, mais nous ne pratiquerons pas ce sport ici.

On trouve des équations différentielles dans tous les domaines de la physique. Par exemple la charge électrique $q(t)$ d'un condensateur dans un circuit RLC (résistance-bobine-condensateur), alimentée par une source de courant alternatif, doit vérifier l'équation

$$Lq''(t) + Rq'(t) + \frac{1}{C}q(t) = U\cos(\omega t).$$

La biologie est aussi une source importante d'équations différentielles. La modélisation des systèmes prédateurs-proies, due à Volterra, est particulièrement éclairante. Au niveau de ce cours, on peut aussi penser à l'évolution d'une population de bactéries : on peut être amené à penser que le taux de croissance de leur nombre est proportionnel à ce nombre. Celui-ci est alors décrit par l'équation différentielle

$$N'(t) = kN(t),$$

où k est une constante, que l'on pourra ajuster de sorte que la solution de l'équation coïncide au mieux avec les données expérimentales.

Signalons enfin que les mathématiques elles-mêmes peuvent être source d'équations différentielles. Si l'on cherche les fonctions dérivables y telles que $y(a+b) = y(a)y(b)$ pour tous réels a, b, on arrive très vite à l'équation $y' = ky$ où $k = y'(0)$. Il est d'ailleurs important de noter que résoudre l'équation

$$y' = f(x, y),$$

revient à trouver les courbes paramétrées $x \mapsto (x, y(x))$ dont le vecteur vitesse au point d'abscisse x est $(1, f(x, y(x)))$.

1.2 Fonctions de plusieurs variables

On explique tout dans le cas de deux variables x et y. Le cas plus général ne pose pas de problème particulier en dehors de la question des notations.

1.2.1 Continuité

On note d la distance euclidienne entre les points de $\mathbb{R}^2$:

$$d((x_1, y_1), (x_2, y_2)) = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}.$$

On note aussi $\|(x,y)\| = \sqrt{x^2+y^2}$ la norme euclidienne du vecteur (x,y) de $\mathbb{R}^2$, de sorte que

$$d((x_1,y_1),(x_2,y_2)) = \|(x_2-x_1, y_2-y_1)\|.$$

Définition 1.2.1
On dit qu'un sous-ensemble Ω de $\mathbb{R}^2$ est un ouvert de $\mathbb{R}^2$ si, pour tout point (x,y) de Ω, on peut trouver un disque ouvert de rayon $r_{x,y} > 0$ contenu dans Ω.

On peut penser comme exemples de base à $\Omega =]a,b[\times]c,d[$ ou à un disque ouvert).

Définition 1.2.2
Soit Ω un ouvert et $f : \Omega \subset \mathbb{R}^2 \to \mathbb{R}$ une application. On dit que f est continue en un point $(x_0,y_0) \in \Omega$ lorsque

$$f(x,y) - f(x_0,y_0) \to 0 \text{ quand } d((x,y),(x_0,y_0)) \to 0$$

On dit que f est continue (ou de classe C^0) sur Ω lorsque f est continue en chaque point de Ω.

Exemple 1.2.3
La fonction $f : (x,y) \mapsto x^4 + y^4$ est continue en tout point $(x_0,y_0) \in \mathbb{R}^2$.

Il est important de noter que pour (x_0,y_0) donné, la continuité des fonctions f_1 en y_0 et de f_2 en x_0 n'entraîne pas la continuité de f en (x_0,y_0), comme le montre l'exemple suivant.

Exercice 1.2.4
On considère la fonction $f : \mathbb{R}^2 \to \mathbb{R}$ définie par

$$f(x,y) = \begin{cases} \dfrac{xy}{x^2+y^2} & \text{si } (x,y) \neq (0,0), \\ 0 & \text{sinon.} \end{cases}$$

Montrer que f n'est pas continue en $(0,0)$ bien que les deux applications partielles associées le soient. Montrer que f admet même des dérivées partielles en $(0,0)$.

1.2.2 Dérivées partielles

La notion de dérivée partielle de f en un point (x_0, y_0) est alors particulièrement simple. Elle passe par l'introduction des applications partielles associées à f en (x_0, y_0), où l'on fige l'une des variables.

Définition 1.2.5
Soit $\Omega =]a, b[\times]c, d[$ dans $\mathbb{R}^2$, et f une application de Ω dans $\mathbb{R}$. Soit $(x_0, y_0) \in \Omega$, et $f_1 :]a, b[\to \mathbb{R}$ l'application définie par

$$f_1(x) = f(x, y_0).$$

On dit que f admet une dérivée partielle par rapport à la première variable en (x_0, y_0) lorsque f_1 est dérivable en x_0. On note $\partial_1 f(x_0, y_0)$ ou encore $\partial_x f(x_0, y_0)$ (ou encore $\dfrac{\partial f}{\partial x}(x_0, y_0)$) le nombre $f_1'(x_0)$.

De la même manière, si elle existe, on note $\partial_2 f(x_0, y_0)$ la dérivée partielle de f par rapport à la deuxième variable en (x_0, y_0).

Remarque 1.2.6
Plus généralement, on peut prendre comme Ω dans la définition ci-dessus un ouvert de $\mathbb{R}^2$. Dans ce cas la fonction f_1 est définie sur $]-r_{x_0,y_0}, r_{x_0,y_0}[$.

Exercice 1.2.7
Calculer les dérivées partielles des fonctions suivantes au point (x_0, y_0), lorsqu'elles existent.

$$f(x, y) = x^2 + y^3,\ \ f(x, y) = x^2 y^4,\ \ f(x, y) = x\cos(y) + y^2 + 2,$$

et

$$f(x, y) = |x| + \frac{y}{x^2 + y^2}\ .$$

On définit ensuite par récurrence les dérivées partielles d'ordre supérieur. Par exemple, en supposant que les dérivées partielles existent dans Ω, $\partial^2_{xx} u(x_0, y_0)$ désigne en fait $\partial_x(\partial_x u)(x_0, y_0)$, c'est à dire la dérivée partielle (si elle existe) par rapport à la première variable en (x_0, y_0) de la fonction de $\mathbb{R}^2$ dans $\mathbb{R}$, $(x, y) \mapsto \partial_x u(x, y)$.

Exercice 1.2.8
Calculer $\partial^2_{xx} u(x_0, y_0)$, $\partial^2_{yy} u(x_0, y_0)$, $\partial^2_{xy} u(x_0, y_0)$,$\partial^2_{yx} u(x_0, y_0)$ et $\partial^2_{xyx} u(x_0, y_0)$, pour les trois premières fonctions de l'exercice précédent.

On observe dans l'exercice que $\partial^2_{xy} u = \partial^2_{yx} u$. On donnera plus tard des conditions suffisantes pour que ce soit le cas. Retenons pour l'instant que lorsque la fonction est suffisamment "gentille" (par exemple si toutes les dérivées partielles sont continues) le résultat d'une succession de dérivées partielles ne dépend pas de l'ordre dans lequel on les fait.

Ceci nous conduit à une dernière définition qui étend celle des classes C^0 dont nous avons déjà parlé :

Définition 1.2.9
Soit Ω un ouvert de $\mathbb{R}^2$ et $k \in \mathbb{N}$ ($k > 0$). On dira que f est de classe C^k dans Ω (et on notera $f \in C^k(\Omega)$, si f est de classe C^{k-1} et si ses dérivées partielles existent et sont aussi de classe C^{k-1} dans Ω.

Remarque 1.2.10
La classe C^k est effectivement "gentille".

1.3 Définition d'une équation différentielle ordinaire

Définition 1.3.1
Soit F une fonction réelle définie sur $U \times \Omega$, où U est un intervalle de $\mathbb{R}$ et Ω est un ouvert de $\mathbb{R}^n$. Si I est un intervalle de $\mathbb{R}$ et $y : x \mapsto y(x)$ une fonction définie sur I, de classe C^n, on dit que (I, y) est une solution de l'équation différentielle d'ordre n

$$(ED) \qquad y^{(n)} = F(x, y, y', y'', \ldots, y^{(n-1)})$$

lorsque $I \subset U$ et, pour tout $x \in I$, on a $(y(x), y'(x), y''(x), \ldots, y^{(n-1)}(x)) \in \Omega$ et

$$y^{(n)}(x) = F(x, y(x), y'(x), y''(x), \ldots, y^{(n-1)}(x)),$$

pour $x \in I$.

Question 1.3.2
Donner la fonction F, U et Ω dans les exemples précédents.

Remarque 1.3.3
On dit parfois que les équations différentielles de la forme (ED) sont des équations différentielles résolues (la dérivée de plus haut degré s'écrit comme fonction des dérivées d'ordre inférieur), et l'on s'autorise à considérer comme équations différentielles des expressions de la forme

$$G(x, y, y', \ldots, y^{(n)}) = 0.$$

Cependant la résolution de ce genre d'équations passe toujours par une mise sous la forme (ED). Par exemple l'expression $xy' + y = 0$ n'est pas une équation différentielle résolue, et ne peut pas l'écrire sous la forme (ED) sur $\mathbb{R}$ tout entier : on n'obtient au mieux qu'une équation différentielle résolue ($y' = -y/x$) sur chacun des intervalles $U =]-\infty, 0[$ et $U =]0, +\infty[$.

Attention !
On ne peut pas toujours trouver de solution définie sur U tout entier, même pour des équations différentielles simples. Soit par exemple F la fonction définie par $F(x, y) = 1 + y^2$. Son domaine de définition est $U \times \Omega$ avec $U = \mathbb{R}$ et $\Omega = \mathbb{R}$. L'équation différentielle

$$y' = F(x, y) = 1 + y^2$$

a pour solution $y = \tan x$ sur chaque intervalle I où cette fonction est définie (par exemple $I =]-\pi/2, \pi/2[$). Mais il n'y a pas de solution définie sur $U = \mathbb{R}$ tout entier.

Définition 1.3.4
On dit que (I, y) est une solution globale de l'équation différentielle (ED) lorsque $I = U$.

Supposons que l'on ait déterminé une solution (I, y) de l'équation différentielle (ED) par un procédé quelconque, et que ce ne soit pas une solution globale ($I \neq U$). Est-il possible de trouver un intervalle J plus grand que I sur lequel la fonction y est encore solution de (ED) ? On vient de voir que ce n'est pas toujours le cas : la solution $(]-\pi/2, \pi/2[, x \mapsto \tan x)$ de l'exemple précédent ne peut pas être prolongée. Par contre, si on avait obtenu la solution $(]-1, 1[, x \mapsto \tan x)$, on aurait pu la prolonger en $(]-\pi/2, \pi/2[, x \mapsto \tan x)$.

Définition 1.3.5
Soit (I_1, y_1) et (I_2, y_2) deux solutions de l'équation différentielle (ED). On dit que (I_2, y_2) prolonge (I_1, y_1) lorsque I_2 contient I_1, et y_2 coïncide avec y_1 sur I_1 :

$$\text{pour tout } x \in I_1,\ y_2(x) = y_1(x).$$

On dit que (I, y) est une solution maximale de (ED) lorsqu'elle n'admet pas d'autre prolongement qu'elle-même.

1.4 Equations différentielles linéaires d'ordre 1

On considère maintenant les équations différentielles de la forme

$$(EDL1) \qquad y' + a(x)y = f(x),$$

où a et f sont deux fonctions définies et continues sur un intervalle U. Ce sont des équations du type (ED), d'ordre 1, avec F définie sur $U \times \mathbb{R}$ par

$$F(x, y) = f(x) - a(x)y \ ,$$

Notant H la partie de F qui dépend de y, ici $H(x, y) = -a(x)y$, on voit facilement que H est linéaire par rapport à la variable y :

$$H(x, \lambda_1 y_1 + \lambda_2 y_2) = \lambda_1 H(x, y_1) + \lambda_2 H(x, y_2),$$

pour tous $(\lambda_1, \lambda_2) \in \mathbb{R}^2$ et tous $(y_1, y_2) \in \mathbb{R}^2$. On parle donc d'équations différentielles linéaires d'ordre 1.

Nous allons voir que pour ce type d'équations, il est possible d'exprimer toutes les solutions à l'aide d'intégrales et de fonctions connues.

Attention !

Il ne faut surtout pas croire que c'est le cas de toutes les équations différentielles. . .

1.4.1 Le principe de superposition

La linéarité de l'équation est une propriété très utile. On a en particulier la

Proposition 1.4.1

Soit (I, y_1) une solution de l'équation (EDL1). Toute solution (I, y_2) de (EDL1) s'écrit $y_2 = y_1 + z$, où z est solution sur I de l'équation différentielle homogène associée :

$$z' + a(x)z = 0.$$

Preuve

Pour tout $x \in I$, on a

$$(y_1)'(x) + a(x)y_1(x) = f(x)$$

et

$$(y_2)'(x) + a(x)y_2(x) = f(x) \ .$$

On a donc, par soustraction

$$(y_2)'(x) - (y_1)'(x) + a(x)(y_2(x) - y_1(x)) = 0,$$

et, posant $z = y_2 - y_1$*, il suffit de remarquer que* $z' = (y_2 - y_1)' = (y_2)' - (y_1)'$.

Autrement dit, pour trouver toutes les solutions de (EDL1), il suffit de

(1) trouver l'ensemble des solutions de l'équation homogène associée ;

(2) trouver une solution quelconque de (EDL1).

1.4.2 Solutions de l'équation homogène associée

Proposition 1.4.2
Soit a *une fonction continue sur* $U \subset \mathbb{R}$*. Les solutions maximales de l'équation* $z' + a(x)z = 0$ *sont globales, et sont définies par* $z : x \mapsto Ce^{-A(x)}$*, où* $C \in \mathbb{R}$ *est une constante, et*

$$A(x) = \int_{x_0}^{x} a(s)ds\,,$$

avec $x_0 \in U$*.*

Preuve
Il est d'abord très simple de vérifier que pour n'importe quel C *et n'importe quel* $x_0 \in U$*, la fonction* $x \mapsto Ce^{-A(x)}$ *est* C^1 *sur* U *et y vérifie l'équation.*

Soit maintenant (I, z) *une solution quelconque de l'équation. La fonction* $w : x \mapsto e^{A(x)}z(x)$ *est constante sur l'intervalle* I *: en effet, pour tout* $x \in I$*, on a*

$$w'(x) = e^{A(x)}z'(x) + a(x)e^{A(x)}z(x) = e^{A(x)}(z'(x) + a(x)z(x)) = 0.$$

Donc il existe $C_0 \in \mathbb{R}$ *tel que, pour tout* $x \in I$*,* $w(x) = C_0$*, ou encore* $z(x) = C_0e^{-A(x)}$*. Or* $x \mapsto C_0e^{A(x)}$ *est une fonction* C^1 *sur* U*, donc* (I, z) *se prolonge bien en la solution globale* $(U, x \mapsto C_0e^{-A(x)})$*.*

On peut se demander comment l'on a deviné la forme des solutions. Une façon de procéder est de raisonner par condition nécessaire : si (I, z) est une solution de l'équation, on doit avoir, pour tout $x \in I$,

$$z'(x) = -a(x)z(x).$$

On est alors bien sûr tenté de diviser les deux membres de cette égalité par $z(x)$, mais il faut pour cela faire l'hypothèse que $z(x) \neq 0$ pour tout $x \in I$. Compte tenu du résultat qui précède, ce n'est pas un réel problème : les solutions de l'équation homogène $z' + a(x)z = 0$ ne s'annulent jamais, sauf s'il s'agit de la fonction constante nulle ($C = 0$).

Continuons donc, en supposant que z ne s'annule jamais sur I : on arrive à

$$\frac{z'(x)}{z(x)} = -a(x),$$

et en intégrant chacun des membres de cette égalité,

$$\ln|z(x)| - \ln|z(x_0)| = -\int_{x_0}^{x} a(s)ds = -A(x).$$

On a donc

$$|z(x)| = Ke^{-A(x)},$$

où $K = e^{\ln|z(x_0)|} = |z(x_0)|$ est une constante strictement positive. On doit donc avoir $z(x) = \epsilon(x)Ke^{-A(x)}$, où $\epsilon(x) = \pm 1$. Mais puisque z doit être continue, la fonction ϵ est nécessairement contante sur I, et l'on obtient bien

$$z(x) = Ce^{-A(x)},$$

pour une constante $C \in \mathbb{R}$.

1.4.3 Recherche d'une solution particulière : variation de la constante

Grâce au principe de superposition, il reste à trouver une solution particulière de l'équation (EDL1). On va utiliser la méthode dite "de variation de la constante", qui ressemble beaucoup à ce que l'on vient de faire. L'idée est la suivante :
On cherche une solution (I, y) de (EDL1) sous la forme

$$y(x) = C(x)e^{-A(x)},$$

où C est une fonction C^1 à déterminer, et $A(x) = \int_{x_0}^{x} a(s)ds$ est défini comme ci-dessus. De manière un peu rapide, on dit que l'on fait varier la constante C qui apparaît dans l'expression de la solution de l'équation homogène associée à (EDL1).

Pour que cette fonction soit une solution, il faut et il suffit que

$$f(x) = y'(x)+a(x)y(x) = C'(x)e^{-A(x)}-a(x)C(x)e^{-A(x)}+a(x)C(x)e^{-A(x)} = C'(x)e^{-A(x)},$$

et il suffit donc de prendre pour $C(x)$ une primitive quelconque de $x \mapsto f(x)e^{A(x)}$, c'est-à-dire

$$C(x) = \int_{x_0}^{x} f(u)e^{A(u)}du,$$

o $x_0 \in I$.

Il faut noter au passage que la solution y correspondante, donnée par

$$y(x) = e^{-A(x)} \int_{x_0}^{x} e^{A(u)} f(u) du$$

est une solution sur U tout entier, c'est-à-dire une solution globale.

Attention !
La "variation de la constante" est une méthode qui permet toujours de trouver une solution particulière. Il est important de comprendre que ce n'est certainement pas la seule méthode possible. Par exemple, l'utiliser pour trouver une solution particulière de l'équation $y' = 1$ est très exagéré...

1.4.4 L'ensemble des solutions

Au total, on a trouvé toutes les solutions de l'équation (EDL1), et l'on a montré la

Proposition 1.4.3
Soient a et f deux fonctions continues sur un intervalle U de $\mathbb{R}$. L'ensemble $\mathcal{C}$ des solutions maximales de l'équation

$$y' + a(x)y = f(x)$$

est donné par

$$\mathcal{C} = \left\{ (U, y),\ y : x \mapsto e^{-A(x)}(\alpha + \int_{x_0}^{x} e^{A(s)} f(s) ds), \alpha \in \mathbb{R} \right\},$$

où $A(x) = \int_{x_0}^{x} a(s) ds$, avec $x_0 \in U$. En particulier toutes les solutions maximales sont des solutions globales.

1.5 Résolution de quelques équations différentielles non linéaires classiques

1.5.1 Autour des équations de Hamilton

L'exemple le plus simple est celui du mouvement d'un corps (identifié) à un point sur la droite. La variable x correspond alors au temps et le mouvement est décrit par l'équation :

$$y''(x) = f(y(x)) \,, \tag{1.1}$$

(c'est la célèbre formule $\vec{F} = m\gamma$, où γ est l'accélération).
La fonction G qui intervient est ici la fonction

$$(x, y_0, y_1, y_2) \mapsto G(x, y_0, y_1, y_2) = y_2 - f(y_0) \ .$$

On note que la fonction G ne dépend pas de x et de y_1.

Lorsque $f(y) = -v'(y)$ pour une fonction v continûment dérivable, on peut montrer, en dérivant par rapport à x, la fonction "énergie" :

$$x \mapsto \frac{1}{2}u'(x)^2 + v(u(x)) \ ,$$

avec u solution de (1.1), que celle-ci est constante au cours du temps :

$$\frac{1}{2}u'(x)^2 + v(u(x)) = E_0 \ ,$$

où E_0 est calculée par la valeur de l'énergie au temps initial x_0.
On obtient une nouvelle équation (plus facile à résoudre) qui a la forme ci-dessus avec cette fois-ci :

$$G(x, y_0, y_1) := \frac{1}{2}y_1^2 + v(y_0) - E_0 \ .$$

On verra dans le prochain paragraphe comment cela peut permettre de résoudre l'équation.

Ici, on a regardé le cas où la dimension d'espace est 1. Pour traiter des cas plus généraux, on utilisera très souvent des résultats du type suivant (dérivée d'une fonction composée).

Lemme 1.5.1
Soit $u : \mathbb{R}^2 \to \mathbb{R}$ une application de classe C^1. Soit aussi f_1 et f_2 deux applications de classe C^1 de $\mathbb{R}$ dans $\mathbb{R}$. Alors l'application $F : \mathbb{R} \to \mathbb{R}$ définie par

$$F(t) = u(f_1(t), f_2(t))$$

est dérivable, sa dérivée est continue et donnée par

$$F'(t) = f_1'(t)\,\frac{\partial u}{\partial x}(f_1(t), f_2(t)) + f_2'(t)\,\frac{\partial u}{\partial y}(f_1(t), f_2(t)) \ .$$

Preuve :
Elle est admise pour l'instant.

Expliquons ce qui se passe en dimension 2, la force F est de la forme

$$F = -(\partial_x V, -\partial_y V) \ ,$$

On peut montrer alors que, si les équations de la mécanique sont satisfaites :

$$x''(t) = -(\partial_x V)(x(t), y(t)) \ , \ y''(t) = -(\partial_y V)(x(t), y(t)) \ ,$$

alors on a "conservation de l'énergie"

$$\frac{1}{2}\left(x'(t)^2 + y'(t)^2\right) + V(x(t), y((t)) = E_0 \ .$$

Mais contrairement au cas $n = 1$ cette remarque ne suffit pas pour déterminer la solution. Il faut trouver une autre quantité conservée. C'est par exemple le cas si $V(x, y) = \frac{1}{2}(x^2+y^2)$ où l'on constate que l'on peut séparer les variables pour résoudre.

1.5.2 Equations à variables séparées

Considérons l'équation

$$y'(x) = a(x)b(y(x)) \ , \tag{1.2}$$

où a et b sont des fonctions données.

Si on suppose que $b(y_0) = 0$ pour un réel y_0, alors il est immédiat de vérifier que la fonction $x \mapsto y(x) = y_0$ est solution.
Si on écarte ce cas, on peut chercher des solutions définies sur un intervalle I telles que $b(y(x)$ ne s'annule pas.
On réécrit alors l'équation sous la forme

$$\frac{y'}{b(y)} = a(x) \ .$$

Si cette solution existe avec $y(x_0) = y_0$, elle doit vérifier

$$\int_{x_0}^{x} \frac{y'(t)}{b(y(t)} dt = \int_{x_0}^{x} a(t) dt \ .$$

Après changement de variable dans le terme de gauche, ceci s'écrit

$$\int_{y_0}^{y(x)} \frac{1}{b(u)} \, du = \int_{x_0}^{x} a(t) dt \ .$$

Si on désigne par A une primitive de a et par C une primitive de $\frac{1}{b}$, on obtient

$$C(y(x)) - C(y_0) = A(x) - A(x_0) \ .$$

Dans un petit intervalle $]y_0 - r, y_0 + r[$ tel que b est différent de zéro, la fonction C est monotone et admet une fonction inverse C^{-1}. On obtient donc que nécessairement

$$y(x) = C^{-1}(A(x) + C(y_0) - A(x_0)) \ ,$$

pour $x - x_0$ assez petit.

Exemple 1.5.2
Etudier $y' = y^2$. Discuter en fonction de la condition initiale en $x = 0$. On distinguera trois cas selon que $y(0) > 0$, $y(0) = 0$ et $y(0) < 0$. On cherchera dans chaque cas des solutions maximales.

Exemple 1.5.3
Etudier

$$2xy'y = 1 \ .$$

1.5.3 Equations différentielles à coefficients constants d'ordre plus élevé.

On regarde l'équation avec second membre :

$$(ed) \qquad \sum_{j=0}^{n} a_j y^{(n-j)}(t) = b(t) \ .$$

Equations différentielles homogènes.

Pour le système homogène, qui est défini par :

$$(eh) \qquad \sum_{j=0}^{n} a_j y^{(n-j)}(t) = 0 \ ,$$

on peut faire une réduction a un système différentiel d'ordre 1 $n \times n$: ceci sera expliqué ultérieurement.

On peut aussi chercher plus directement des solutions de la forme $\exp \lambda t$, ce qui conduit, en mettant dans l'équation à :

$$(ei) \qquad \Phi(\lambda) := \sum_{j=0}^{n} a_j \lambda^{n-j} = 0 \ .$$

La fonction $\exp \lambda t$ est donc solution du système si et seulement si λ est racine de cette équation.

On peut alors reprendre la discussion faite dans le cas des {equations d'ordre 1.

Un premier point est que :

Théorème 1.5.4
L'espace des solutions de l'équation homogène (eh) est de dimension n.

Si l'équation précédente possède n racines réelles distinctes λ_j ($j = 1, \cdots, n$), une base est constituée par les fonctions $\exp \lambda_j t$.

Dans le cas où l'on a une valeur propre complexe (non réelle) $\lambda_0 = \mu + i\nu$, deux solutions complexes indépendantes sont données par $\exp \lambda_0 t$ et $\exp \overline{\lambda_0} t$. Si on cherche les solutions réelles, on vérifie que $\exp \mu t \cos \nu t$ et $\exp \mu t \sin \nu t$ sont des solutions indépendantes.

Si λ_0 est une racine double de l'équation, on peut montrer que $t \exp \lambda_0 t$ est aussi solution (il faut penser[1] que c'est $(\frac{d}{d\lambda} \exp \lambda t)_{/\lambda=\lambda_0}$). Plus généralement, si λ_0 est une racine de multiplicité k de l'équation, $t^j \exp \lambda_0 t$ est solution pour $j = 0, 1, \cdots, k-1$.

Ceci fournit un moyen de déterminer toutes les solutions homogènes.

La méthode de variation des constantes

Il ne reste plus qu'à expliquer la méthode de variation des constantes. On se contente de détailler le cas de l'ordre 2. Elle sera expliquée après la réduction aux systèmes. Elle a aussi été expliquée en L1. On rappelle ici juste la règle sans justification.
On considère donc (on peut se ramener au cas $a_0 = 1$ en divisant par a_0) l'équation :

$$(ed) \qquad y''(t) + a_1 y'(t) + a_2 y(t) = b(t) \ .$$

et son équation homogène associée :

$$(eh) \qquad y''(t) + a_1 y'(t) + a_2 y(t) = 0 \ .$$

Dans tous les cas, on vient de montrer (quitte à passer par la recherche de solutions complexes) que l'on pouvait trouver deux solutions indépendantes $y_1(t)$ et $y_2(t)$. On cherche une solution (pour (SD)) sous la forme :

$$y(t) := c_1(t) y_1(t) + c_2(t) y_2(t)$$

[1] On peut écrire pour tout λ que

$$(\sum_j a_j \frac{d^{n-j}}{dt^{n-j}} \exp \lambda t) = \Phi(\lambda) \exp \lambda t \ .$$

On peut alors dériver par rapport à λ cette identité et prendre $\lambda = \lambda_0$. Pour le résultat plus général, il faut continuer de dériver par rapport à λ, jusqu'à l'ordre $(k-1)$.

qui doit satisfaire les **deux** équations :

$$\begin{array}{ll} c_1' y_1' + c_2' y_2' & = b(t) \ , \\ c_1' y_1 + c_2' y_2 & = 0 \ . \end{array} \tag{1.3}$$

La matrice qui apparaît dans le terme de gauche

$$M_w(y_1, y_2) = \begin{pmatrix} y_1' & y_2' \\ y_1 & y_2 \end{pmatrix}$$

est appelée la matrice wronskienne de y_1 et y_2. Le déterminant de la matrice wronskienne est appelé le wronskien :

$$W(t) := w(y_1, y_2) = y_1'(t) y_2(t) - y_2'(t) y_1(t) \ .$$

Ce déterminant est non nul, ce qui reflète le choix de deux solutions indépendantes du système homogène. On peut alors résoudre (1.3) en reconnaissant qu'il s'agit d'un système de Cramer et déterminer les fonctions c_1' et c_2' puis c_1 et c_2 comme primitives des précédentes.

Exercice 1.5.5
Montrer que le wronskien est indépendant de t si $a_1 = 0$. Dans le cas général, montrer que $t \mapsto w(y_1(t), y_2(t)$ est solution d'une équation différentielle du premier ordre.

Travaux pratiques : exemple vu en S2
Il s'agit de l"exemple

$$y'' + a_1 y' + a_2 y = \alpha \cos(\omega t + \phi) \ .$$

On cherche les racines de :

$$\lambda^2 + a_1 \lambda + a_2 = 0 \ .$$

On se contente de traiter le cas où cette équation a deux racines distinctes et réelles : r_1 et r_2.

Suivant la règle établie ci-dessus, on tombe sur :

$$\begin{array}{ll} r_1 c_1'(t) \exp r_1 t + r_2 c_2'(t) \exp r_2 t & = b(t) \\ c_1'(t) \exp r_1 t + c_2' \exp r_2 t & = 0 \end{array}$$

Chacun peut résoudre, à t fixé, ce système de deux équations pour $c_1'(t)$ et $c_2'(t)$ par sa méthode favorite. Suivons une méthode matricielle.

On peut réécrire le système sous la forme :

$$\begin{pmatrix} r_1 & r_2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \exp r_1 t\ c_1' \\ \exp r_2 t\ c_2' \end{pmatrix} = \begin{pmatrix} b(t) \\ 0 \end{pmatrix} .$$

En utilisant la matrice inverse, on obtient :

$$\begin{pmatrix} \exp r_1 t\ c_1' \\ \exp r_2 t\ c_2' \end{pmatrix} = \frac{1}{r_1 - r_2} \begin{pmatrix} 1 & -r_2 \\ -1 & r_1 \end{pmatrix} \begin{pmatrix} b(t) \\ 0 \end{pmatrix} .$$

Ceci conduit à :

$$\begin{aligned} c_1'(t) &= \frac{1}{r_1 - r_2}\ \exp -r_1 t\ b(t) , \\ c_2'(t) &= -\frac{1}{r_1 - r_2}\ \exp -r_2 t\ b(t) . \end{aligned}$$

D'où une solution particulière obtenue par :

$$\begin{aligned} c_1(t) &= \frac{1}{r_1 - r_2}\ \int_0^t \exp -r_1 s\ b(s)\ ds , \\ c_2(t) &= -\frac{1}{r_1 - r_2}\ \int_0^t \exp -r_2 s\ b(s)\ ds . \end{aligned}$$

On peut pousser le calcul lorsque $b(t) = \alpha(\cos \omega t + \phi)$. Un moyen pour se faciliter ce calcul est de penser que $b(t) = \alpha \operatorname{Re} \exp i(\omega t + \phi)$ et de faire le calcul d'abord avec $\alpha \exp i(\omega t + \phi)$.

Par exemple :

$$c_1(t) = \operatorname{Re} \left(\frac{1}{r_1 - r_2}\ \int_0^t \exp((i\omega - r_1)s + i\phi)\ ds \right) .$$

On laisse la suite au lecteur .... le cas où $r_1 = i\omega$, $r_2 = -i\omega$ est un peu particulier.

Remarque 1.5.6
La recherche d'une solution particulière dans le cas particulier $b(t) = \alpha \cos(\omega t + \phi)$, peut aussi être menée de la manière suivante.
On prend d'abord $b(t) = z \exp i\omega t$, (avec $z = \alpha \exp i\phi$). On cherche une solution particulière de la forme $\tilde{z} \exp i\omega t$. On trouve :

$$\tilde{z}\Phi(i\omega) = z ,$$

où $\Phi(\lambda) = \lambda^2 + a_1\lambda + a_2$.
Ceci fonctionne dès que $\Phi(i\omega) \neq 0$, c'est à dire $i\omega \neq r_1$ et $i\omega \neq r_2$.
On vérifie alors que $\operatorname{Re}(\tilde{z} \exp i\omega t)$ est une solution particulière.

1.5.4 Système : Cas d'une matrice triangulaire

Expliquons (voir plus loin pour une étude plus détaillée) comment on traite le cas triangulaire sur un exemple très simple, mais la méthode est générale. Considérons par exemple :

$$\begin{aligned} dx_1/dt &= a_{11}x_1(t) + a_{12}x_2(t) \\ dx_2/dt &= a_{22}x_2(t)\ . \end{aligned}$$

Il suffit de commencer par résoudre explicitement la deuxième équation. Une fois trouvé $x_2(t)$, la première équation n'est plus qu'une équation différentielle pour $x_1(t)$.

1.6 Problème de Cauchy

On vient de le voir, une équation différentielle a en général beaucoup de solutions, même si l'on ne s'intéresse qu'aux solutions maximales. D'un autre côté, on rappelle que la trajectoire $M(t)$ d'un point matériel au cours du temps est complètement déterminé par l'équation de Newton (une équation différentielle d'ordre 2), à condition de préciser la position et la vitesse initiale du point. Ceci conduit à la notion de problème de Cauchy pour l'équation différentielle (ED), pour lequel on espère avoir une solution unique.

Définition 1.6.1
Soient U un intervalle de $\mathbb{R}$, Ω un ouvert de $\mathbb{R}^n$, x_0 un point de U et $\hat{y} = (\hat{y}_0, \hat{y}_1, \ldots, \hat{y}_{n-1})$ un point de Ω. Soient F une fonction définie sur $U \times \Omega$. On appelle problème de Cauchy (avec condition initiale $\hat{y}$ en x_0) pour l'équation différentielle

$$(ED) \qquad y^{(n)} = F(x, y, y', y'', \ldots, y^{(n-1)})$$

la recherche des solutions[2] *de (ED) vérifiant la condition initiale*

$$y(x_0) = \hat{y}.$$

L'exemple suivant montre que la situation n'est pas aussi simple qu'on pourrait le souhaiter : il arrive qu'un problème de Cauchy ait plusieurs solutions.

[2]Plus précisément, la recherche d'un intervalle ouvert I contenant x_0 et d'une fonction de classe C^n dans I telle que $(y(x), \ldots, y^{(n-1)}(x))$ reste dans Ω pour $x \in I$ et soit solution de

$$y^{(n)}(x) = F(x, y(x), y'(x), \ldots, y^{(n-1)}(x))\ ,\ \forall x \in I\ .$$

Exemple 1.6.2
La fonction nulle est une solution sur $\mathbb{R}$ de l'équation différentielle $y' = 3|y|^{2/3}$. La fonction $x \mapsto x^3$ est également une solution sur $\mathbb{R}$, et le problème de Cauchy

$$\begin{cases} y' = 3|y|^{2/3}, \\ y(0) = 0, \end{cases}$$

admet donc au moins deux solutions[3].

Voici cependant une réponse satisfaisante, qui porte le nom de théorème de Cauchy-Lipschitz. Sous certaines hypothèses relativement faibles sur la fonction F, un problème de Cauchy admet une unique solution localement, c'est à dire sur un intervalle I contenant x_0.
Attention !
On n'a, en général, aucune information sur l'intervalle I d'existence de la solution. On se contente d'un énoncé pour les équations différentielles d'ordre 1, mais ce résultat est très général.

Proposition 1.6.3
Soit F une fonction définie sur $U \times \Omega$, où U et Ω sont des intervalles ouverts de $\mathbb{R}$. Soit aussi $x_0 \in U$ et $\hat{y} \in \Omega \subset \mathbb{R}$. On considère le problème de Cauchy

$$(P) \qquad \begin{cases} y' = F(x, y), \\ y(x_0) = \hat{y}. \end{cases}$$

Si F est continue sur $U \times \Omega$ et admet une dérivée partielle $\dfrac{\partial F}{\partial y}$ continue sur $U \times \Omega$, alors il existe un intervalle $I \subset U$ contenant x_0 et une fonction y de classe C^1 sur I solution de (P). De plus si (J, y_1) est une autre solution de (P), avec $x_0 \in J$, alors $y_1(x) = y(x)$ pour tout $x \in I \cap J$.

Question 1.6.4
Pourquoi le Théorème de Cauchy-Lipschitz ne s'applique-t-il pas dans le cas de l'exemple précédent ?

Dans le cas des équations linéaires d'ordre 1, on a vu que :
$F(x, y) = -a(x)y + f(x)$.
Lorsque a et f sont continues sur U, la fonction F est continue sur $U \times \mathbb{R}$, et est dérivable par rapport à y avec $\partial_y F(x, y) = -a(x)$. En particulier $\partial_y F$ est continue sur $U \times \mathbb{R}$, et le Théorème de Cauchy-Lipschitz s'applique :

[3]En travaillant un peu, le lecteur en trouvera quatre

Pour $x_0 \in U$ et $y_0 \in \mathbb{R}$ donnés, il existe un intervalle $I \subset U$ contenant x_0 et une fonction y de classe C^1 sur I qui est l'unique solution sur I du problème de Cauchy

$$\begin{cases} y' = -a(x)y + f(x), \\ y(x_0) = \hat{y}. \end{cases}$$

Pour ce type d'équations, on a déjà obtenu bien mieux :
On connaît toutes les solutions de l'équation, et il est très facile de vérifier que le problème de Cauchy ci-dessus admet une unique solution. C'est la fonction de l'ensemble $\mathcal{C}$ correspondant à $\alpha = \hat{y}$. On sait d'ailleurs aussi que l'on a $I = U$.

Autrement dit, le théorème de Cauchy-Lipschitz n'est pas d'une grande utilité dans le cas où l'on sait déterminer explicitement l'ensemble des solutions. Mais, rappelons-le, cela est extrêmement rare.

Exercice 1.6.5
Montrer que le problème de Cauchy ($y' = (1+x)^x e^{\cos y}$; $y(0) = y_0$) admet une solution unique au voisinage de $x_0 = 0$.

1.7 Equations aux Dérivées Partielles (EDP)

Dans le cas de deux variables, une EDP d'ordre 1 s'écrit

$$F(x, y, u(x,y), \partial_x u(x,y), \partial_y u(x,y)) = 0. \tag{1.4}$$

et une équation du second ordre s'écrit

$$\begin{aligned} F(x, y, u(x,y), \partial_x u(x,y), \partial_y u(x,y), \\ \partial_x^2 u(x,y), \partial_x \partial_y u(x,y) = 0 \ . \end{aligned} \tag{1.5}$$

Plus généralement, on peut considérer des équations mettant en jeu des dérivées $\partial_x^{m_j} \partial_y^{n_j} u$. L'ordre d'une EDP est alors le plus grand ordre de dérivation $m_j + n_j$ qui apparaît dans l'équation.

Résoudre une EDP dans un domaine Ω de $\mathbb{R}^d$ (d est le nombre de variables), c'est trouver une fonction suffisamment régulière (i.e. dans une classe C^k avec k assez grand) dans Ω telle que la relation (1.4) soit satisfaite pour toutes les valeurs des variables dans Ω.

Voici quelques exemples, très simples a priori, d'EDP à deux variables. Certaines de ces EDP modélisent l'évolution au cours du temps de certains systèmes, et il est d'usage de garder la notation t pour la variable temps.

1. $\partial_t u(t,x) + c\partial_x u(t,x) = 0$ (une équation de transport) ; (Etudier s'il existe des solutions de la forme $g(x-at)$ avec g de classe C^1).
2. $\partial_t u(t,x) + u(t,x)\partial_x u(t,x) = 0$ (une équation d'onde de choc) ;
3. $\partial_x \partial_y u(x,y) = 0$ (variante de l'équation des ondes) ;
4. $\partial^2_{xx} u(x,y) + \partial^2_{yy} u(x,y) = 0$ (l'équation de Laplace) ;
5. $\partial^2_{tt} u(t,x) = \partial^2_{xx} u(t,x)$ (l'équation des ondes ou des cordes vibrantes).

Comme pour les EDO, on parle d'EDP linéaires ou non-linéaires. Dans la liste ci-dessus, seule l'équation 3. est non-linéaire. Pour mieux comprendre de quoi il s'agit, il est commode de parler de l'opérateur aux dérivées partielles associé à une EDP. Il s'agit de l'application qui à une fonction u associe le membre de gauche de l'EDP. Par exemple l'opérateur associée à l'équation 1. est $P_1 : u \mapsto \partial_x u + \partial_y u$, celui associée à l'équation (3) est $P_3 : u \mapsto \partial_x u + u\partial_y u$. On dit que l'EDP est linéaire lorsque l'opérateur P qui lui est associé l'est, c'est à dire que, pour toutes fonctions u, v "gentilles" et

$$\forall \alpha, \beta \in \mathbb{R}, P(\alpha u + \beta v) = \alpha P(u) + \beta P(v) \, . \tag{1.6}$$

C'est bien le cas pour P_1, et il est très simple de vérifier que $P_3(\alpha u) \neq \alpha P_3(u)$ en général.

D'autre part on parle également d'EDP linéaire homogène lorsque la fonction nulle $u = 0$ est solution. En d'autres termes tous les termes de l'équation contiennent la fonction inconnue ou l'une de ses dérivées partielles. Toutes les équations linéaires ci-dessus sont homogènes, alors que l'EDP

$$\partial^2_{xx} u + \partial^2_{yy} u = f(x,y) \tag{1.7}$$

ne l'est pas ! Notons que l'opérateur aux dérivées partielles associé à (1.7) est $P_5 = \partial^2_{xx} + \partial^2_{yy}$ comme pour l'équation 5. ci-dessus.

Comme pour les EDO, les EDP linéaires homogènes ont une propriété particulière, communément appelé principe de superposition : toute combinaison linéaire de solutions est encore une solution. Enfin lorsque l'on ajoute à une solution d'une EDP linéaire inhomogène une solution quelconque de l'EDP homogène associée, on obtient encore une solution de l'EDP inhomogène.

Chapitre 2

Courbes paramétrées, Intégrales curvilignes et de surface

2.1 Rappels sur les courbes paramétrées

Cette partie a déjà été enseignée. Seuls des rappels seront donnés en cours oral.

2.1.1 Motivation

La trajectoire d'un point qui se déplace dans un plan, est donnée par deux fonctions $x(t)$ et $y(t)$ du temps.

Lorsque les fonctions $t \mapsto x(t)$ et $t \mapsto y(t)$ sont données, on veut tracer la courbe à la main et étudier ses caractéristiques.

On sait déjà tracer des trajectoires particulières, celles où $x(t) = t$. En effet, dans ce cas, la courbe est le graphe d'une fonction d'une variable réelle. On va voir que le tracé dans le cas général se déduit de ce cas particulier.

La courbe tracée ne garde pas toutes les informations obtenues de la donnée des deux fonctions $t \mapsto x(t)$ et $t \mapsto y(t)$. On ajoute parfois sur le tracé le sens dans lequel est parcouru la courbe : on parle alors de courbe orientée.

a. Définition

Une *courbe paramétrée* (continue) consiste à se donner un intervalle I de $\mathbb{R}$ et deux fonctions continues $t \mapsto x(t)$ et $t \mapsto y(t)$ sur I. Tracer la courbe, c'est représenter dans le plan muni d'un repère $0xy$ l'ensemble des points de la forme $(x(t), y(t))$ lorsque t décrit l'intervalle I.

On peut aussi parler de courbe paramétrée, de classe C^1, de classe C^2. De manière analogue, on peut parler de courbe paramétrée dans $\mathbb{R}^3$. On note alors souvent :
$t \mapsto (x(t), y(t), z(t))$),
ou dans $\mathbb{R}^n$, et on note alors :
$t \mapsto (x_1(t), x_2(t), \cdots, x_n(t))$.

Il ne faut pas confondre la notion de courbe paramétrée avec la notion de courbe (ou de trajectoire ou d'image de la courbe). Une courbe peut-être parcourue plusieurs fois, avec une vitesse différente....

b. Exemple : Représentation paramétrique d'une droite.

On considère la courbe paramétrée définie par $x(t) = 2t+1$, $y(t) = 3t-1$, $I = \mathbb{R}$. La courbe obtenue est la droite D passant par $(1, -1)$ et de vecteur directeur $(2, 3)$. Si on se limite à l'intervalle $I = [0, 1]$, on obtient seulement le segment de droite reliant les points $(1, -1)$ et $(3, 2)$.

La représentation $x_1(t) = 6t + 1$, $y_1(t) = 9t - 1$, $I = \mathbb{R}$, donne la même droite D. Si on se limite à l'intervalle $I = [0, 1]$, on obtient maintenant le segment deux fois plus long reliant les points $(1, -1)$ et $(7, 8)$.

c. Exemple : Graphe d'une fonction.

Soit $f : I \to \mathbb{R}$ une fonction dérivable. La courbe paramétrée $x(t) = t$, $y(t) = f(t)$ est exactement le graphe de f.

d. Vecteur vitesse et tangente.

C'est le vecteur $v(t) = (x'(t), y'(t))$ obtenu en dérivant les coordonnées par rapport au temps. On note aussi $v_x(t) = x'(t)$ et $v_y(t) = y'(t)$ ses composantes.

La *vitesse absolue* est la norme du vecteur vitesse, $\| v(t) \| = \sqrt{v_x(t)^2 + v_y(t)^2}$.

Si le vecteur $v(t_0)$ n'est pas nul, la droite passant par $(x(t_0), y(t_0))$ et de vecteur directeur $v(t_0)$ est (par définition) la *tangente* à la courbe. Si $v_x(t_0) = 0$, cette tangente est verticale. Si $v_y(t_0) = 0$, elle est horizontale.

En un point, où la vitesse est nulle, on est obligé de revenir à une définition plus géométrique. Soit $t_0 \in I$, et $(x(t_0), y(t_0))$ le point de la courbe associé. On suppose que, dans un petit intervalle $]t_0 - \alpha, t_0 + \alpha[$, l'application $t \mapsto (x(t), y(t)$ est injective. Considérons, pour tout t dans cet intervalle $(t \neq t_0)$, la droite passant par les deux points $(x(t_0), y(t_0))$ et $(x(t), y(t))$ et supposons que cette droite tend vers une limite quand t tend vers t_0 alors cette limite sera appelée la tangente en $(x(t_0), y(t_0))$. On retrouvera la définition précédente quand la vitesse est non-nulle en utilisant (développement de Taylor à l'ordre 1) que

$$x(t) = x(t_0) + (t - t_0)(x'(t_0) + \epsilon_1(t - t_0))$$

et que

$$y(t) = y(t_0) + (t - t_0)(y'(t_0) + \epsilon_2(t - t_0))$$

où ϵ_1 et ϵ_2 sont des fonctions tendant vers 0 en 0.

Notons aussi qu'il peut y avoir plusieurs tangentes en un point double, c'est à dire lorsqu'il existe deux points (au moins) t_0 et t_1 (avec $t_0 \neq t_1$) tels que $(x(t_0), y(t_0)) = (x(t_1), y(t_1))$.

e. Paramétrages particuliers.

Théorème 2.1.1
Supposons que pour tout t dans l'intervalle ouvert $]t_0, t_1[$, $v_x(t) > 0$. Alors la courbe obtenue lorsque t décrit l'intervalle fermé $[t_0, t_1]$ est le graphe d'une fonction f dérivable définie sur l'intervalle $[x(t_0), x(t_1)]$.

Il y a un énoncé analogue en échangeant les rôles des variables x et y.

Preuve du théorème.
Comme la fonction $t \mapsto x(t)$ est continue et strictement croissante sur $[t_0, t_1]$, c'est une bijection de $[t_0, t_1]$ sur $[x(t_0), x(t_1)]$. Notons $g : [x(t_0), x(t_1)] \to [t_0, t_1]$ la fonction réciproque. Elle est dérivable et strictement croissante (voir cours de première année).

Alors un point (x_1, y_1) se trouve sur la partie de la courbe décrite lorsque $t \in [t_0, t_1]$ si et seulement si $x_1 \in [x(t_0), x(t_1)]$ et $y_1 = y(g(x_1))$. Par conséquent, cette courbe est le graphe de la fonction composée $f : x \mapsto y(g(x))$.
■

Interprétation.

Tant que la vitesse ne s'annule pas, le tracé se ramène à celui de graphes de fonctions, tantôt y comme fonction de x, tantôt x comme fonction de y.

Procédé pratique.

On indique sur un même tableau les variations des fonctions $t \mapsto x(t)$ et $t \mapsto y(t)$. On place les points et les tangentes correspondant aux valeurs particulières de t (celles où l'une des dérivées s'annule). Pour chacun des intervalles du tableau, on trace, comme on sait le faire depuis le lycée, le graphe d'une fonction dont on connait le sens de variation et les tangentes aux extrémités.

2.1.2 Fonctions implicites

Le cercle centré en 0 et de rayon 1 est représenté par : $y^2 + x^2 = 1$. On peut essayer de paramétrer cette courbe par rapport à x. On trouve $y = \pm\sqrt{1 - x^2}$ avec $x \in [-1, +1]$. On observe d'une part qu'il y a deux branches de courbes, et que chacune des deux courbes paramétrées introduites n'est

pas différentiable aux points $x = -1$ et $x = 1$. Si on paramètre en prenant $x \in]-1, +1[$, on constate qu'on a paramétré le cercle moins deux points correspondant à $(-1, 0)$ et $(0, 1)$ dans $\mathbb{R}^2$.

On peut aussi essayer de paramétrer par y, en considérant $x = \pm\sqrt{1-y^2}$ avec $y \in]-1, +1[$. Il manque encore deux points ! Sur cet exemple on voit bien que l'on peut toujours "près" d'un point donné du cercle paramétrer le cercle, ou par la variable x ou par la variable y.

Plus généralement, c'est le cas pour les courbes définies comme les zéros d'une application f de classe C^1 de $\mathbb{R}^2$ dans $\mathbb{R}$, telle que $(\partial f/\partial x), (\partial f/\partial y)$ soit différent de $(0, 0)$ en tout point de la courbe $f(x, y) = 0$.

Localement (près de tout point de la courbe (x_0, y_0)), on peut, si par exemple la condition

$$(\partial f/\partial y)(x_0, y_0) \neq 0 \ ,$$

est vérifiée, trouver une fonction ϕ de classe C^1 définie dans un petit intervalle ouvert contenant x_0, telle que la courbe est décrite localement (c'est à dire à l'intérieur d'une petite boule contenant (x_0, y_0)) par $y = \phi(x)$.
C'est ce qui est communément appelé le théorème des fonctions implicites. De même, si $(\partial f/\partial x)(x_0, y_0) \neq 0$, on peut trouver une fonction ψ de classe C^1 définie dans un petit intervalle ouvert contenant y_0, telle que la courbe est décrite localement par $x = \psi(y)$.

La tangente en un point (x_0, y_0) de la courbe est la droite passant par (x_0, y_0) et orthogonale au vecteur $(\partial f/\partial x)(x_0, y_0), (\partial f/\partial y)(x_0, y_0)$.

Démontrons cette dernière assertion. Supposons par exemple $(\partial f/\partial y)(x_0, y_0) \neq 0$. Alors, la tangente est la droite passant par (x_0, y_0) et parallèle au vecteur vitesse $(1, \phi'(x_0))$. On doit donc juste démontrer que ce vecteur vérifie la condition d'orthogonalité :

$$(\partial f/\partial x)(x_0, y_0) + \phi'(x_0)(\partial f/\partial y)(x_0, y_0) = 0$$

avec $y_0 = \phi(x_0)$.

On observe maintenant qu'on a l'identité :

$$f(x, \phi(x)) = 0 \ , \ \forall x \in]x_0 - \alpha, x_0 + \alpha[\ .$$

Si on dérive cette identité par rapport à x, on obtient en utilisant les règles de dérivation d'une fonction composée et en observant que f et ϕ sont de classe C^1, l'identité

$$(\partial f/\partial x)(x, \phi(x)) + \phi'(x)(\partial f/\partial y)(x, \phi(x)) = 0 \ , \ \forall x \in]x_0 - \alpha, x_0 + \alpha[\ ,$$

qui donne le résultat recherché en $x = x_0$.

2.1.3 Longueur

a. Lignes polygonales

Une ligne polygonale est une application $t \mapsto (x(t), y(t))$ telle que les fonctions $t \mapsto x(t)$ et $t \mapsto y(t)$ soient continues et affines par morceaux. Autrement dit, l'intervalle de définition I est réunion d'intervalles $[t_i, t_{i+1}]$ sur lesquels les fonctions coordonnées sont de la forme $x(t) = x(t_i)+a_i(t-t_i)$, $y(t) = y(t_i) + b_i(t - t_i)$.

Chaque segment de la courbe a pour longueur

$$|t_{i+1} - t_i| \parallel (a_i, b_i) \parallel .$$

La longueur d'une ligne polygonale est la somme des longueurs des segments qui la composent. On peut l'écrire sous la forme

$$\text{longueur} = \int_I \parallel v(t) \parallel \, dt.$$

En effet, sur chaque intervalle $[t_i, t_{i+1}]$, le vecteur vitesse $v(t)$ est constant et vaut (a_i, b_i).

b. Définitions

Soit $t \mapsto (x(t), y(t))$ une courbe paramétrée de classe C^1 sur un intervalle I. On note $v(t)$ le vecteur vitesse. La *longueur* de la courbe est

$$\text{longueur} = \int_I \parallel v(t) \parallel \, dt.$$

On peut montrer que lorsqu'on approche la courbe par des lignes polygonales, la longueur converge.

Exemple

On considère le cercle unité du plan, paramétré par l'angle au centre :

$$x(t) = \cos t \ , \ y(t) = \sin t \ , \ t \in [0, 2\pi[\ .$$

Alors la vitesse absolue est constante, $\parallel v(t) \parallel = 1$, donc la longueur vaut 2π.

Si P_n est un polygone régulier à n côtés, inscrit dans le cercle unité, alors chaque côté de P_n est de longueur égale à $2\sin(\pi/n)$, donc $\text{longueur}(P_n) = 2n\sin(\pi/n)$ qui tend bien vers 2π quand n tend vers $+\infty$.

c. Changement de paramètrage

Changer de paramètrage sur une courbe, c'est remplacer t par $\tau = \phi(t)$ où ϕ est une bijection de I sur un intervalle J, dérivable, à dérivée continue

et partout strictement positive. La nouvelle courbe paramétrée est donnée par

$$x_1(\tau) = x(\phi^{-1}(\tau)) \ , \ y_1(\tau) = y(\phi^{-1}(\tau)) \ , \ \text{pour } \tau \in J \ .$$

Le tracé donne le même ensemble de points dans le plan.

Le nouveau vecteur vitesse $v_1 = (\frac{dx_1}{d\tau}, \frac{dy_1}{d\tau})$ est relié à $v = (\frac{dx}{dt}, \frac{dy}{dt})$ par

$$v(t) = \phi'(t) v_1(\phi(t)).$$

Autrement dit, la direction du vecteur vitesse en un point de la courbe ne dépend pas du choix de paramètrage (c'est la direction de la tangente), mais sa longueur, la vitesse absolue, en dépend.

Théorème 2.1.2
La longueur d'une courbe ne dépend pas du choix de paramètrage.

Preuve
On vérifie que :

$$\text{longueur} = \int_I \parallel v(t) \parallel \ dt = \int_I \parallel v_1(\phi(t)) \parallel \phi'(t)\, dt = \int_J \|v_1(\tau)\|\, d\tau = \text{longueur}_1 \ .$$

Ici on a utilisé la formule de changement de variable. ■

Exemple du cercle revisité
Retrouvons que le cercle unité a comme longueur 2π. Pour cela, nous utilisons une méthode de paramétrisation du cercle privé d'un point qui se généralise pour n'importe quelle conique. On fixe un point du cercle, soit $(-1, 0)$ et l'intersection de la droite de pente t passant par ce point, coupe le cercle unité centré en 0 au point $x(t) = \frac{1-t^2}{1+t^2}$, $y(t) = \frac{2t}{1+t^2}$ pour $t \in \mathbb{R}$. C'est bien une paramétrisation du cercle unité privé du point $(-1, 0)$. On calcule le vecteur vitesse

$$v(t) = (\frac{-4t}{(1+t^2)^2}, \frac{2-2t^2}{(1+t^2)^2})$$

puis sa norme

$$\parallel v(t) \parallel = \frac{2}{1+t^2}$$

Pour tout $A > 0$, la longueur de la partie de cette courbe paramétrée par $[-A, A]$ vaut

$$\int_{-A}^{A} \frac{2dt}{1+t^2} = 4\text{Arctan(A)}$$

qui tend vers 2π lorsque A tend vers $+\infty$.

d. Abscisse curviligne.

Définition 2.1.3
On dit qu'une courbe est paramétrée par son abscisse curviligne si le vecteur vitesse est unitaire, i.e. si sa vitesse absolue est constante et égale à 1.

Si une courbe est paramétrée par son abscisse curviligne, alors la longueur de la portion de courbe entre les points correspondant aux paramètres t_0 et t_1 est $|t_0 - t_1|$.

Exemple
Sur le cercle unité, paramétré par $[0, 2\pi] \ni t \mapsto (\cos t, \sin t)$, t est une abscisse curviligne. l'angle au centre est une abscisse curviligne.

Théorème 2.1.4
Toute courbe paramétrée dont le vecteur vitesse est continu et ne s'annule pas peut être reparamétrée par son abscisse curviligne.

Preuve
Fixons une origine $t_0 \in I$. Pour $t \in I$, on pose

$$\phi(t) = \int_{t_0}^{t} \parallel v(u) \parallel \, du.$$

Alors ϕ est dérivable et sa dérivée $\phi'(t) = \parallel v(t) \parallel$ est continue et partout strictement positive. Par conséquent, c'est une bijection sur un intervalle J de $\mathbb{R}$. Le nouveau paramètrage $\tau = \phi(t)$ est une abscisse curviligne. En effet, dans ce paramètrage, la vitesse absolue vaut

$$v_1(\tau) = v_1(\phi(t)) = (\phi'(t))^{-1} v(t)$$

qui est de norme 1 par construction.
■

2.1.4 Courbes dans $\mathbb{R}^3$

En dehors du tracé, rien n'est à changer.

2.2 Intégrales curvilignes

Lorsqu'on déplace un point matériel dans un champ de force, le travail mécanique fournit par le champ de force est donné par une intégrale curviligne le long de la trajectoire.

On se propose de démontrer la formule de Green-Riemann qui relie intégrale curviligne et intégrale double.

2.2.1 Champ de vecteurs et circulation

Un champ de vecteurs dans le plan ou l'espace consiste à se donner en chaque point (x, y) de $\mathbb{R}^2$ ou d'un ouvert Ω de $\mathbb{R}^2$ (resp. (x, y, z)) un vecteur $w(x, y)$ (resp. $w(x, y, z)$).

On supposera toujours que l'application $(x, y) \mapsto w(x, y) \in \mathbb{R}^2$ est de classe C^0 (c'est à-dire continu) sur Ω. On aura souvent besoin qu'il soit de classe C^1, c'est à dire que les deux composantes w_1 et w_2 de w définissent des applications de classe C^1 de Ω dans $\mathbb{R}$. Dans les applications Ω peut être $\mathbb{R}^2$ tout entier, un disque ouvert, $R^2 \setminus 0$, un carré .....

Exemple : Un champ de forces.
On sait alors que le mouvement d'un point de masse m soumis à cette force est connu dès que l'on connait la position et la vitesse à un instant t_0. On a alors à résoudre :

$$md^2x/dt^2 = F_1(x(t), y(t)) \ ,$$
$$md^2y/dt^2 = F_2(x(t), y(t))$$

avec comme condition initiale :

$$(x(t_0), y(t_0)) = (x_0, y_0) \ , \ (x'(t_0), y'(t_0)) = v_0 \ .$$

C'est un moyen très courant de rencontrer des courbes paramétrées!!

Exemple : le *gradient* d'une fonction u.
On rappelle que le gradient d'une fonction de deux variables u est le vecteur dont les composantes en coordonnées cartésiennes orthonormées sont les dérivées partielles,

$$\nabla u = (\tfrac{\partial u}{\partial x} \ , \ \tfrac{\partial u}{\partial y})$$

et idem en dimension 3. Dans la suite, on se place en dimension 2. On ne mentionne la dimension 3 que lorsque la généralisation ne va pas de soi. On a vu précédemment que, dans le cas de la dimension 2, ∇f (ou grad f) détermine la normale à la courbe $f = 0$.

a. Définition de la circulation

Soit $t \mapsto c(t) = (x(t)), y(t))$, $t \in I$ une courbe paramétrée de classe C^1 (son vecteur vitesse $v(t)$ est continu). Soit $(x, y) \mapsto w(x, y)$ un champ de vecteurs continu. La circulation de w le long de la courbe c est définie par :

$$\text{circulation} = \int_I \langle w(c(t)), v(t)\rangle \, dt.$$

Exemple où on se ramène à une notion connue.

Posons $w(x, y) = (y, 0)$. Soit f une fonction dérivable sur un intervalle I. Son graphe $t \mapsto (t, f(t))$, $t \in I$ est une courbe paramétrée, et la circulation du champ w le long de cette courbe vaut $\displaystyle\int_I f(t)\, dt$.

Théorème 2.2.1 .
La circulation d'un champ de vecteur le long d'une courbe ne dépend pas du paramétrage choisi sur la courbe.

Preuve.
On a déjà vu ce qu'était un "bon" changement de paramètrage. On remplace le paramètre t par $\tau = \phi(t)$, on supppose que ϕ est une bijection sur son image, de classe C^1 ainsi que son inverse, et que $\phi'(t) > 0$.

On note $c_1(\tau) = c(t)$. Le vecteur vitesse est changé en $v_1(\tau) = v(t)/\phi'(t)$. Alors

$$\begin{aligned}
\text{circulation}_1 &= \int_J \langle w(c_1(\tau)), v_1(\tau)\rangle \, d\tau \\
&= \int_I \langle w(c_1(\phi(t))), v_1(\phi(t))\rangle \phi'(t)\, dt \\
&= \int_I \langle w(c(t)), v(t)\rangle \, dt \\
&= \text{circulation}.
\end{aligned}$$

■

Remarque 2.2.2 (Changement d'orientation) .
Considérons le changement de paramétrage $t \mapsto -t$. Ce n'est pas un "bon" changement de paramétrage. La courbe est décrite dans le sens opposé. Le calcul montre alors que la circulation est transformée en son opposé!! Le même calcul montre que la longueur n'est pas modifiée.

Corollaire 2.2.3 .
Soit c une courbe paramétrée par son abscisse curviligne s. Soit $u(s)$ le vecteur unitaire tangent à c. Alors la circulation d'un champ de vecteur w le long de c s'écrit

$$\int \langle w, u\rangle(c(s))\, ds\ .$$

b. Cas des champs de vecteurs dérivant d'un potentiel

Théorème 2.2.4
Soit u une fonction, et $t \mapsto c(t)$, $t \in I$, une courbe paramétrée. Pour tous t_0 et $t_1 \in I$,

$$\text{circulation}(\nabla u, c[t_0, t_1]) = u(c(t_1)) - u(c(t_0)).$$

Autrement dit, la circulation d'un champ de vecteurs qui dérive d'un potentiel ne dépend que de l'état initial et de l'état final, et non du chemin choisi.
Par exemple, lorsqu'un point matériel se déplace dans un potentiel U (i.e $F = -\nabla U$), le travail fourni par la force est égale à la variation de l'énergie potentiel entre l'état final et l'état initial.

2.2.2 Formes différentielles de degré 1

a. Définition d'une forme différentielle.

Une forme différentielle de degré 1 en deux variables est une expression de la forme $\alpha = P(x, y)\, dx + Q(x, y)\, dy$, où P et Q sont deux fonctions continues (au moins) sur $\mathbb{R}^2$. On écrit aussi que α est une 1-forme[1].

On peut ajouter deux 1-formes de manière naturelle :

$$\alpha_1 + \alpha_2 = (P_1(x, y) + P_2(x, y))dx + (Q_1(x, y) + Q_2(x, y))dy\ .$$

On peut aussi multiplier une 1-forme par une fonction $f(x, y)$ en écrivant :

$$f \cdot \alpha = (fP)(x, y)dx + (fQ)(x, y)dy\ .$$

Ces notations seront moins mystérieuses si on considère l'**exemple** de ce qu'on appelle la différentielle totale d'une fonction u :
Si u est de classe C^1, on note

$$du = \frac{\partial u}{\partial x}dx + \frac{\partial u}{\partial y}dy\ .$$

[1]On rencontre aussi naturellement en Physique ou en Mathématiques des p-formes mais on n'en parlera pas dans ce cours.

On a donc ici

$$P(x,y) = \frac{\partial u}{\partial x}(x,y)\ ,\ Q(x,y) = \frac{\partial u}{\partial y}(x,y)\ .$$

Les deux cas de base sont alors donnés par les fonctions $u(x,y) = x$ et $v(x,y) = y$, donnant lieu aux deux 1-formes dx et dy. L'addition et la multiplication par des fonctions permettent alors de construire toutes les 1-formes à partir de dx et dy.

Remarque 2.2.5
Si u et v sont de classe C^1, on a

$$d(uv) = udv + vdu\ .$$

Exemple 2.2.6
La 1-forme $\alpha = y\,dx$ n'est pas la différentielle totale d'une fonction (voir plus loin).

Définition 2.2.7
L'intégrale curviligne d'une forme différentielle $\alpha = P(x,y)\,dx + Q(x,y)\,dy$ le long d'une courbe c est

$$\int_c \alpha = \int_I (P(c(t))x'(t) + Q(c(t))y'(t))\,dt.$$

Exemple :
L'intégrale de la forme différentielle $\alpha = y\,dx$ le long du graphe d'une fonction $f : t \mapsto (t, f(t))$, $t \in I$, vaut $\displaystyle\int_I f(t)\,dt$.

b. Lien avec la circulation

A chaque forme différentielle de degré 1 $\alpha = P(x,y)\,dx + Q(x,y)\,dy$ correspond le champ de vecteur $w(x,y) = (\,P(x,y), Q(x,y)\,)$, de sorte que la notion d'intégrale curviligne correspond à la notion de circulation et celle de différentielle totale à la notion de gradient. Attention, cette correspondance dépend du choix de coordonnées.

C'est d'ailleurs uniquement dans le contexte où on a à changer de coordonnées dans un calcul de circulation que le point de vue "formes différentielles" sera utile dans le cadre de ce cours.

Notons que, comme on l'a vu dans le cas de la circulation d'un champ de vecteurs l'intégrale d'une 1-forme différentielle ne dépend pas du paramétrage.

c. Changement de coordonnées

Pour changer de coordonnées dans une forme différentielle, on substitue les nouvelles coordonnées aux anciennes, comme suit. Soit $(x, y) = (\theta_1(\tilde{x}, \tilde{y}), \theta_2(\tilde{x}, \tilde{y}),$ le changement de variable. On suppose que c'est un "bon" changement de variables. On entend par là que l'application $(\tilde{x}, \tilde{y}) \mapsto (x, y) = \theta(\tilde{x}, \tilde{y})$ est bijective, de classe C^1, et que son inverse a les mêmes propriétés.
On se laisse "porter" par les notations et on obtient :

$$\begin{aligned} dx = d\theta_1 &= (\partial\theta_1/\partial\tilde{x})\ d\tilde{x} + (\partial\theta_1/\partial\tilde{y})d\tilde{y}\ , \\ dy = d\theta_2 &= (\partial\theta_2/\partial\tilde{x})\ d\tilde{x} + (\partial\theta_2/\partial\tilde{y})d\tilde{y}\ . \end{aligned}$$

Il faut maintenant penser ainsi. Il y a un objet "α" qui s'écrivait dans les coordonnées (x, y) sous la forme : $\alpha = P(x, y)dx + Q(x, y)dy$ et qui s'écrira sous la forme $\alpha = \tilde{P}(\tilde{x}, \tilde{y})d\tilde{x} + \tilde{Q}(\tilde{x}, \tilde{y})d\tilde{y}$.

Le calcul de la paire $\tilde{P}, \tilde{Q}$ est immédiatement obtenu en utilisant les formules ci-dessus. Décrivons le calcul plus précisément. On a

$$\begin{aligned} \alpha &= P(x, y)dx + Q(x, y)dy \\ &= P(\theta(\tilde{x}, \tilde{y}))\ ((\partial\theta_1/\partial\tilde{x})d\tilde{x} + (\partial\theta_1/\partial\tilde{y})d\tilde{y}) \\ &\quad +Q(\theta(\tilde{x}, \tilde{y}))\ ((\partial\theta_2/\partial\tilde{x}))d\tilde{x} + (\partial\theta_2/\partial\tilde{y})d\tilde{y})\ . \end{aligned}$$

En réordonnant, on trouve :

$$\begin{aligned} \tilde{P}(\tilde{x}, \tilde{y}) &= P(\theta(\tilde{x}, \tilde{y}))(\partial\theta_1/\partial\tilde{x}) + Q(\theta(\tilde{x}, \tilde{y}))(\partial\theta_2/\partial\tilde{x})\ , \\ \tilde{Q}(\tilde{x}, \tilde{y}) &= P(\theta(\tilde{x}, \tilde{y}))(\partial\theta_1/\partial\tilde{y}) + Q(\theta(\tilde{x}, \tilde{y}))\ (\partial\theta_2/\partial\tilde{y})\ . \end{aligned}$$

Il n'y a rien à apprendre par coeur ; il faut plutôt comprendre comment on fait ce calcul naturellement.

Exemple.
Regardons plus concrètement le cas du passage en coordonnées polaires

$$x = r\cos\theta\ ,\ y = r\sin\theta\ .$$

On notera au passage (sans s'en inquiéter outre mesure) que ce n'est pas tout à fait un bon changement de variable dans $\mathbb{R}^2$ (il faut enlever une semi-droite issue de l'origine). Etant donné $\alpha = P(x, y)\,dx + Q(x, y)\,dy$, on différentie

$$dx = \cos\theta\,dr - r\sin\theta\,d\theta, \quad dy = \sin\theta\,dr + r\cos\theta\,d\theta, \tag{2.1}$$

et on substitue

$$\begin{aligned} \alpha &= (\cos\theta\,P(r\cos\theta, r\sin\theta) + \sin\theta\,Q(r\cos\theta, r\sin\theta))\,dr \\ &\quad +r(-\sin\theta\,P(r\cos\theta, r\sin\theta) + \cos\theta\,Q(r\cos\theta, r\sin\theta))\,d\theta. \end{aligned}$$

Exemple 2.2.8
On a :

$$xdx + ydy = rdr \ , \ -ydx + xdy = r^2 d\theta \ .$$

Pour la première, on peut aussi remarquer que :

$$xdx + ydy = \frac{1}{2}d(x^2 + y^2) = \frac{1}{2}d(r^2) = rdr \ .$$

Théorème 2.2.9 .
L'intégration des formes différentielles de degré 1 *est invariante par changement de coordonnées.*

Preuve.
On se contente de faire le cas du changement en coordonnées polaires (le cas général n'est pas différent).
En effet

$$P(r\cos\theta, r\sin\theta)(\cos\theta\tfrac{\partial r}{\partial t} - r\sin\theta\tfrac{\partial\theta}{\partial t}) + Q(r\cos\theta, r\sin\theta)(\sin\theta\tfrac{\partial r}{\partial t} + r\cos\theta\tfrac{\partial\theta}{\partial t})$$
$$= P(x,y)\tfrac{dx}{dt} + Q(x,y)\tfrac{dy}{dt}.$$

■

d. Formes différentielles exactes et fermées

Définition 2.2.10
On dit qu'une forme différentielle de degré 1 α *définie sur un ouvert* D *de* $\mathbb{R}^2$ *est* exacte *si c'est la différentielle totale d'une fonction* u *de classe* C^1 *définie sur* D.

Une condition nécessaire pour que $\alpha = P(x,y)\,dx + Q(x,y)\,dy$ (avec des coefficients de classe C^1) soit exacte est que

$$\frac{\partial P}{\partial y} = \frac{\partial Q}{\partial x}$$

en chaque point de D.
En effet, si $\alpha = du$, alors $P = \dfrac{\partial u}{\partial x}$ et $Q = \dfrac{\partial u}{\partial x}$. Donc

$$\frac{\partial P}{\partial y} = \frac{\partial^2 u}{\partial y \partial x} = \frac{\partial^2 u}{\partial x \partial y} = \frac{\partial Q}{\partial x}.$$

Définition 2.2.11
Une forme différentielle α qui satisfait en tout point

$$\frac{\partial P}{\partial y} = \frac{\partial Q}{\partial x}$$

est dite fermée.

Théorème 2.2.12 .
Soit D une partie convexe[2] du plan. Une forme différentielle définie sur D est exacte si et seulement si elle est fermée.

Nous démontrerons qu'une forme fermée dans un convexe est exacte après la démonstration de la formule de Green-Riemann.

Exemple

La forme $\alpha = d\theta = \dfrac{x\,dy - y\,dx}{x^2 + y^2}$ définie sur le plan privé de l'origine est fermée mais non exacte.

Corollaire 2.2.13 .
Soit $(x, y) \mapsto w(x, y) = (\, P(x, y)\ ,\ Q(x, y)\,)$ un champ de vecteurs défini sur une partie convexe D du plan. Alors w dérive d'un potentiel défini sur D si et seulement si

$$\frac{\partial P}{\partial y} = \frac{\partial Q}{\partial x}$$

en tout point de D.

e. Rotationnel

Définition 2.2.14
Soit $(x, y, z) \mapsto w(x, y, z) = (\, P(x, y, z)\ ,\ Q(x, y, z)\ ,\ R(x, y, z)\,)$ un champ de vecteurs suffisamment régulier. Son rotationnel est le champ de vecteurs

$$rot\ w = \nabla \wedge w = (\, -\tfrac{\partial Q}{\partial z} + \tfrac{\partial R}{\partial y}, \tfrac{\partial P}{\partial z} - \tfrac{\partial R}{\partial x}, -\tfrac{\partial P}{\partial y} + \tfrac{\partial Q}{\partial x}\,)\,.$$

[2]On rappelle qu'on dit que D est convexe, si pour tous z et z' dans D, le segment de droite $[z, z']$ est contenu dans D. Un disque par exemple est convexe. Par contre $\mathbb{R}^2 \setminus \{0, 0\}$ n'est pas convexe.

En dimension 2, le rotationnel d'un champ de vecteurs $w = (w_1, w_2)$ est simplement donné par :

$$\text{rot } w = \partial w_2/\partial x - \partial w_1/\partial y \ .$$

La correspondance avec la définition en dimension 3 est la suivante. On regarde le vecteur dans $\mathbb{R}^3$: $W(x, y, z) = (w_1(x, y), w_2(x, y), 0)$ et on a alors :

$$\text{rot } W = (0, 0, \text{rot } w) \ .$$

Comme en deux variables, une condition nécessaire pour que w dérive d'un potentiel est que son rotationnel soit nul en tout point.

Théorème 2.2.15 .
Soit $(x, y, z) \mapsto w(x, y, z)$ un champ de vecteurs défini sur une partie convexe D de l'espace. Alors w dérive d'un potentiel défini sur D si et seulement si son rotationnel est nul en tout point de D.

f. Formule de Green-Riemann.

Si α est exacte sur D, alors, pour toute courbe c fermée contenue dans D, $\displaystyle\int_c \alpha = 0$. En effet, comme $\alpha = du$, $\displaystyle\int_c \alpha$ est la variation de u entre les extrémités, donc nulle si la courbe est fermée. (voir ce que l'on a vu concernant la circulation d'un champ de vecteur qui est le gradient d'une fonction).

En général, l'intégrale d'une forme différentielle le long d'une courbe fermée qui borde un domaine s'écrit comme une intégrale double sur le domaine.

Théorème 2.2.16 .
Soit $\alpha = P(x, y)\, dx + Q(x, y)\, dy$ une forme différentielle de degré 1. Soit c une courbe fermée sans point double, qui entoure un domaine[3] D. On suppose que D est à gauche lorsqu'on parcourt c. Alors

$$\int_c \alpha = \int_D (\frac{\partial Q}{\partial x} - \frac{\partial P}{\partial y})\, dx\, dy.$$

[3]On dit que D est un domaine s'il est ouvert et si pour tous z et z' dans D, il existe une ligne polygonale contenue dans D joignant z et z'

Preuve.

Pour simplifier, on suppose D convexe. Notons I la projection du domaine D sur l'axe Ox. Comme D est convexe, il est défini par des inégalités $f_1(x) \leq y \leq f_2(x)$ où f_1 et f_2 sont des fonctions continues sur I. On calcule (en utilisant le théorème de Fubini) l'intégrale double :

$$\begin{aligned}\int_{\{x\in I,\ f_1(x)\leq y\leq f_2(x)\}} \frac{\partial P}{\partial y}(x,y)\,dx\,dy &= \int_I dx \int_{f_1(x)}^{f_2(x)} \frac{\partial P}{\partial y}(x,y)\,dy \\ &= \int_I (P(x,f_2(x)) - P(x,f_1(x)))\,dx \\ &= -\int_c P\,dx.\end{aligned}$$

De même (en échangeant le rôle de x et y), on trouve

$$\int_D \frac{\partial Q}{\partial x}\,dx\,dy = \int_c Q\,dy\ .$$

■

Cas des formes fermées

On voit que l'intégrale d'une forme fermée (définie sur un convexe) sur une courbe fermée sans point double est nulle.

Application : Démonstration du Théorème 2.2.12.

On peut maintenant montrer qu'une forme fermée dans un convexe est exacte. Soit z_0 un point de ce convexe (ouvert !). Alors, pour tout $z = (x, y)$ dans ce convexe, je pose :

$$U(z) = \int_{[z_0,z]} \alpha\ .$$

Ici $[z_0, z]$ désigne la courbe paramétrée :

$$[0,1] \ni t \mapsto (1-t)z_0 + tz\ .$$

On peut remarquer que le théorème de Green-Riemann nous dit en particulier que, pour toute courbe paramétrée γ joignant z_0 à z, dont l'image est dans D, on a :

$$\int_\gamma \alpha + \int_{[z,z_0]} \alpha = 0\ .$$

La courbe paramétrée constituée par la courbe paramétrée γ suivie de la courbe paramétrée $[z, z_0]$ est en effet une courbe fermée.

Si on se rappelle (voir ce que l'on a dit sur le changement d'orientation) que l'on a toujours :

$$\int_{[z,z_0]} \alpha = -\int_{[z_0,z]} \alpha \ ,$$

on obtient que

$$U(z) = \int_\gamma \alpha \ .$$

La fonction U ne dépend pas du chemin choisi joignant z_0 à z.

Il reste à montrer que la différentielle totale de U est α. En revenant à la définition, il faut montrer que, en notant $\alpha = P\,dx + Q\,dy$, on a :

$$\partial U/\partial x = P \text{ et } \partial U/\partial y = Q \ .$$

Montrons la première relation, si on revient à la définition d'une dérivée partielle, on doit montrer que pour tout $(x, y) \in D$, la limite

$$\lim_{h\to 0} \frac{U(x+h, y) - U(x, y)}{h}$$

existe et est égale à $P(x, y)$.

On remarque maintenant que, grâce au théorème de Green-Riemann, on a :

$$\int_{[z_0,z]} \alpha + \int_{[z,z+(h,0)]} \alpha + \int_{[z+(h,0),z_0]} \alpha = 0 \ .$$

On peut réécrire cette identité sous la forme :

$$U(z + (h, 0)) - U(z) = \int_{[z,z+(h,0)]} \alpha \ .$$

Il est maintenant temps de revenir à la définition de l'intégrale curviligne. On a :

$$\int_{[z,z+(h,0)]} \alpha = h \int_0^1 P(x + th, y)dt \ .$$

Le dernier point est alors de montrer que, si P est continu, alors

$$\lim_{h\to 0} \int_0^1 P(x + th, y)\ dt = P(x, y) \ .$$

On a juste besoin du lemme suivant :

Lemme 2.2.17 .
Soit f une fonction continue sur $[-\epsilon_0, \epsilon_0]$, telle que $f(0) = 0$, alors

$$\lim_{h \to 0} \int_0^1 f(th)dt = O \ .$$

Ce lemme résulte immédiatement de la continuité de f et de la propriété de l'intégrale d'une fonction continue g :

$$| \int_{t_0}^{t_1} g(t)dt| \leq |t_1 - t_0| \sup_{t \in [t_0, t_1]} |g(t)| \ .$$

Exercice 2.2.18

1. *Calcul de l'aire en coordonnées polaires (en intégrant $\frac{1}{2} r^2 \, d\theta$).*
2. *Etude de la forme $d\theta$.*

2.3 Surfaces paramétrées et Intégrales de surface

2.3.1 Rappels de géométrie euclidienne.

Le produit scalaire de deux vecteurs $w = (x, y, z)$ et $w' = (x', y', z')$ dans $\mathbb{R}^3$ est défini par :

$$w \cdot w' = xx' + yy' + zz' \ . \tag{2.2}$$

On l'a aussi noté auparavant $\langle w \,|\, w' \rangle_{\mathbb{R}^3}$.
Il est nul si et seulement si les vecteurs sont orthogonaux. Il satisfait

$$w \cdot (w' + w'') = w \cdot w' + w \cdot w'' \tag{2.3}$$

et

$$w \cdot w = |w|^2 \ .$$

Le produit vectoriel de deux vecteurs $w = (x, y, z)$ et $w' = (x', y', z')$ est le vecteur

$$w \wedge w' = (yz' - y'z, -xz' + x'z, xy' - x'y) \ . \tag{2.4}$$

Il est nul si et seulement si les vecteurs sont colinéaires. Il satisfait des propriétés de bilinéarité, en particulier

$$w \wedge (w' + w'') = w \wedge w' + w \wedge w'' \ ,$$

et d'antisymétrie

$$w \wedge w' = -w' \wedge w \ .$$

Enfin, si w et w' sont orthogonaux, alors

$$|w \wedge w'| = |w||w'| \ .$$

2.3.2 Surfaces paramétrées

Définition 2.3.1 .
Une surface paramétrée dans l'espace est la donnée de trois fonctions définies sur un domaine D du plan,

$$(u, v) \mapsto s(u, v) = \begin{pmatrix} x(u, v) \\ y(u, v) \\ z(u, v) \end{pmatrix} .$$

On supposera toujours que les fonctions $(u, v) \mapsto x(u, v)$, $(u, v) \mapsto y(u, v)$ et $(u, v) \mapsto z(u, v)$ admettent des dérivées partielles continues. Autrement dit, l'application (u, v) est de classe C^1 de D dans $\mathbb{R}^3$.

Définition 2.3.2 *Plan tangent.*
Lorsque les vecteurs

$$\frac{\partial s}{\partial u}(u,v) = \begin{pmatrix} \frac{\partial x}{\partial u}(u,v) \\ \frac{\partial y}{\partial u}(u,v) \\ \frac{\partial z}{\partial u}(u,v) \end{pmatrix} \quad et \quad \frac{\partial s}{\partial v}(u,v) = \begin{pmatrix} \frac{\partial x}{\partial v}(u,v) \\ \frac{\partial y}{\partial v}(u,v) \\ \frac{\partial z}{\partial v}(u,v) \end{pmatrix}$$

sont linéairement indépendants, le plan qu'ils engendrent est le plan tangent à la surface au point $s(u,v)$.

On remarque que ce plan contient le vecteur vitesse de toute courbe tracée sur la surface et passant par ce point.
Leur produit vectoriel

$$\frac{\partial s}{\partial u}(u,v) \wedge \frac{\partial s}{\partial v}(u,v)$$

est un vecteur normal à la surface au point $s(u,v)$. Il est orthogonal au vecteur vitesse de toute courbe tracée sur la surface et passant par ce point.

Définition 2.3.3
Le vecteur unitaire

$$\nu(u,v) = \frac{\frac{\partial s}{\partial u}(u,v) \wedge \frac{\partial s}{\partial v}(u,v)}{|\frac{\partial s}{\partial u}(u,v) \wedge \frac{\partial s}{\partial v}(u,v)|}$$

s'appelle la normale unitaire orientée au point $s(u,v)$.

Paramétrisation par rapport à une projection .
Un cas particulier de surface paramétrée est le cas où l'on a :

$$x = u \ , \ y = v \ , \ z = f(u,v) \ ,$$

qu'on peut bien sûr décrire plus simplement :

$$z = f(x,y) \ ,$$

où on précise : $(x,y) \in D$ si D est différent de $\mathbb{R}^2$.

Surfaces définies implicitement .
Plus généralement, une surface peut être décrite comme l'ensemble S des zéros d'une fonction de classe C^1 h de $\mathbb{R}^3$ (ou d'un ouvert de $\mathbb{R}^3$) dans $\mathbb{R}$, telle que $\nabla h \neq 0$ pour $(x,y,z) \in S$. Il faut juste savoir que l'espace tangent en un point (x,y,z) de S est le plan passant par ce point et orthogonal à

$(\nabla h)(x,y,z)$. Notons que ∇h détermine une orientation de la surface.
Un théorème (théorème des fonctions implicites) permet de montrer que si par exemple $h(x_0,y_0,z_0)=0$ et $(\partial_z h)(x_0,y_0,z_0)\neq 0$ alors on peut paramétrer dans une boule assez petite contenant (x_0,y_0,z_0) la surface par (x,y) comme au paragraphe précédent.

Exemple 2.3.4
L'équation

$$h(x,y,z)=x^2+y^2+z^2-1\ ,$$

définit une sphère.

2.3.3 Notion d'aire sur une surface

Aire des parallélogrammes .

L'aire d'un parallélogramme est le produit de la base par la hauteur. En voici une expression vectorielle. Si les sommets du parallélogramme sont 0, a, b et $a+b$, alors

$$\text{Aire} = |a\wedge b|.$$

En effet, soit c la projection de b sur la droite engendrée par a, i.e. c est colinéaire à a et $b-c$ est orthogonal à a. Alors $|a\wedge b| = |a\wedge(b-c)| = |a||b-c| =$ base$\times$hauteur.

Heuristique .

Si $(u,v)\mapsto s(u,v)$ est une surface paramétrée, l'image d'un rectangle de sommets (u,v) et dont les côtés δu et δv sont très petits est approximativement un parallélogramme construit sur les vecteurs $\dfrac{\partial s}{\partial u}(u,v)\delta u$ et $\dfrac{\partial s}{\partial v}(u,v)\delta v$, donc son aire est voisine de

$$|\frac{\partial s}{\partial u}(u,v)\wedge\frac{\partial s}{\partial v}(u,v)|\,\delta u\,\delta v.$$

Définition de l'aire .
Cela motive la définition suivante.

Définition 2.3.5 .
L'aire d'une surface paramétrée est donnée par l'intégrale double

$$\text{Aire} = \int_D |\frac{\partial s}{\partial u}(u,v)\wedge\frac{\partial s}{\partial v}(u,v)|\,du\,dv.$$

Exercice 2.3.6
Calculer l'aire du triangle de sommets $a = (1,0,0)$, $b = (0,-1,2)$ *et* $c = (0,2,1)$.

Solution.
On utilise la paramétrisation $s(u,v) = a+u(b-a)+v(c-a)$ où $u \geq 0$, $v \geq 0$, $u+v \leq 1$. On calcule

$$\frac{\partial s}{\partial u}(u,v) \wedge \frac{\partial s}{\partial v}(u,v) = (b-a) \wedge (c-a) = \begin{pmatrix} -5 \\ -1 \\ -3 \end{pmatrix}.$$

Sa norme est constante et vaut $\sqrt{35}$. On l'intègre sur un triangle d'aire $\frac{1}{2}$. L'aire cherchée vaut donc $\sqrt{35}/2$.

Exercice 2.3.7
Calculer l'aire de la sphère unité, en utilisant les coordonnées sphériques

$$s(\theta,\phi) = \begin{pmatrix} \sin\theta\sin\phi \\ \sin\theta\cos\phi \\ \cos\theta \end{pmatrix}, \quad \theta \in]0,\pi[, \quad \phi \in [0,2\pi[.$$

Solution.
On note que le paramétrage ci-dessus paramètre la sphère moins les deux poles (il faudrait aussi enlever $\phi = 0$ pour avoir un bon paramétrage) mais ceci n'intervient pas dans des calculs d'aire. On calcule :

$$\frac{\partial s}{\partial \theta} \wedge \frac{\partial s}{\partial \phi} = \begin{pmatrix} \cos\theta\sin\phi \\ \cos\theta\cos\phi \\ -\sin\theta \end{pmatrix} \wedge \begin{pmatrix} \sin\theta\cos\phi \\ -\sin\theta\sin\phi \\ 0 \end{pmatrix} = \begin{pmatrix} -\sin^2\theta\sin\phi \\ -\sin^2\theta\cos\phi \\ -\cos\theta\sin\theta \end{pmatrix}$$

dont la norme vaut $\sin\theta$. (Il y a un petit problème aux poles (les deux vecteurs ne sont plus indépendants) qui n'a pas de conséquence pour le calcul de l'aire. Par conséquent

$$\text{Aire} = \int_0^{2\pi} d\phi \int_0^{\pi} \sin\theta \, d\theta = 4\pi.$$

Invariance .
Comme dans le cas de la longueur d'une courbe, on peut montrer le :

Théorème 2.3.8 .
L'aire ne dépend pas du choix de paramétrage.

Preuve
Changer de paramétrage, c'est remplacer (u, v) par

$$(u', v') = \theta(u, v) \ , \tag{2.5}$$

où on suppose que θ est de classe C^1 et qu'il admet un inverse de classe C^1 $\widehat{\theta}$.
On peut alors définir le nouveau paramétrage de la surface, en posant

$$s_1(u', v') = s(\widehat{\theta}(u', v')) \ ,$$

et on a inversement

$$s(u, v) = s_1(\theta(u, v)) \ .$$

On se contente souvent d'écrire

$$s(u, v) = s_1(u', v') \ ,$$

en sous-entendant la relation (2.5).

Ci-dessous on utilise la notation

$$\widehat{\theta}(u', v') = (u(u', v'), v(u', v'))$$

qui peut poser problème en première lecture mais qui rend l'écriture assez automatique.

D'après la formule de dérivation des fonctions composées, le nouveau paramétrage $s_1(u', v') = s(u, v)$ satisfait

$$\frac{\partial s_1}{\partial u'} = \frac{\partial s}{\partial u}\,\frac{\partial u}{\partial u'} + \frac{\partial s}{\partial v}\,\frac{\partial v}{\partial u'} \ , \quad \frac{\partial s_1}{\partial v'} = \frac{\partial s}{\partial u}\,\frac{\partial u}{\partial v'} + \frac{\partial s}{\partial v}\,\frac{\partial v}{\partial v'} \ .$$

Il vient, en utilisant les propriétés du produit vectoriel,

$$\frac{\partial s_1}{\partial u'} \wedge \frac{\partial s_1}{\partial v'} = \left(\frac{\partial s}{\partial u} \wedge \frac{\partial s}{\partial v}\right)\left(\frac{\partial u}{\partial u'}\,\frac{\partial v}{\partial v'} - \frac{\partial u}{\partial v'}\,\frac{\partial v}{\partial u'}\right)$$

et on conclut avec la formule de changement de variable dans les intégrales doubles :
Pour passer du calcul de l'intégrale dans les coordonnées (u, v) au calcul de l'intégrale dans les coordonnées (u', v'), il faut remplacer $du\,dv$ par

$$\left|\left(\frac{\partial u}{\partial u'}\,\frac{\partial v}{\partial v'} - \frac{\partial u}{\partial v'}\,\frac{\partial v}{\partial u'}\right)\right| du'\,dv' \ .$$

Autrement dit pour toutes fonctions continues f (définie sur D) et g définie sur D' telles que $f(u,v) = g(u',v')$ avec $(u',v') = \theta(u,v)$, on a

$$\int\int_D f(u,v)dudv = \int\int_{D'} g(u',v')|\left(\frac{\partial u}{\partial u'}\,\frac{\partial v}{\partial v'} - \frac{\partial u}{\partial v'}\,\frac{\partial v}{\partial u'}\right)|\,du'\,dv'\,.$$

■

2.3.4 Intégrales sur des surfaces, Flux

Définition 2.3.9 .
Soit $(x,y,z) \mapsto w(x,y,z)$ un champ de vecteurs continu sur $\Omega \subset \mathbb{R}^3$. Soit $D \ni (u,v) \mapsto s(u,v) \in \Omega$ une surface paramétrée que l'on notera $\mathcal{S}$. Le flux du champ w à travers la surface $\mathcal{S}$ est donné par l'intégrale double

$$\text{Flux} = \int_D w(s(u,v)) \cdot \left(\frac{\partial s}{\partial u}(u,v) \wedge \frac{\partial s}{\partial v}(u,v)\right)\,du\,dv.$$

Notez bien que dans la formule ci-dessus pour le flux, ce qui apparaît sous le signe intégral est le produit scalaire dans $\mathbb{R}^3$ du vecteur $w(x,y,z)$ pris au point $(x,y,z) = s(u,v)$ et du vecteur $\dfrac{\partial s}{\partial u}(u,v) \wedge \dfrac{\partial s}{\partial v}(u,v)$.

Bien sûr, il suffit que le champ de vecteur soit défini au voisinage de la surface (la surface est par définition l'image de D par l'application $(u,v) \mapsto s(u,v)$ dans $\mathbb{R}^3$). On notera aussi que si l'on échange u et v, l'orientation de la surface est changée.

Exercice 2.3.10
Calculer le flux du champ de vecteurs $w(x,y,z) = (x,y,0)$ à travers la sphère unité.

Solution.
Notez tout d'abord que la question n'est pas bien posée puisque la réponse dépend d'une orientation (voir ci-dessous Theorem 2.3.11). Dans la solution ci-dessous, on résout avec l'orientation associée au paramétrage (θ,ϕ).
On calcule :

$$\begin{aligned} w(s(\theta,\phi)) \cdot (\frac{\partial s}{\partial \theta}(\theta,\phi) \wedge \frac{\partial s}{\partial \phi}(\theta,\phi)) &= \begin{pmatrix} \sin\theta\sin\phi \\ \sin\theta\cos\phi \\ 0 \end{pmatrix} \cdot \begin{pmatrix} -\sin^2\theta\sin\phi \\ -\sin^2\theta\cos\phi \\ -\cos\theta\sin\theta \end{pmatrix} \\ &= -\sin^3\theta, \end{aligned}$$

et on intègre

$$\begin{aligned}\text{Flux} &= -\int_0^{\pi} \sin^3\theta\, d\theta \int_0^{2\pi} d\phi \\ &= -2\pi \int_0^{\pi} (1-\cos^2\theta)\, \sin\theta\, d\theta \\ &= -2\pi \int_{-1}^{+1} (1-u^2) du \\ &= -\frac{8\pi}{3}.\end{aligned}$$

Flux et élément d'aire .

Si on note

$$\nu = \frac{\frac{\partial s}{\partial u}(u,v) \wedge \frac{\partial s}{\partial v}(u,v)}{|\frac{\partial s}{\partial u}(u,v) \wedge \frac{\partial s}{\partial v}(u,v)|}$$

la normale orientée unitaire et

$$d\sigma = |\frac{\partial s}{\partial u}(u,v) \wedge \frac{\partial s}{\partial v}|\, du\, dv$$

l'élément d'aire, alors le flux peut aussi s'écrire

$$\text{Flux} = \int w \cdot \nu\, d\sigma.$$

Invariance .

Théorème 2.3.11 .
Le flux ne dépend pas du choix du paramétrage de la surface mais seulement de son orientation. Changer d'orientation change le signe du flux.

Preuve
On renvoie à la preuve de l'invariance de l'aire, à ceci près que le signe a maintenant de l'importance. Changer de paramétrage sans changer l'orientation, c'est remplacer (u,v) par $(u',v') = \theta(u,v)$, où θ est une fonction inversible de u et v, sans changer la normale unitaire orientée. C'est le cas si et seulement si le déterminant jacobien de θ est positif. Comme c'est la valeur absolue du jacobien qui intervient dans la formule de changement de variables, tout va bien. Si le déterminant jacobien est négatif (changement d'orientation), il est égal à l'opposé de sa valeur absolue, d'où un changement de signe pour le flux.

■

Exemple 2.3.12 .
On appelle angle solide d'une surface vue d'un point p le flux à travers cette surface du champ de vecteurs w_p défini en tout point $q \neq p$ de $\mathbb{R}^3$ par

$$w_p(q) = \frac{q-p}{|q-p|^3}.$$

Ce champ radial est le champ électrique d'une charge ponctuelle placée en p. Il faut toutefois orienter la surface!!

On peut montrer que toute sphère centrée en p a vu de p un angle solide égal à 4π. On prend en effet comme orientation une normale pointant vers l'extérieur de la sphère.
Le long de la sphère de rayon R centrée en p, $w_p \cdot \nu = R^{-2}$. Or l'aire de la sphère est $4\pi R^2$.

Chapitre 3

Algèbre linéaire

Les notes de ce chapitre sont fortement inspirées de notes de P. Pansu.

3.1 Déterminants

3.1.1 Echauffement dans le cas $n = 2$

La motivation initiale est de résoudre le système

$$(S) := \begin{cases} a_{11}x + a_{12}y &= b_1 \\ a_{21}x + a_{22}y &= b_2 \end{cases} \tag{3.1}$$

On va faire le calcul à la main avec en vue de mettre en évidence un objet mathématique intéressant.
Si $a_{11} \neq 0$, le système (S) est équivalent à

$$\begin{cases} a_{11}x + a_{12}y &= b_1 \\ (a_{22} - a_{12}\dfrac{a_{21}}{a_{11}})y &= b_2 - \dfrac{a_{21}}{a_{11}}b_1 \end{cases} \tag{3.2}$$

On a simplement soustrait à la deuxième ligne un multiple convenable de la première. Si de plus

$$a_{11}a_{22} - a_{12}a_{21} \neq 0 \ , \tag{3.3}$$

on trouve, pour toute paire (b_1, b_2) une solution unique (x, y) définie par

$$x = \frac{a_{22}b_1 - a_{12}b_2}{a_{11}a_{22} - a_{12}a_{21}} \ , \ y = \frac{a_{11}b_2 - a_{21}b_1}{a_{11}a_{22} - a_{12}a_{21}} \ . \tag{3.4}$$

Cette formule donne également la solution, sous la condition (3.3), quand $a_{11} = 0$. En travaillant un peu plus, on montre que le système (S) a une

unique solution si et seulement si (3.3) est satisfaite. La quantité $a_{11}a_{22} - a_{12}a_{21}$ est appelée le déterminant de la matrice

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} .$$

On note :

$$\text{Dét } A = a_{11}a_{22} - a_{12}a_{21} . \tag{3.5}$$

Une autre notation apparaissant dans la littérature est :

$$\text{Dét } A = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} . \tag{3.6}$$

Ce déterminant est calculé en prenant le produit des termes de la diagonale moins le produit des termes de l'antidiagonale.
Notons aussi que l'on peut écrire le système (S) sous la forme matricielle

$$AX = B , \tag{3.7}$$

où X est le vecteur colonne $X = \begin{pmatrix} x \\ y \end{pmatrix}$ et B le vecteur colonne $B = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$.
On aura aussi de la définition suivante :
Si v_1 et v_2 sont deux vecteurs de $\mathbb{R}^2$, on désigne par Dét (v_1, v_2) le déterminant de la matrice dont les vecteurs colonnes sont v_1 et v_2.

Remarque 3.1.1
Comme on l'a vu au chapitre précédent, $|$ *Dét* $(v_1, v_2)|$ *représente l'aire*[1] *les vecteurs du parallélogramme associé aux deux vecteurs* v_1 *et* v_2*. Il est donc naturel d'interprèter le déterminant de* v_1 *et* v_2 *comme l'aire algébrique de ce parallélogramme.*

Exemple 3.1.2
Si $v_1 = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$ *et* $v_2 = \begin{pmatrix} 3 \\ 5 \end{pmatrix}$*, on a*

$$\textit{Dét } (v_1, v_2) = \textit{ Dét } \begin{pmatrix} 1 & 3 \\ 2 & 5 \end{pmatrix} = 5 - 6 = -1 .$$

[1]Ici on est dans le cadre de $\mathbb{R}^2$, mais on peut toujours plonger la situation dans $\mathbb{R}^3$ en identifiant $\mathbb{R}^2$ au sous-espace de $\mathbb{R}^3$ défini par $z = 0$: Si v_j a comme coordonnées dans $\mathbb{R}^2$ (v_{1j}, v_{2j}), il suffit d'introduire de $\mathbb{R}^3$ $(v_{1j}, v_{2j}, 0)$ $(j = 1, 2)$ puis de considérer le produit tensoriel.

Propriétés élémentaires du déterminant

1. L'application :

$$\mathbb{R}^2 \times \mathbb{R}^2 \ni (v_1, v_2) \mapsto \text{ Dét } (v_1, v_2) \in \mathbb{R} \, ,$$

est bilinéaire et antisymétrique[2](voir ci-dessous (3.33) pour la définition).

2. Si on désigne par A^T la matrice transposée[3] de A, c'est à dire la matrice

$$A^T = \begin{pmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \end{pmatrix} \, ,$$

obtenue par échange des deux termes de l'antidiagonale, on a

$$\text{Dét}(A^T) = \text{ Dét}(A) \, . \tag{3.8}$$

3. Si A est triangulaire (i.e. si $a_{12} = 0$ ou $a_{21} = 0$), alors

$$\text{Dét}(A) = a_{11} \, a_{22} \, . \tag{3.9}$$

Dans ce cas c'est donc le produit des termes sur la diagonale.

4. La matrice A est inversible si et seulement si $\text{ Dét}(A) \neq 0$. Comme on l'a calculé plus haut (voir la formule (3.4) qui exprime X en fonction de B et qu'on peut réécrire sous la forme $X = A^{-1}B$), on a alors

$$A^{-1} = \frac{1}{\text{Dét}(A)} \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix} \, . \tag{3.10}$$

Toutes les assertions ci-dessus sont immédiates par simple calcul. La suivante pourrait aussi résulter d'un calcul "bête" mais on en donnera une démonstration plus "intelligente" à portée plus générale.

Théorème 3.1.3
Si A et B sont deux matrices 2×2, on a

$$\textit{Dét}(AB) = \textit{ Dét}(A) \ \textit{Dét}(B) \, . \tag{3.11}$$

La preuve est immédiate si on observe que, pour tous $v_1, v_2 \in \mathbb{R}^2$ et toute matrice C, on a :

$$\text{Dét}(Cv_1, Cv_2) = \text{ Dét}(C) \ \text{Dét}(v_1, v_2) \tag{3.12}$$

[2]Attention, la bonne généralisation quand on remplacera $\mathbb{R}^2$ par $\mathbb{R}^n$ sera celle de forme multilinéaire alternée

[3]Pour une matrice $n \times n$, la matrice $B = A^T$ transposée de A est la matrice $B = (b_{ij}$ avec $b_{ij} = a_{ji}$.

Remarque 3.1.4
Une interprétation naturelle de cette formule est que l'aire du parallèlogramme, image par C du parallèlogramme engendré par v_1 et v_2, est l'aire de ce dernier multipliée par $|$ Dét $C|$.

La preuve de cette propriété passe par deux définitions et un théorème. Nous posons ci-dessous $E = \mathbb{R}^2$.

Définition 3.1.5
On dit qu'une application φ de $E \times E$ dans $\mathbb{R}$ est bilinéaire si

$$\varphi(\lambda_1 v_1 + \mu_1 w_1, v_2) = \lambda_1 \varphi(v_1, v_2) + \mu_1 \varphi(w_1, v_2) \ , \tag{3.13}$$

et

$$\varphi(v_1, \lambda_2 v_2 + \mu_2 w_2) = \lambda_2 \varphi(v_1, v_2) + \mu_2 \varphi(w_1, v_2) \ . \tag{3.14}$$

Le produit scalaire sur $\mathbb{R}^2$ de deux vecteurs définit une forme bilinéaire. L'application $E \times E \ni (v_1, v_2) \mapsto$ Dét(v_1, v_2) définit également une forme bilinéaire.

Définition 3.1.6
On dit qu'une application φ de $E \times E$ dans $\mathbb{R}$ est antisymétrique (ou alternée) si

$$\varphi(v_1, v_2) = -\varphi(v_2, v_1) \ . \tag{3.15}$$

Notre théorème dit

Théorème 3.1.7
Soit φ une forme bilinéaire antisymétrique sur $\mathbb{R}^2$ alors il existe une constante c_φ telle que

$$\varphi(v_1, v_2) = c_\varphi \ D\acute{e}t \ (v_1, v_2) \ , \ \forall v_1 \ , \ \forall v_2 \ . \tag{3.16}$$

La preuve se fait par un calcul direct en exprimant v_1 et v_2 sur la base canonique de $\mathbb{R}^2$: $e_1 = (1, 0)$,$e_2 = (0, 1)$.
On écrit, avec $v_1 = a_{11}e_1 + a_{21}e_2$ et $v_2 = a_{12}e_1 + a_{22}e_2$,

$$\begin{aligned} \varphi(v_1, v_2) &= \varphi(a_{11}e_1 + a_{21}e_2, a_{12}e_1 + a_{22}e_2) \\ &= 0 \ + \ a_{11}a_{22}\varphi(e_1, e_2) \ + \ a_{21}a_{12}\varphi(e_2, e_1) \ + \ 0 \\ &= (a_{11}a_{22} - a_{21}a_{12}) \, \varphi(e_1, e_2) \\ &= \ \text{Dét} \ (v_1, v_2)\varphi(e_1, e_2) \ . \end{aligned}$$

Pour passer de la première ligne à la deuxième, on a utilisé que

$$\varphi(e_1, e_1) = -\varphi(e_1, e_1) = 0 \ , \ \varphi(e_2, e_2) = 0 \ .$$

Ceci démontre le théorème avec

$$c_\varphi = \varphi(e_1, e_2) \ . \tag{3.17}$$

On peut maintenant démontrer la formule (3.12). Il suffit d'appliquer le théorème à la forme

$$(v_1, v_2) \mapsto \ \text{Dét}(Cv_1, Cv_2) \ .$$

Déterminant d'un endomorphisme

Nous terminons l'échauffement par l'introduction d'une notion indépendante du choix d'une base. On appelle endomorphisme u une application linéaire de E dans E. Une fois choisie une base $\mathcal{B}$ de E, on sait qu'on peut associer à u sa matrice dans la base $\mathcal{B}$ qu'on notera $A_\mathcal{B}$. On sait que lorsque l'on choisit une nouvelle base $\mathcal{B}'$, la matrice $A_{\mathcal{B}'}$ de u dans la nouvelle base vérifie

$$A_{\mathcal{B}'} = P^{-1} A_\mathcal{B} P \ . \tag{3.18}$$

En appliquant deux fois (3.11), on obtient

$$\text{Dét } A_{\mathcal{B}'} = \ \text{Dét } P^{-1} \ \text{Dét } A_\mathcal{B} \ \text{Dét } P \ . \tag{3.19}$$

Par ailleurs, on peut aussi appliquer (3.11) dans la formule

$$I = P^{-1} \ P \ ,$$

ce qui conduit à

$$1 = \ \text{Dét } I = \ \text{Dét } P^{-1} \ \ \text{Dét } P \ .$$

On a donc

$$\text{Dét } P^{-1} = 1/ \ \text{Dét } P \ , \tag{3.20}$$

et

$$\text{Dét } A_{\mathcal{B}'} = \ \text{Dét } A_\mathcal{B} \ . \tag{3.21}$$

La dernière équation s'interprète ainsi. Le calcul du déterminant ne dépend pas du choix de la base. Il est donc naturel de définir le déterminant d'un endomorphisme u par

$$\text{Dét } u = \ \text{Dét } A_\mathcal{B} \ . \tag{3.22}$$

3.1.2 Rappels sur les systèmes linéaires.

Un système linéaire de p équations à n inconnues s'écrit sous la forme

$$\sum_{j=1}^{n} a_{ij} x_j = b_i \ , \quad \text{for } i = 1, \ldots, p \ . \tag{3.23}$$

Les n inconnues sont les x_j $(j = 1, \ldots, n)$ et les données sont les b_i $(i = 1, \ldots, p)$.
Sous forme matricielle on l'écrit

$$AX = B \ ,$$

où A est la matrice à p lignes et n colonnes (a_{ij}), $X \in \mathbb{R}^n$ (mais écrit comme un vecteur colonne), $B \in \mathbb{R}^p$ (aussi écrit comme un vecteur colonne).

Exemple 3.1.8
Le système

$$(S) := \left\{ \begin{array}{ll} x + 2y + 3z & = 1 \\ 2x + \beta y + 6z & = \alpha \end{array} \right. ,$$

correspond à

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & \beta & 6 \end{pmatrix} \ , \ B = \begin{pmatrix} 1 \\ \alpha \end{pmatrix} \ .$$

Définition 3.1.9
Deux systèmes sont dits équivalents s'ils ont les mêmes solutions. Pour un B donné un système est dit compatible s'il admet des solutions.

Une manière assez systématique d'étudier la compatibilité d'un système est la méthode du pivot.
Par les opérations suivantes

- ajouter à une équation (ligne) une combinaison linéaire des autres,
- permuter les lignes,
- permuter les colonnes (ce qui revient à renuméroter les variables),

on peut ramener tout système linéaire à un système équivalent de la forme

$$A'X' = B' \ ,$$

avec

(a) X' se déduisant de X par permutation des variables [4]

(b)

$$A' = \begin{pmatrix} T & U \\ 0 & 0 \end{pmatrix} \ , \ B' = \begin{pmatrix} B'_1 \\ B'_2 \end{pmatrix} \ ,$$

où

1. T est une matrice $r \times r$ triangulaire supérieure dont tous les termes sur la diagonale sont non nuls,

[4] Il existe donc une bijection f de $\{1, \ldots, n\}$ sur lui-même telle que : $x'_i = x_{f(i)}$.

2. U est une matrice $r \times (n-r)$,
3. $B'_1 \in \mathbb{R}^r$, $B'_2 \in \mathbb{R}^{p-r}$.

De plus r (qui vérifie bien sûr $r \leq \min(p,n)$) est le rang (voir plus loin pour le rappel de la définition et un critère pour calculer ce rang) de la matrice A'. r est la dimension de l'image de A' et $n-r$ est la dimension du noyau de A'.
On notera que **le système est compatible si et seulement si** $B'_2 = 0$. Si cette condition de stabilité est satisfaite, l'ensemble des solutions est un espace affine de dimension $n-r$.
Plus concrètement, si cette condition de compatibilité est satisfaite et si X'_0 est une solution particulière du système, toute solution X' s'écrit sous la forme $X'_0 + V'$, où V' est une solution du système homogène

$$A'V' = 0 \ .$$

Précisons comment l'on fait en utilisant la forme particulière de A'.

Les inconnues (finales) non principales sont par définition $x'_{r+1}, \ldots, x'_n$. On recherche une solution particulière en résolvant le système en assignant la valeur 0 aux inconnues non principales.

La recherche d'une base de solutions du système homogène est obtenue (pour $j = r+1, \ldots, n$) en assignant aux inconnues non principales les valeurs

$$x'_k = \delta_{kj} \ , \text{ pour } k = r+1, \ldots, n \ ,$$

où δ_{kj} est l'indice de Kronecker[5].

Sous forme matricielle, on remarque que T est inversible (c'est une matrice triangulaire dont tous les termes sur la (première) diagonale sont non nuls) et que si on écrit $X' = \begin{pmatrix} X'_1 \\ X'_2 \end{pmatrix}$ avec $X'_1 \in \mathbb{R}^r$ correspondant aux r-premières coordonnées de X', on a :

$$X'_1 = T^{-1}(B'_1 - UX'_2) \ . \tag{3.24}$$

On retrouve alors immédiatement les assertions ci-dessus. En particulier, une solution particulière est donnée par

$$X'_0 = \begin{pmatrix} T^{-1}B'_1 \\ 0 \end{pmatrix} \ . \tag{3.25}$$

[5] $\delta_{kj} = 1$ si $k = j$ et 0 sinon.

La solution du système homogène a la forme

$$V' = \begin{pmatrix} -T^{-1}UX_2' \\ X_2' \end{pmatrix} . \tag{3.26}$$

Montrons sur l'exemple 3.1.8 comment marche la méthode du pivot.
On garde la première ligne et on soustrait à la deuxième ligne deux fois la première. On obtient comme nouveau système équivalent :

$$(S') := \begin{cases} x + 2y + 3z &= 1 \\ (\beta - 4)y &= (\alpha - 2) \end{cases} ,$$

On voit apparaître deux cas selon que $\beta \neq 4$ ou $\beta = 4$.

Cas $\beta \neq 4$
Dans ce cas, on résout immédiatement la deuxième ligne et on trouve d'abord :

$$y = \frac{\alpha - 2}{\beta - 4} .$$

La première ligne prend la forme :

$$x + 3z = 1 - 2\frac{\alpha - 2}{\beta - 4} = \frac{\beta - 2\alpha}{\beta - 4} .$$

Pour tout $z \in \mathbb{R}$, on trouve une solution x définie par cette dernière équation.
Réinterprètons ce qui vient d'être fait en reprenant le langage général. On est dans le cas où $r = 2$. Comme $p = 2$, il n'y a pas de condition de compatibilité à vérifier.
Les matrices T et U sont simplement

$$T = \begin{pmatrix} 1 & 2 \\ 0 & \beta - 4 \end{pmatrix} , \; U = \begin{pmatrix} 3 \\ 0 \end{pmatrix} .$$

Cas $\beta = 4$
Le système devient :

$$(S') := \begin{cases} x + 2y + 3z &= 1 \\ 0 &= (\alpha - 2) \end{cases} ,$$

On voit apparaître la condition de compatibilité :

$$\alpha = 2 .$$

Sous cette condition, on a une infinité de solutions (x, y, z) ou pour tous $(y, z) \in \mathbb{R}^2$, x est défini par

$$x = 1 - 2y - 3z \ .$$

Réinterprètons ce qui vient d'être fait en reprenant le langage général. On est cette fois-ci dans le cas où $r = 1$. Les matrices T et U sont simplement

$$T = \begin{pmatrix} 1 \end{pmatrix} \ , \ U = \begin{pmatrix} 2 & 3 \end{pmatrix} \ .$$

Ceci termine l'étude de cet exemple.

Terminons par rappeler une définition standard.
Un **système de Cramer** est un système linéaire de n équations à n inconnues tel que le système homogène associé admette uniquement la solution $(0, \cdots, 0)$.
On vient de montrer que : un système est de Cramer si et seulement si, quel que soit le choix des seconds membres, il existe une solution unique.
Par rapport à ce que l'on a fait dans le cas de la méthode du pivot, cela correspond au cas où

$$r = p = n \ .$$

On verra plus tard qu'un système est de Cramer si et seulement si le déterminant de la matrice associée est non nul.

3.1.3 Sur le chemin des déterminants généraux : déterminant d'une matrice 3×3

L'étude à la main des systèmes 3×3 conduit à l'introduction de l'objet suivant associé à une matrice 3×3 $A = (a_{ij})$, qui est appelé le déterminant de A et est défini par :

$$\text{Dét}A = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{31}a_{22}a_{13} - a_{11}a_{23}a_{32} - a_{21}a_{12}a_{33} \ . \tag{3.27}$$

Expliquons brièvement la démonstration dans le cas $a_{11} \neq 0$. Partant du système

$$\begin{aligned} a_{11}x + a_{12}y + a_{13}z &= b_1 \\ a_{21}x + a_{22}y + a_{23}z &= b_2 \\ a_{31}x + a_{32}y + a_{33}z &= b_3 \ , \end{aligned}$$

on procède aux opérations suivantes.

1. On garde la première ligne.

2. On soustrait à la deuxième ligne $\dfrac{a_{21}}{a_{11}}$ fois la première ligne.
3. On soustrait à la troisième ligne $\dfrac{a_{31}}{a_{11}}$ fois la première ligne.

Le résultat est qu'on a un nouveau système de la forme

$$\widetilde{A}X = \widetilde{B}\ ,$$

où $\widetilde{A}$ est la matrice

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ 0 & a_{22} - a_{12}\dfrac{a_{21}}{a_{11}} & a_{23} - a_{13}\dfrac{a_{21}}{a_{11}} \\ 0 & a_{32} - a_{12}\dfrac{a_{31}}{a_{11}} & a_{33} - a_{13}\dfrac{a_{31}}{a_{11}} \end{pmatrix}$$

On pourrait continuer ainsi en travaillant sur les deux dernières lignes pour obtenir une triangulation complète, mais on peut aussi utiliser (amorce d'une récurrence plus générale) le résultat obtenu sur les systèmes 2×2, puisque les deux dernières lignes ne font intervenir que y et z comme inconnues.
Le critère pour résoudre est alors

$$a_{11}\ \text{Dét}\ \begin{pmatrix} a_{22} - a_{12}\dfrac{a_{21}}{a_{11}} & a_{23} - a_{13}\dfrac{a_{21}}{a_{11}} \\ a_{32} - a_{12}\dfrac{a_{31}}{a_{11}} & a_{33} - a_{13}\dfrac{a_{31}}{a_{11}} \end{pmatrix} \neq 0\ .$$

Après calcul, on trouve que le terme de gauche est exactement DétA.
Quand $a_{11} = 0$, on échange la première ligne et la deuxième ligne. Si $a_{21} \neq 0$, on peut alors procéder comme dans le premier cas.
Si $a_{21} = 0$ et $a_{31} \neq 0$, c'est la troisième ligne que l'on fait passer en première ligne.
Si toute la première colonne de A est nulle, alors la variable x a disparu dans le terme de gauche et le système n'est pas de Cramer.

Concrètement, on peut mémoriser la formule du déterminant (3.27) par la règle de Sarrus qui est spécifique des matrices 3×3. Pour chaque diagonale (il y en a 3), on fait le produit des trois coefficients apparaissant puis la somme des trois calculs. On fait le même calcul relativement aux antidiagonales mais en multipliant par -1

Une autre technique de calcul qui apparaîtra de portée plus générale est de vérifier que

$$\text{Dét}A = a_{11}\Delta_{11} - a_{21}\Delta_{21} + a_{31}\Delta_{31}\ , \tag{3.28}$$

où Δ_{ij} est le déterminant de la matrice 2×2 obtenue en rayant la i-ème ligne et la j-ème colonne.
Pour tout (i, j), Δ_{ij} est appelé le **cofacteur** de A associé à la paire (i, j).

Noter l'alternance des signes dans le terme de droite : le coefficient de a_{ij} est en fait $(-1)^{i+j}$.

Nous utiliserons aussi la notion de comatrice. On appelle **comatrice** de A la matrice C qui est simplement définie par

$$C_{ij} = (-1)^{i+j} \Delta_{ij} \ . \tag{3.29}$$

Avec cette définition, la formule du déterminant devient :

$$\text{Dét}A = a_{11}C_{11} + a_{21}C_{21} + a_{31}C_{31} \tag{3.30}$$

Concrètement, cela correspond au calcul

$$\text{Dét}A = a_{11}(a_{22}a_{33} - a_{32}a_{23}) - a_{21}(a_{12}a_{33} - a_{13}a_{13}) + a_{31}(a_{21}a_{23} - a_{22}a_{13}) \ .$$

On vient de procéder à un développement selon la première colonne. On peut en fait développer selon n'importe quelle colonne ou n'importe quelle ligne en suivant les mêmes règles. Ceci donne les formules, pour tout $j = 1, \ldots, n$,

$$\text{Dét}A = \sum_i a_{ij} C_{ij} \ , \tag{3.31}$$

(formule qui correspond au développement par rapport à la j-ème colonne) et, pour tout $i = 1, \ldots, n$,

$$\text{Dét}A = \sum_j a_{ij} C_{ij} \ , \tag{3.32}$$

(formule qui correspond à la i-ème ligne).

Cette formule se généralisera facilement dans la mesure où on a su calculer le déterminant 3×3 en se ramenant au calcul de trois déterminants 2×2.

Déterminant de trois vecteurs
Comme on a défini le déterminant de deux vecteurs, on peut définir dans $\mathbb{R}^3$ (muni de sa base canonique) le déterminant[6] $\text{Dét}\,(v_1, v_2, v_3)$ de trois vecteurs v_1, v_2, v_3. C'est le déterminant de la matrice dont les colonnes sont constituées

[6] Attention ! Ce déterminant dépend de la base choisie.

des composantes des trois vecteurs dans la base canonique.

Cette fois-ci, on peut vérifier l'application de $\mathbb{R}^3 \times \mathbb{R}^3 \times \mathbb{R}^3$ dans $\mathbb{R}$ qui associe à trois vecteurs de $\mathbb{R}^3$ le déterminant de ces trois vecteurs correspond à une forme trilinéaire alternée.

On dit qu'une forme trilinéaire φ sur un espace vectoriel E est **alternée** si pour tous v_1, v_2, v_3 dans E on a :

$$\begin{array}{l} \varphi(v_1, v_2, v_3) = -\varphi(v_2, v_1, v_3) \ , \\ \varphi(v_1, v_2, v_3) = -\varphi(v_1, v_3, v_2) \ , \\ \varphi(v_1, v_2, v_3) = -\varphi(v_3, v_2, v_1) \ . \end{array} \tag{3.33}$$

Comme dans le cas des formes bilinéaires alternées sur un expace vectoriel de dimension 2, on peut démontrer qu'une forme **tri**-linéaire alternée sur un espace de dimension **trois** est unique à une multiplication près. Choisissant la base canonique (e_1, e_2, e_3) de $\mathbb{R}^3$, il est en effet facile de montrer que

$$\varphi(v_1, v_2, v_3) = \varphi(e_1, e_2, e_3) \ \text{Dét}\,(v_1, v_2, v_3) \ . \tag{3.34}$$

En particulier la première ligne de (3.33) exprime que l'échange de deux colonnes dans le calcul du déterminant change le signe du déterminant.

On en déduit aussi assez facilement que si v_1, v_2 et v_3 sont linéairement dépendants, alors

$$\text{Dét}\,(v_1, v_2, v_3) = 0 \ . \tag{3.35}$$

En effet supposons par exemple que $v_1 = \alpha v_2 + \beta v_3$. On a alors

$$\text{Dét}\,(v_1, v_2, v_3) = \ \text{Dét}\,(\alpha v_2 + \beta v_3, v_2, v_3) = \alpha \ \text{Dét}\,(v_2, v_2, v_3) + \beta \ \text{Dét}\,(v_3, v_2, v_3) = 0 \ .$$

(3.35) est d'ailleurs une condition suffisante. Si cette condition est satisfaite, alors v_1, v_2 et v_3 sont linéairement dépendants. Le système associé à la matrice $A := \begin{pmatrix} v_1 & v_2 & v_3 \end{pmatrix}$ n'est pas de Cramer. On peut donc trouver $(\alpha, \beta, \gamma) \neq (0, 0, 0)$ tel que

$$A \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} = 0 \ ,$$

qui est équivalent à

$$\alpha v_1 + \beta v_2 + \gamma v_3 = 0 \ .$$

Cette dernière égalité exprime que v_1, v_2 et v_3 sont linéairement dépendants. On a ainsi démontré la

Proposition 3.1.10
Trois vecteurs v_1, v_2 et v_3 dans $\mathbb{R}^3$ sont linéairement indépendants si et seulement si

$$Dét\,(v_1, v_2, v_3) \neq 0\ . \tag{3.36}$$

Comme dans le cas du déterminant d'une matrice 2×2, on peut vérifier que :

1.
$$\text{Dét}\, A = \ \text{Dét}\, A^T\ . \tag{3.37}$$

2. Si A est triangulaire, alors

$$\text{Dét}\, A = a_{11}\, a_{22}\, a_{33}\ . \tag{3.38}$$

3.
$$\text{Dét}\,(Cv_1, Cv_2, Cv_3) = \ \text{Dét}\, C \cdot\ \text{Dét}\,(v_1, v_2, v_3)\ . \tag{3.39}$$

4.
$$\text{Dét}\,(AB) = \ \text{Dét}\, A\ \cdot\ \text{Dét}\, B\ . \tag{3.40}$$

L'item (3.39) se déduit de (3.34) par le même principe de démonstration que dans le cas 2×2. On déduit du dernier item que si A est inversible alors $\text{Dét}A \neq 0$ et comme on avait déjà observé la propriété inverse, on a finalement

Proposition 3.1.11
A est inversible si et seulement si $Dét\ A \neq 0$.

Comme dans le cas des espaces de dimension 2, on peut définir pour les espaces de dimension 3, le déterminant d'un endomorphisme.

Nous pouvons terminer par l'analogue de la formule (3.10) démontrée dans le cas de la dimension 2 qui donne une expression de l'inverse.

Proposition 3.1.12
Si A est inversible, alors

$$A^{-1} = \frac{1}{Dét\, A} C^T\ , \tag{3.41}$$

où C est la comatrice de A.

Démonstration
On calcule AC^T. On a

$$(AC^T)_{ij} = \sum_k a_{ik} C_{jk}\ .$$

Il suffit de démontrer que

$$(AC^T)_{ij} = \delta_{ij} \text{ Dét } A \ .$$

Lorsque $i = j$, on remarque que cela correspond au développement du déterminant le long de la i-ème ligne (voir 3.32). Lorsque $i \neq j$, on remarque que cela correspond au calcul du déterminant de la matrice A' où on a remplacé dans A la j-ème ligne par la i-ème. A' a deux lignes égales. A'^T a donc deux colonnes égales. Son déterminant (qui est égal au déterminant de A') est donc nul.

Remarque 3.1.13
On vérifie facilement que

$$Dét\ (v_1, v_2, v_3) = v_1 \cdot (v_2 \wedge v_3) \ . \tag{3.42}$$

Dans le cas de la dimension 3*, on a donc de nouveau une interprétation géométrique comme le volume d'un parallélépipède qui pourrait nous être utile dans l'étude des intégrales de volume.*

3.1.4 Le cas général des matrices $n \times n$

Une première définition par récurrence.

Il y a plusieurs manières de définir le déterminant. La première est par récurrence et la deuxième est plus élégante mais inexploitable pour calculer effectivement le déterminant.

Commençons par la définition par récurrence. On va juste prendre comme définition la propriété (3.32) qu'on avait vérifiée pour les déterminants 3×3, et qui correspond au développement le long de la première ligne.

Définition 3.1.14
Soit A une matrice $n \times n$, soit Δ_{ij} le cofacteur de A qui est le déterminant de la matrice déduite de A en effaçant la i-ème ligne et la j-ème colonne. Alors, on définit le déterminant de A par

$$Dét\, A = \sum_j (-1)^{1+j} a_{1j} \Delta_{1j} \ . \tag{3.43}$$

On remarque que tout prendra un sens par récurrence. On a défini le déterminant d'une matrice 2×2. Si on suppose que l'on a défini le déterminant de matrices $(n-1) \times (n-1)$ alors la définition ci-dessus nous permet de définir celui d'une matrice $n \times n$ puisque les Δ_{ij} sont des déterminants de telles matrices.

Exemple 3.1.15

$$\begin{vmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 2 \\ 3 & 0 & -1 & 0 \end{vmatrix} = 1 \times \begin{vmatrix} 1 & 1 & 0 \\ 1 & 0 & 2 \\ 0 & -1 & 0 \end{vmatrix} - 0 \times \begin{vmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 3 & -1 & 0 \end{vmatrix}$$
$$+0 \times \begin{vmatrix} 0 & 1 & 0 \\ 0 & 1 & 2 \\ 3 & 0 & 0 \end{vmatrix} - 1 \times \begin{vmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 3 & 0 & -1 \end{vmatrix}$$
$$= \begin{vmatrix} 1 & 1 & 0 \\ 1 & 0 & 2 \\ 0 & -1 & 0 \end{vmatrix} - \begin{vmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 3 & 0 & -1 \end{vmatrix} .$$

Il reste deux déterminants 3×3 *à calculer. Pour le premier, on a (en développant par rapport à la dernière ligne) :*

$$\begin{vmatrix} 1 & 1 & 0 \\ 1 & 0 & 2 \\ 0 & -1 & 0 \end{vmatrix} = (-1)^{3+2} \times (-1) \times \begin{vmatrix} 1 & 0 \\ 1 & 2 \end{vmatrix} = 2 .$$

Pour le second, on a, en développant par rapport à la première colonne,

$$\begin{vmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 3 & 0 & -1 \end{vmatrix} = (-1)^{1+3} \times 3 \times \begin{vmatrix} 1 & 1 \\ 1 & 0 \end{vmatrix} = -3 .$$

On a donc finalement

$$\begin{vmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 2 \\ 3 & 0 & -1 & 0 \end{vmatrix} = 5 .$$

Pour celles ou ceux qui ont du mal avec la question des signes noter que la matrice constituée des signes de la matrice $(-1)^{i+j}$ est donnée par :

$$\begin{vmatrix} + & - & + & - \\ - & + & - & + \\ + & - & + & - \\ - & + & - & + \end{vmatrix} .$$

Proposition 3.1.16
Si $E = \mathbb{R}^n$*, l'application de* E^n *dans* $\mathbb{R}$ $(v_1, v_2, \ldots, v_n) \mapsto D\acute{e}t(v_1, v_2, \ldots, v_n)$ *est une forme n-linéaire alternée*[7].

[7]Ici la définition d'alternée est l'extension naturelle de celle donnée pour $n = 3$ en (3.33)

Preuve
La preuve se fait par récurrence sur n.

Comme dans le cas $n = 3$, on obtient que

$$\text{Dét}\,(v_1 - \sum_{j=2}^{n} \lambda_j v_j, v_2, \ldots, v_n) = \text{Dét}\,(v_1, v_2, \ldots, v_n)\ , \tag{3.44}$$

et, que si v_1,v_2,..., v_n sont linéairement dépendants alors

$$\text{Dét}\,(v_1, v_2, \ldots, v_n) = 0\ . \tag{3.45}$$

On énonce maintenant sans démonstrations (elles sont très voisines de celles qu'on a faites lorsqu'on est passé du cas de la dimension 2 au cas de la dimension 3) un certain nombre de propriétés utiles des déterminants.

1. Si A est triangulaire inférieure alors

$$\text{Dét}\,A = \Pi_{j=1}^{n} a_{jj}\ . \tag{3.46}$$

2. Si A est triangulaire par bloc

$$A = \begin{pmatrix} B & 0 \\ C & D \end{pmatrix}$$

avec B et D matrices carrées, alors

$$\text{Dét}\,A = \text{Dét}\,B \cdot \text{Dét}\,D\ . \tag{3.47}$$

3. Toute forme n-linéaire alternée sur $\mathbb{R}^n$ est proportionnelle au déterminant.
4.
$$\text{Dét}\,(AB) = \text{Dét}\,A \cdot \text{Dét}\,B\ . \tag{3.48}$$

5. A est inversible si et seulement si $\text{Dét}\,A \neq 0$.
6. Si A est inversible alors

$$A^{-1} = \frac{1}{\text{Dét}\,A} C^T\ , \tag{3.49}$$

où C est la comatrice.

7. On peut définir de manière intrinsèque (c'est-à-dire indépendamment du choix de la base) le déterminant d'un endomorphisme.

Une autre formule pour le déterminant

On cherche une formule plus directement associée à la donnée des a_{ij}. Pour cela nous avons besoin de définir les permutations d'un ensemble fini et leurs propriétés.

Définition 3.1.17
Une permutation de $\{1,\dots,n\}$ *est une bijection de* $\{1,\dots,n\}$ *sur lui-même.*

L'ensemble $\mathfrak{S}_n$ des permutations a une structure de groupe pour la composition des applications.
L'ensemble $\{1,2\}$ a exactement 2 permutations, l'identité e et la transposition τ de 1 et 2. Le groupe $\mathfrak{S}_2$ a deux éléments. e est l'élément neutre et τ vérifie $\tau^2 = e$.
L'ensemble $\{1,2,3\}$ a 6 permutations :

- l'identité e,
- la transposition[8] τ_{12} de 1 et 2 conservant 3,
- la transposition τ_{23} de 2 et 3 conservant 1,
- la transposition τ_{31} de 3 et 1 conservant 2,
- la permutation circulaire c envoyant 1 sur 2, 2 sur 3, 3 sur 1,
- son carré c_2 qui envoie 1 sur 3, 2 sur 1 et 3 sur 2.

On laisse le lecteur vérifier que $\mathfrak{S}_n$ est constitué de $n!$ éléments. On peut aussi montrer que tout élément de $\mathfrak{S}_n$ est un produit de transpositions.

On peut maintenant associer à tout élément de $\mathfrak{S}_n$ sa signature. Cette signature prend ses valeurs dans le groupe multiplicatif $\{-1,+1\}$ et est l'homomorphisme[9] de $\mathfrak{S}_n$ dans $\{-1,+1\}$ qui vérifie :

$$\epsilon(e) = 1\ ,\ \epsilon(\tau_{ij}) = -1\ ,\ \forall i \neq j\ . \tag{3.50}$$

Une formule pour ϵ, qui n'a qu'un intérêt théorique, est

$$\epsilon(\sigma) = \Pi_{i<j}\frac{\sigma(j)-\sigma(i)}{j-i} \in \{-1,+1\}\ . \tag{3.51}$$

(On peut commencer par vérifier que $\epsilon(\sigma)$ est effectivement de valeur absolue 1).

[8] Une transposition est une bijection qui permutent deux éléments et conserve les autres.

[9] On entend par là que si σ et σ' sont deux permutations, la signature de la composée $\sigma\circ\sigma'$ de ces deux permutations vérifie :

$$\epsilon(\sigma\circ\sigma') = \epsilon(\sigma)\epsilon(\sigma')\ .$$

Toute permutation pouvant s'écrire comme composée de transpositions, le nombre de transpositions utilisées détermine la parité de la signature et donc la signature.

On peut alors démontrer le théorème

Théorème 3.1.18
Si $A = (a_{ij})$, alors

$$D\acute{e}t(a_{ij}) = \sum_{\sigma \in \mathfrak{S}_n} \epsilon(\sigma)\, a_{\sigma_1 1}\, a_{\sigma_2 2} \cdots a_{\sigma_n n}\ , \tag{3.52}$$

où $\sigma_n = \sigma(n)$ pour la permutation σ.

On démontre ce théorème en montrant que le membre de droite définit aussi une forme n-linéaire alternée, qui est donc proportionnelle au déterminant. La vérification que le coefficient de proportionalité est 1 se fait en calculant la valeurs des deux formes n-linéaires avec $(v_1, \ldots, v_n) = (e_1, \ldots, e_n)$ les éléments de la base canonique de $\mathbb{R}^n$.
On déduit facilement de la formule ci-dessus que

$$\text{Dét}\, A^T = \text{Dét}\, A\ . \tag{3.53}$$

Calcul pratique des déterminants.

Voilà quelques conséquences pratiques des propriétés théoriques que nous avons présentées.

1. L'échange de deux colonnes dans la matrice change juste le signe du déterminant.
2. (3.53) permet alors de montrer que l'échange de deux lignes dans la matrice change juste le signe du déterminant.
3. On peut calculer le déterminant en développant le long de n'importe quelle colonne (voir formule (3.31)).
4. (3.53) permet alors de montrer que l'on peut calculer le déterminant en développant le long de n'importe quelle ligne (voir formule (3.32)).
5. Ajouter à une colonne une combinaison linéaire des autres colonnes ne change pas le déterminant.
6. Ajouter à une ligne une combinaison linéaire des autres lignes ne change pas le déterminant.

Concrètement, on cherche dans le cas de matrices creuses (c'est à dire avec beaucoup de coefficients nuls) à développer par rapport à la ligne ou la colonne ayant le maximum de zéros et on n'oublie pas d'appliquer la règle des signes dans le calcul de la comatrice.

Rang et Mineurs

Définition 3.1.19
Un mineur de taille q extrait de A est le déterminant d'une matrice $q \times q$ extraite de A.

Par exemple, les mineurs de taille 2 extraits de la matrice $A = \begin{pmatrix} 2 & 3 & -1 \\ 4 & 0 & 5 \end{pmatrix}$ sont :

$$\begin{vmatrix} 2 & 3 \\ 4 & 0 \end{vmatrix}, \begin{vmatrix} 3 & -1 \\ 0 & 5 \end{vmatrix}, \begin{vmatrix} 2 & -1 \\ 4 & 5 \end{vmatrix}.$$

Notons qu'ils sont tous non nuls.

Les mineurs de taille 2 extraits de la matrice $A = \begin{pmatrix} 2 & 3 & -1 & 0 \\ 4 & 0 & 5 & -3 \\ 5 & -2 & 1 & 6 \end{pmatrix}$ sont :

$$\begin{vmatrix} 2 & 3 \\ 4 & 0 \end{vmatrix}, \begin{vmatrix} 3 & -1 \\ 0 & 5 \end{vmatrix}, \begin{vmatrix} 2 & -1 \\ 4 & 5 \end{vmatrix}, \begin{vmatrix} 3 & -1 \\ 0 & 5 \end{vmatrix}, \begin{vmatrix} 3 & 0 \\ 0 & -3 \end{vmatrix}, \begin{vmatrix} -1 & 0 \\ 5 & -3 \end{vmatrix}, \begin{vmatrix} 4 & 0 \\ 5 & -2 \end{vmatrix}, \begin{vmatrix} 4 & 5 \\ 5 & 1 \end{vmatrix}, \begin{vmatrix} 4 & -3 \\ 5 & 6 \end{vmatrix}, \ldots$$

Théorème 3.1.20
Le rang d'une matrice A est $\geq q$ si et seulement si il existe un mineur non nul de taille q extrait de A.

Preuve
On rappelle que le rang de A est la dimension de l'espace vectoriel engendré par les vecteurs colonnes de A.
Si $\text{Rang}\,(A) < q$, alors toute famille de q colonnes de A est liée. En ne gardant que certaines lignes, on obtient encore une famille liée (projection sur un sous espace vectoriel). Le déterminant correspondant, un mineur de taille q, est donc nul.

Réciproquement, si $\text{Rang}\,(A) \geq q$, alors des opérations sur les lignes de A amènent A sur $A' = \begin{pmatrix} T & U \\ 0 & V \end{pmatrix}$, où T est une $q \times q$ matrice triangulaire de coefficients diagonaux non nuls et $\text{Dét}\,T$ est égal à un mineur de A.

En particulier, lorsque A est une matrice $n \times n$ de rang n, le système est de Cramer et on a donc :

Proposition 3.1.21
Un système $n \times n$ est de Cramer si et seulement si son déterminant est non nul.

Remarque 3.1.22
Dans tout ce qui précède, on aurait pu remplacer $\mathbb{C}^n$ par $\mathbb{R}^n$. Il n'y a aucun changement dans les différentes définitions.

Applications : Polynôme caractéristique

Définition 3.1.23
Soit u une endomorphisme de $\mathbb{R}^n$. Alors

$$\mathbb{R} \ni X \mapsto P_n(X) := Dét(XI_n - u) \,, \tag{3.54}$$

est un polynôme dont le terme de plus haut degré est X^n. On l'appelle polynôme caaractéristique de u. Il ne dépend pas du choix de la base.

Considérons par exemple la matrice 3×3

$$A = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 3 & 4 \\ 1 & -1 & -1 \end{pmatrix} \,.$$

La matrice $XI_3 - A$ s'écrit

$$(XI_3 - A) = \begin{pmatrix} X-1 & -2 & -1 \\ 0 & X-3 & -4 \\ -1 & 1 & X+1 \end{pmatrix} \,,$$

et on trouve

$$P_A(X) = (X-3)(X^2+2) \,.$$

Remarques 3.1.24
Si u est un endomorphisme, dont la matrice dans la base canonique est A, on a :

1. *Le terme constant est*

$$P_u(0) = (-1)^n Dét(u) \,. \tag{3.55}$$

2. *Le coefficient de X^{n-1} est*

$$-\sum_{i=1}^{n} a_{ii} = -Trace\, u \,. \tag{3.56}$$

(3.56) permet en fait de définir la trace d'un endomorphisme indépendant du choix de la base.
On remarquera que la trace est une application linéaire :

$$Trace\,(\alpha A + \beta B) = \alpha\, Trace\, A + \beta\, Trace\, B\ . \tag{3.57}$$

3.2 Diagonalisation

3.2.1 Motivation

On souhaite donner une expression du terme général d'une suite donnée par une relation de récurrence linéaire.

La récurrence simple $au_{n+1}+bu_n = 0$, $a \neq 0$, donne une suite géométrique $u_n = (-a/b)^n u_0$.

La récurrence double

$$au_{n+2} + bu_{n+1} + cu_n = 0, \quad a \neq 0, \tag{3.58}$$

se ramène à une récurrence simple vectorielle, pour le vecteur

$$X_n = \begin{pmatrix} u_{n+1} \\ u_n \end{pmatrix} ,$$

$$X_{n+1} = AX_n$$

où

$$A = \begin{pmatrix} -b/a & -c/a \\ 1 & 0 \end{pmatrix} .$$

Recette.
On suppose $a \neq 0$ et $c \neq 0$ pour éviter les cas spéciaux se ramenant à des suites r{ecurrentes simples.
On cherche d'abord une solution sous la forme d'une suite géométrique

$$u_n = r^n .$$

On voit que pour une solution de ce type r doit satisfaire l'**équation caractéristique** :

$$ar^2 + br + c = 0 . \tag{3.59}$$

Si cette équation caractéristique possède deux racines distinctes r_1 et r_2, on cherche la suite solution de (3.58) de conditions initiales $u_0 = x_0$ et $u_1 = x_1$ sous la forme

$$u_n = c_1 r_1^n + c_2 r_2^n. \tag{3.60}$$

On trouve c_1 et c_2 en résolvant un système linéaire de deux équations à deux inconnues.

Interprétation.
Si r est racine de l'équation caractéristique, la condition initiale $X_0 = \begin{pmatrix} r \\ 1 \end{pmatrix}$ donne l'expression simple $X_n = r^n X_0$ parce que $AX_0 = rX_0$. Autrement dit X_0 sera ce qu'on appellera un vecteur propre de A au paragraphe suivant.

3.2.2 Vecteurs propres

Commençons donc par la définition suivante.

Définition 3.2.1
Soit f un endomorphisme de $\mathbb{R}^n$ ou $\mathbb{C}^n$. Un vecteur v est un vecteur propre de f s'il est non nul et si $f(v)$ est colinéaire à v, $f(v) = \lambda v$. Un nombre λ est une valeur propre de f s'il existe un vecteur non nul v tel que $f(v) = \lambda v$. L'espace propre associé à λ est $E_\lambda = \ker(\lambda id - f)$.

La détermination des valeurs propres d'un endomorphisme s'appuie sur la caractérisation suivante :

Proposition 3.2.2
λ est valeur propre de f si et seulement si λ est racine de $P_f = \det(\lambda\, Id - f)$.

Preuve
On peut se ramener à l'étude dans une base donnée $\mathcal{B}$ du système

$$(A - \lambda)X = B\ ,$$

où A est la matrice de u dans la base $\mathcal{B}$.
On a vu que l'existence d'un X non nul solution avec $B = 0$ est caractérisée (système de Cramer) par la condition Dét $(A - \lambda\, Id) \neq 0$.

Exemple 3.2.3
Si la matrice est triangulaire les valeurs propres sont les éléments de la diagonale.

Exemple 3.2.4
La matrice $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ *définit un endomorphisme de $\mathbb{R}^2$ qui n'a aucune valeur propre, et un endomorphisme de $\mathbb{C}^2$ qui en a deux.*

Exemple 3.2.5
La matrice $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ *a zero comme valeur propre mais son espace propre est de dimension* 1.

Nous étudions maintenant sous quelle condition on peut diagonaliser un endomorphisme.

Définition 3.2.6
On dit qu'un endomorphisme est diagonalisable si il admet une base de vecteurs propres. Une matrice $n \times n$ à coefficients réels est diagonalisable sur $\mathbb{R}$ (resp. sur $\mathbb{C}$) si l'endomorphisme de $\mathbb{R}^n$ (resp. de $\mathbb{C}^n$) qu'elle définit est diagonalisable.

On ne peut pas diagonaliser l'exemple précédent.

Proposition 3.2.7
Une matrice $n \times n$ à coefficients réels est diagonalisable sur $\mathbb{R}$ (resp. sur $\mathbb{C}$) si et seulement si il existe une matrice inversible P à coefficients réels (resp. complexes) telle que $P^{-1}AP$ soit diagonale.

Les colonnes de P sont alors des vecteurs propres de l'endomorphisme f défini par A. Les coefficients diagonaux de $P^{-1}AP$ sont les valeurs propres correspondantes.

3.2.3 Conditions nécessaires

Polynômes scindés

Définition 3.2.8
Un polynôme à coefficients réels (resp. complexes) est dit scindé s'il s'écrit comme le produit de polynômes de degré 1.

Autrement dit, un polynôme P de degré d dont le coefficient directeur vaut 1 est scindé si et seulement si il s'écrit

$$P(X) = \prod_{i=1}^{d} (X - z_i) \, , \tag{3.61}$$

où $z_i \in \mathbb{R}$ (resp. $z_i \in \mathbb{C}$).

Exemple 3.2.9
Un polynôme réel du second degré est scindé si et seulement si son discriminant est positif ou nul.

Dans le cas complexe, un théorème célèbre, que nous ne démontrons pas ici, énonce la propriété :

Théorème 3.2.10 *(D'Alembert-Gauss)*
Tout polynôme à coefficients complexes est scindé.

Autrement dit, on peut montrer que si P est de degré k et que le coefficient de X^k est supposé égal à 1, alors on peut toujours trouver k nombres complexes z_i, tels que (3.61) soit vérifiée.
On en déduit immédiatement que dans le cas réel, on a :

Corollaire 3.2.11
Un polynôme réel est scindé si et seulement si toutes ses racines complexes sont en fait réelles.

Proposition 3.2.12
Si f est diagonalisable, alors le polynôme caractéristique de f P_f est scindé.

Ses valeurs propres sont en effet les racines de P_f.

Multiplicités

Définition 3.2.13
Soit P un polynôme, λ une racine de P. La multiplicité de λ est le plus grand entier m tel que P soit divisible par $(x-\lambda)^m$.

Autrement dit, on peut écrire $P(x) = (x-\lambda)^m Q(x)$ où $Q(\lambda) \neq 0$.

Cela généralise les notions de racines simples et doubles des polynômes de degré 2, qui s'étudient facilement à l'aide du discriminant.

On a alors un critère pour déterminer si un polynôme est scindé.

Proposition 3.2.14
Un polynôme à coefficients réels de degré d est scindé si et seulement si la somme des multiplicités des racines réelles vaut d.

Définition 3.2.15
Soient f un endomorphisme et λ une valeur propre de f. La multiplicité de λ comme valeur propre de f est sa multiplicité comme racine de P_f.

On a alors le

Lemme 3.2.16
Soit f un endomorphisme. Alors pour toute valeur propre λ, de multiplicité $m(\lambda)$,

$$\dim E_\lambda \leq m(\lambda).$$

On peut en effet trouver une base de $\mathbb{R}^n$ (ou $\mathbb{C}^n$) constituée d'une base de E_λ et complétée par d'autres vecteurs. Dans cette base, le calcul du déterminant de $(XI - f)$ (propriété des matrices diagonalisées par bloc) met en évidence un facteur $(X - \lambda)^{\dim E_\lambda}$, ce qui démontre l'inégalité.

Proposition 3.2.17
Si f est diagonalisable, alors pour toute valeur propre λ, de multiplicité $m(\lambda)$,

$$\dim E_\lambda = m(\lambda) \ .$$

On a en effet

$$n = \sum_\lambda \dim E_\lambda \leq \sum_\lambda m(\lambda) \leq n \ .$$

L'inégalité n'est possible que si $\dim E_\lambda = m(\lambda)$.

3.2.4 Critère de diagonalisabilité

Théorème 3.2.18
Soit f un endomorphisme. Alors f est diagonalisable si et seulement si les deux conditions suivantes sont satisfaites :

- *P_f est scindé ;*
- *pour toute valeur propre λ, de multiplicité $m(\lambda)$,*

$$\dim E_\lambda = m(\lambda).$$

Corollaire 3.2.19
Soit f un endomorphisme de $\mathbb{R}^n$ (resp. $\mathbb{C}^n$). Si P_f possède n racines réelles (resp. complexes) de multiplicité 1, alors f est diagonalisable.

En effet, comme $\dim E_\lambda \geq 1$, on obtient compte-tenu du lemme précédent $\dim E_\lambda = 1 = m(\lambda)$ et P_f est scindé.

Attention, la réciproque est fausse, comme le montre l'exemple suivant.

Exemple 3.2.20
Une matrice diagonale est diagonalisable, même si elle admet des valeurs propres multiples.

La preuve du théorème 3.2.18 repose sur le lemme suivant.

Lemme 3.2.21
Soient $v_1, \ldots, v_k$ des vecteurs propres de f. On suppose que tous les vecteurs de cette famille relatifs à une même valeur propre sont linéairement indépendants. Alors $v_1, \ldots, v_k$ sont linéairement indépendants.

Indication sur la preuve
Raisonnons avec deux valeurs propres distinctes λ et λ'. La question se ramène à montrer que si $u \in E_\lambda$ et $v \in E_{\lambda'}$, vérifient $u + v = 0$ alors $u = 0$ et $v = 0$. Mais si $u + v = 0$, on a alors $f(u + v) = f(0) = 0$ et $f(u + v) = \lambda u + \lambda' v$.
On déduit de ces calculs que

$$u + v = 0 \ , \ \lambda u + \lambda' v = 0 \ .$$

Ceci implique immédiatement $u = v = 0$.

On peut ensuite pour diagonaliser, choisir dans chaque espace propre E_λ une base et obtenir, en prenant la réunion de ces bases, une base de $\mathbb{R}^n$ (ou $\mathbb{C}^n$).

3.2.5 Pratique de la diagonalisation

Soit A une matrice $n \times n$ à coefficients réels. Essayer de diagonaliser A, c'est d'abord décider si A est diagonalisable ou non sur $\mathbb{R}$ (resp. sur $\mathbb{C}$). Si oui, c'est alors calculer une matrice P telle que $P^{-1}AP$ soit diagonale.

Procédé pratique.
- Calculer et factoriser le polynôme caractéristique P_A.
  Dans le cas réel, si certaines racines sont non réelles, on conclura que A n'est pas diagonalisable sur $\mathbb{R}$. Si toutes les racines sont réelles, on peut continuer.
  On n'a pas de problème si on diagonalise sur $\mathbb{C}$.
- Pour chaque valeur propre λ de multiplicité $m(\lambda) \geq 2$, calculer le rang de $\lambda I - A$. En déduire $\dim(E_\lambda)$. Si $\dim(E_\lambda) < m(\lambda)$, conclure que A n'est pas diagonalisable, ni sur $\mathbb{R}$ ni sur $\mathbb{C}$. Sinon, continuer.
- Pour chaque valeur propre λ, calculer une base de E_λ. Mettre ces bases ensemble, construire la matrice de passage P dont les colonnes sont les vecteurs de la base obtenue.

Remarque 3.2.22
Lors de la dernière étape, il n'est pas nécessaire
- *de vérifier que les vecteurs obtenus forment une base ;*
- *de vérifier que $P^{-1}AP$ est diagonale,*

car c'est automatique.

Exercice 3.2.23
Discuter en fonction de α de la diagonalisabilité de la famille de matrices

$$A_\alpha = \begin{pmatrix} 1+\alpha & 1 \\ -\alpha & 0 \end{pmatrix} \ .$$

Définition 3.2.24
Si $P(x) = \sum_{i=0}^{d} a_i x^i$ est un polynôme et M une matrice carrée, on définit $P(M)$ par :

$$P(M) = a_0 I + a_1 M + \cdots + a_d M^d \ .$$

De même, on peut définir $P(f)$ lorsque f est un endomorphisme.

On vérifie aisément que, si $P = QR$ est un produit de polynômes, alors $P(f) = Q(f) \circ R(f) = R(f) \circ Q(f)$.

Proposition 3.2.25
Soit f un endomorphisme. Soit Q un polynôme tel que $Q(f) = 0$. Alors, pour toute valeur propre λ de f, $Q(\lambda) = 0$.

Il suffit en effet de choisir un vecteur propre v_λ de f et d'observer que $Q(f)v_\lambda = Q(\lambda)v_\lambda$.

Exemple 3.2.26
Projecteurs. Si f est le projecteur sur E parallèlement à F, alors $f \circ f = f$. Les valeurs propres de f sont 0 et 1.

Exemple 3.2.27
Considérons l'exemple d'une symétrie. Si f est la symétrie par rapport à E parallèlement à F, alors $f \circ f = id$. Les valeurs propres de f sont -1 et 1.

3.2.6 Application aux suites définies par une relation de récurrence double

Revenons à l'étude des suites récurrentes et plaçons nous dans le cas où $a \neq 0$ et $c \neq 0$.
Nous avons vu que nous pouvions ramener l'étude à celle de

$$X_{n+1} = AX_n \ .$$

Dans l'esprit de ce qui précède, on doit donc étudier si l'on peut diagonaliser A. Le calcul du polynôme caractéristique donne

$$P_A(X) = X^2 + \frac{b}{a}X + \frac{c}{a} \ .$$

Une valeur propre λ de A doit donc satisfaire

$$a\lambda^2 + b\lambda + c = 0 \ . \tag{3.62}$$

C'est exactement l'équation (3.59) rencontrée dans la sous-section "Motivation".
Les valeurs propres (dans $\mathbb{C}$) sont distinctes si et seulement si $b^2 - 4ac \neq 0$. On les notes λ_1 et λ_2.
Dans ce cas une base de vecteurs propres est constituée des deux vecteurs $\begin{pmatrix} \lambda_1 \\ 1 \end{pmatrix}$ et $\begin{pmatrix} \lambda_2 \\ 1 \end{pmatrix}$. On pose alors

$$P = \begin{pmatrix} \lambda_1 & \lambda_2 \\ 1 & 1 \end{pmatrix} .$$

Par la théorie présentée auparavant, on a

$$\widehat{A} := P^{-1}AP = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$$

Posant $\widehat{X}_n = P^{-1}X_n$, on voit que

$$\widehat{X}_{n+1} = \widehat{A}\widehat{X}_n .$$

La résolution de ce système est immédiate. On trouve que

$$\widehat{X}_n = \alpha_1\lambda_1^n \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \alpha_2\lambda_2^n \begin{pmatrix} 0 \\ 1 \end{pmatrix} .$$

Il n'y a plus qu'à revenir en arrière pour retrouver les formules du paragraphe de motivation (3.60).
On trouve d'abord

$$X_n = P\widehat{X}_n = \alpha_1\lambda_1^n P \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \alpha_2\lambda_2^n P \begin{pmatrix} 0 \\ 1 \end{pmatrix} .$$

D'où

$$X_n = \alpha_1\lambda_1^n \begin{pmatrix} \lambda_1 \\ 1 \end{pmatrix} + \alpha_2\lambda_2^n \begin{pmatrix} \lambda_2 \\ 1 \end{pmatrix} .$$

Prenant la deuxième composante, on retrouve

$$u_n = \alpha_1\lambda_1^n + \alpha_2\lambda_2^n ,$$

qui correspond aux notations près à ce que nous avions intuité directement. Il ne reste alors plus qu'à ajuster les constantes α_1 et α_2 en fonction des données de u_0 et u_1.

Nous avions laissé de côté le cas où l'équation caractéristique avait une racine double. Si l'équation caractéristique a une racine double λ, on cherche la suite solution de (3.58) de conditions initiales $u_0 = x_0$ et $u_1 = x_1$ sous la forme $u_n = c_1\lambda^n + c_2 n\lambda^n$. On trouve c_1 et c_2 en résolvant un système linéaire de deux équations à deux inconnues.

3.3 Application aux systèmes différentiels

3.3.1 Systèmes différentiels à coefficients constants

Propriétés générales

Nous retournons à la recherche des solutions générales du système différentiel :

$$(SD) \qquad dX/dt = AX + B(t) \ ,$$

où $X(t) \in \mathbb{R}^N$ et $B(t) \in \mathbb{R}^N$.

Le premier principe concerne la linéarité. Commençons par une définition. On appelle système homogène (H) associé le système correspondant au second membre $B(t) \equiv 0$:

$$(H) \qquad dX/dt = AX \ .$$

Théorème 3.3.1
Soit (SD) un système différentiel à coefficients constants et (H) le système homogène associé et soit $X_0(t)$ une solution de (SD). Alors toute solution $X(t)$ de (SD) s'écrit sous la forme

$$X(t) = X_0(t) + Z(t)$$

où $Z(t)$ est une solution du système homogène (H).

La démonstration est immédiate, si on observe que $X(t) - X_0(t)$ est effectivement une solution du système homogène. Il est utile d'observer que l'espace des solutions de (H) est un espace vectoriel.

Par conséquent, résoudre (SD), c'est trouver
- une solution particulière $X_0(t)$,
- une base de l'espace vectoriel des solutions de H.

Existence et Unicité.

On commence par redonner la traduction du théorème de Cauchy dans le cas particulier.

Théorème 3.3.2
Supposons que $t \mapsto B(t)$ est continue sur $\mathbb{R}$. Alors, pour tout vecteur $v \in \mathbb{R}^N$, il existe une et une seule solution $X(t)$ du système (SD) définie pour tout $t \in \mathbb{R}$ telle que $X(0) = v$. En particulier, l'espace vectoriel des solutions du système associé homogène est de dimension N.

Exemple élémentaire

Considérons le cas $N = 1$. Le système s'écrit : $y'(t) = ay(t) + b(t)$. On résout d'abord le système homogène. Pour tout $v \in \mathbb{R}$, la solution de (H) telle que $y(0) = v$ est donnée par $y(t) = v \exp at$. L'espace des solutions du système homogène est donc bien de dimension 1.

Pour déterminer la solution du système non-homogène (on dit aussi "avec second membre"), on fait ce qui est communément appelé la méthode de variation des constantes. On écrit : $y(t) = e^{at}z(t)$ et on cherche l'équation vérifiée par $z(t)$. On trouve d'abord :

$$z'(t) = b(t)e^{-at} ,$$

et on est ainsi ramené à la recherche d'une primitive convenable. Pour $t = 0$, on observe que $z(0) = v$ (si on cherche y tel que $y(0) = v$). D'où :

$$z(t) = v + \int_0^t \exp -as\ b(s)\, ds .$$

Ceci conduit finalement à :

$$y(t) = v \exp at + \exp at \int_0^t \exp -as\ b(s)\, ds .$$

Etude du système dans le cas où A a des racines réelles distinctes

Solutions du système homogène
La première information est donnée par :

Théorème 3.3.3
Soit (H) le système homogène. Alors si A admet une valeur propre réelle λ et si v est un vecteur propre associé : $Av = \lambda v$ (avec $v \neq 0$), alors $X(t) = \exp \lambda tv$ est solution de (H).

La démonstration est immédiate, on observe en effet que :

$$X'(t) = \lambda \exp \lambda t\ v = A(X(t)) .$$

Dans le cas favorable, cela conduit au théorème :

Théorème 3.3.4

Supposons que pour une matrice A on soit dans la situation où il existe n valeurs propres réelles distinctes λ_1, λ_2, ..., λ_n. Si u_1, u_2, ...u_n, sont des vecteurs propres associés, alors les solutions $X_j(t) = \exp \lambda_j t\ u_j$ constituent une base de l'espace des solutions de (H).

On reprendra tout ceci en détail dans le cas des systèmes 2×2.

Méthode de variation des constantes

On peut aussi alors faire la variation des constantes de la manière suivante.

On écrit :

$$B(t) = \sum_j b_j(t) X_j(t) \ .$$

On utilise ici que pour tout t, $X_j(t)$ est une base de $\mathbb{R}^n$, ce qui se déduit immédiatement du fait que les u_j forment une base de $\mathbb{R}^n$.

On cherche une solution particulière de $X'(t) = AX(t)$, sous la forme :

$$X(t) = \sum_j c_j(t) X_j(t) \ ,$$

où les $c_j(t)$ sont à déterminer.

En remplaçant dans l'équation, on obtient :

$$\sum_j c_j'(t) X_j(t) = \sum_j b_j(t) X_j(t) \ ,$$

qui conduit à :

$$c_j'(t) = b_j(t) \ , \ \forall j = 1, \cdots, n \ .$$

On peut alors choisir :

$$c_j(t) = \int_0^t b_j(s) ds \ ,$$

pour produire une solution particulière.

Remarque 3.3.5
Rappelons que pour vérifier les hypothèses ci dessus. On peut calculer le déterminant $dét\,(A - \lambda I)$. *C'est un polynôme de degré* n *à coefficients réels (car on suppose ici* A *matrice réelle). On cherche alors les racines de ce polynôme et on vérifie si la condition ci-dessus est satisfaite. Pour chaque racine* λ_j, *on sait que le noyau de* $(A - \lambda_j)$ *est de dimension au moins égale à* 1 *et on peut donc trouver un vecteur propre* u_j.

Systèmes 2×2 homogènes du premier ordre

On considère :

$$\begin{aligned} x'(t) &= ax(t) + by(t) \ , \\ y'(t) &= cx(t) + dy(t) \ . \end{aligned}$$

On va mener une étude complète dans ce cas. Cela nous permettra en particulier de répondre à l'exemple considéré dans la théorie des circuits.

Cas de deux racines réelles distinctes
On a déjà traité ce cas. On regarde donc juste un exemple.

Exemple 3.3.6

$$x'(t) = y(t) \ , \ y'(t) = x(t) \ .$$

La matrice A correspondante a deux valeurs propres réelles distinctes : ± 1. On peut alors trouver la solution telle que $X(0) = (0, 1)$ en écrivant ce vecteur sur la base des vecteurs propres de la matrice A.

Cas de deux racines complexes distinctes
Dans ce cas si A est à coefficients réels, on voit facilement que $\lambda_1 = \overline{\lambda_2}$. Autrement dit, les deux valeurs propres sont complexes conjuguées.

Dans ce cas, il vaut mieux oublier un instant que la question posée était la recherche de solutions réelles. Si on oublie ce point, il est immédiat de trouver deux vecteurs propres (dans $\mathbb{C}^2$) de A. On peut même les choisir tels que : $v_2 = \overline{v_1}$.

On a en effet :

$$Av_1 = \lambda_1 v_1 \ ,$$

qui correspond à l'écriture de deux équations dans $\mathbb{C}$.

Si on prend le complexe conjugué de ces deux équations, et en remarquant que la matrice A est à coefficients réels, on obtient :

$$A\overline{v_1} = \overline{\lambda_1}\overline{v_1} \ .$$

Autrement dit, on a démontré que si v_1 est vecteur propre (dans $\mathbb{C}^2$), pour la valeur propre λ_1, alors le vecteur $\overline{v_1}$ dont les coordonnées dans la base canonique de $\mathbb{C}^2$ sont les conjuguées complexes de celles de v_1 est vecteur propre de A attaché à la valeur propre $\overline{\lambda_1}$.

Toute solution complexe de (H) s'écrit donc :

$$X(t) = c_1 X_1(t) + c_2 X_2(t) \ ,$$

avec $X_2(t) = \overline{X_1(t)}$.

Il est alors facile de reconnaître les solutions réelles, telles que $\overline{X(t)} = X(t)$. On doit juste avoir

$$c_2 = \overline{c_1} \ .$$

Les solutions réelles de (H) sont données par :

$$X(t) = c_1 X_1(t) + \overline{c_1}\overline{X_1(t)} \ .$$

On peut alors redonner une écriture réelle de l'espaces des solutions, en introduisant : $c_1 = \gamma + i\delta$, $\lambda_1 = \mu + i\nu$ et $u_1 = v + iw$, avec a, b, μ, ν réels et v et w dans $\mathbb{R}^2$.

On obtient l'écriture suivante :

$$X(t) = (\gamma + i\delta)(v + iw) \exp \mu t(\cos \nu t + i \sin \nu t) + c.\ c\ ,$$

où " c. c " veut dire "complexe conjugué".

Ceci donne :

$$X(t) = ((\gamma v - \delta w) + i(\delta v + \gamma w)) \exp \mu t(\cos \nu t + i \sin \nu t) + c.\ c$$

ou encore :

$$X(t) = 2((\gamma v - \delta w) \cos \nu t - \sin \nu t(\delta v + \gamma w)) \exp \mu t$$

On peut aussi le réécrire sous la forme :

$$X(t) = 2 \exp \mu t\ ((\gamma \cos \nu t - \delta \sin \nu t)v - (\delta \cos \nu t + \gamma \sin \nu t)w)\ .$$

Notons que le théorème de Cauchy dit a priori que, si on cherche $X(t)$ dans $\mathbb{C}^2$ solution de (H) avec $X(0) \in \mathbb{R}^2$, alors $X(t)$ sera en fait dans $\mathbb{R}^2$.

Pour la résolution du problème avec second membre, on peut procéder comme dans le cas réel. De nouveau le théorème de Cauchy dit a priori que, si on cherche $X(t)$ dans $\mathbb{C}^2$ solution de (SD) avec $X(0) \in \mathbb{R}^2$ et $B(t)$ dans $\mathbb{R}^2$, alors la solution $X(t)$ sera en fait dans $\mathbb{R}^2$.

Exemple 3.3.7

$$x' = -y\ ,\ y' = x\ .$$

Alors le polynôme caractéristique a deux racines i et $-i$. L'espace propre associé à la valeur propre i est donné par

$$-iz_1 - z_2 = 0$$

On peut donc prendre $u = (1, 0)$ et $v = (0, -1)$. Si on prend comme condition initiale $X(0) = (0, 1)$, on trouve : $X(t) = (-\sin t, \cos t)$.

Cas d'une racine double

Ecrivons d'abord que la matrice (2×2) a une racine double. Si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, et si λ est la valeur propre double, on a :

$$2\lambda = a + d\ ,\ ad - bc = \lambda^2\ .$$

On observe alors que :

$$A = \lambda I + N \ ,$$

où N a la propriété que :

$$N^2 = 0 \ .$$

Pour le voir, on se ramène immédiatement au cas $\lambda = 0$ en remplçant a par $a - \lambda$ et c par $c - \lambda$.

Il s'agit de montrer qu'une matrice N qui a zero comme valeur propre double est forcément de carré 0. C'est immédiat par un calcul laissé en exercice.

Deux cas peuvent se présenter :

- ou bien $N = 0$ et on peut choisir pour A deux vecteurs propres linéairement indépendants : les deux vecteurs $(1, 0)$ et $(0, 1)$ font l'affaire ! !
- ou bien N n'est pas l'opérateur nul. Comme $N^2 = 0$, N est de rang 1. Son noyau est de dimension 1. On peut toujours alors prendre un vecteur propre de A comme u_1 (il satisfait $Nu_1 = 0$) et un vecteur u_2 indépendant[10] de u_1 tel que $Nu_2 = u_1$.

On peut vérifier à la main que : $\exp \lambda t \ u_1$ et $\exp \lambda t \ (u_2 + tu_1)$ sont solutions.

En effet :

$$\frac{d}{dt} \exp \lambda t \ (u_2 + tu_1) = \lambda \exp \lambda t (u_2 + tu_1) + \exp \lambda t \ u_1 \ ,$$

et

$$\begin{aligned} &A(\exp \lambda t(u_2 + tu_1)) \\ &= (I + N)(\exp \lambda t \ (u_2 + tu_1))\lambda \exp \lambda t \ (u_2 + tu_1) + \exp \lambda t \ Nu_2 \ . \end{aligned}$$

Remarque 3.3.8
Il est intéressant dans chacun des cas de décrire dans $\mathbb{R}^2$ la courbe décrite par une solution $X(t)$.

3.3.2 Traduction pour les équations différentielles d'ordre n

On regarde l'équation avec second membre :

$$(ed) \qquad \sum_{j=0}^{n} a_j y^{(n-j)}(t) = b(t) \ .$$

[10] Montrons ce dernier point. Soit $\tilde{u}_2$, un vecteur linéairement indépendant de u_1. N n'étant pas nul, on a $N\tilde{u}_2$ non nul et $N(N\tilde{u}_2) = 0$. Donc $N\tilde{u}_2 = \alpha_2 u_1$. On pose alors $u_2 = \dfrac{1}{\alpha_2}\tilde{u}_2$.

Equations différentielles homogènes.

Pour le système homogène, qui est défini par :

$$(eh) \qquad \sum_{j=0}^{n} a_j y^{(n-j)}(t) = 0 \ ,$$

on peut faire la réduction a un système différentiel d'ordre 1 $n \times n$, puis suivre la méthode expliquée pour ce cas.

On peut aussi chercher plus directement des solutions de la forme $\exp \lambda t$, ce qui conduit, en mettant dans l'équation à :

$$(ei) \qquad \Phi(\lambda) := \sum_{j=0}^{n} a_j \lambda^{n-j} = 0 \ .$$

La fonction $\exp \lambda t$ est donc solution du système si et seulement si λ est racine de cette équation. Ceci a déjà été discuté au Chapitre 1.

Il ne reste plus qu'à compléter ce que nous avions expliqué sur la méthode de variation des constantes. On se contente de détailler le cas de l'ordre 2. On considère donc (on peut se ramener au cas $a_0 = 1$ en divisant par a_0) l'équation :

$$(ed) \qquad y''(t) + a_1 y' + a_2 y = b(t) \ .$$

et son équation homogène associée :

$$(eh) \qquad y''(t) + a_1 y' + a_2 y = 0 \ .$$

Dans tous les cas, on vient de montrer (quitte à passer par la recherche de solutions complexes) que l'on pouvait trouver deux solutions linéairement indépendantes $y_1(t)$ et $y_2(t)$. Si on pense à la réduction du système, on tombe sur :

$$X' = \begin{pmatrix} -a_1 & -a_2 \\ 1 & 0 \end{pmatrix} X + \begin{pmatrix} b(t) \\ 0 \end{pmatrix} \ ,$$

et $Y_1(t) = (y_1'(t), y_1(t))$ et $Y_2(t) = (y_2'(t), y_2(t)$ sont les solutions du système homogène associé. La méthode décrite précédemment pour les systèmes dit qu'il faut chercher une solution (pour (SD)) sous la forme :

$$c_1(t)Y_1(t) + c_2(t)Y_2(t)$$

et qu'on doit alors résoudre :

$$c_1'(t)Y_1(t) + c_2'(t)Y_2(t) = \begin{pmatrix} b(t) \\ 0 \end{pmatrix} \ .$$

Ceci conduit au système :

$$\begin{array}{ll} c_1'y_1' + c_2'y_2' & = b(t) \ , \\ c_1'y_1 + c_2'y_2 & = 0 \ . \end{array}$$

C'est sous cette forme qu'on décrit la méthode quand on veut expliquer la recette sans passer par les systèmes. Notons que la matrice $(Y_1(t)\ Y_2(t))$ est pour tout t inversible. Cette matrice qu'on peut écrire sous la forme :

$$M_w(y_1, y_2) = \begin{pmatrix} y_1' & y_2' \\ y_1 & y_2 \end{pmatrix}$$

et est appelée la matrice Wronskienne de y_1 et y_2. Le déterminant de la matrice wronskienne est appelé le wronskien :

$$w(y_1, y_2) = y_1'(t)y_2(t) - y_2'(t)y_1(t) \ .$$

Dire que cette matrice est inversible (propriété que l'on peut vérifier en calculant le wronskien et en vérifiant qu'il est non-nul) est en effet une manière de dire que les solutions Y_1 et Y_2 sont indépendantes dans l'espace des solutions de (H). Notons que $(c_1'(t), c_2'(t))$ sont les coordonnées du vecteur $\begin{pmatrix} b(t) \\ 0 \end{pmatrix}$ dans la base $Y_1(t), Y_2(t)$.

3.3.3 Systèmes généraux

Ils se traitent à l'aide de ce qui a été appris sur les réductions des matrices (diagonalisation, triangulation ....). Avant de présenter une méthode générale, on présente d'abord deux remarques.

Suivi du système par changement de base

La première est que si $X(t)$ est solution de (SD), alors $\tilde{X}(t) := P^{-1}X(t)$ est solution du système :

$$d\tilde{X}/dt = \tilde{A}\tilde{X} + \tilde{B} \ ,$$

avec :

$$\tilde{A} = P^{-1}AP \ , \ \tilde{B} = P^{-1}B \ .$$

Par conséquent, si on trouve une matrice P telle que $\tilde{A}$ a une forme plus simple (par bloc, diagonale, triangulaire), alors on a fait un pas vers la solution !!

Cas d'une matrice triangulaire

Expliquons comment on traite le cas triangulaire sur un exemple très simple, mais la méthode est générale.

Considérons par exemple :

$$\begin{aligned} dx_1/dt &= a_{11}x_1(t) + a_{12}x_2(t) \\ dx_2/dt &= a_{22}x_2(t)\ . \end{aligned}$$

Il suffit de commencer par résoudre explicitement la deuxième équation. Une fois trouvé $x_2(t)$, la première équation n'est plus qu'une équation différentielle pour $x_1(t)$.

Méthode générale

Si on ne vous propose pas de technique particulière la technique suivante conduit à une construction d'un système de solutions du problème (H).

On calcule d'abord le polynôme caractéristique :

$$P(\lambda) = \text{ dét } (\lambda I - A)\ .$$

C'est un polynôme de degré n dont on recherche les racines distinctes α_j $(j = 1, \cdots, q)$ dans $\mathbb{C}$. On définit n_j comme étant la multiplicité de α_j et on a la décomposition suivante de P :

$$P(\lambda) = (\lambda - \alpha_1)^{n_1} \cdots (\lambda - \alpha_q)^{n_q}\ .$$

Pour chaque racine α_j, on cherche une base V_i^j de $\ker(A - \alpha_j)^{n_j}$ $(i = 1, \cdots, n_j)$, dont on peut démontrer que c'est un espace (complexe) dont la dimension est n_j. On peut alors construire, pour $j = 1, \cdots, q$, n_j solutions indépendantes de (H) en considérant :

$$Y_{ij}(t) = \exp \alpha_j t \sum_{p=0}^{n_j - 1} \frac{t^p}{p!}(A - \alpha_j)^p V_i^j\ , \quad \text{pour } i = 1, \cdots, n_j\ .$$

On vérifie directement que l'on produit ainsi n solutions indépendantes, en remarquant que $n = \sum_j n_j$.

On remarque que, quand $n_j = 1$, on retrouve le résultat du théorème 3.3.4.

La méthode de variation des constantes se déroule comme dans le cas où les multiplicités sont égales à 1.

Chapitre 4

Arithmétique (d'après un cours de S. Ruette)

4.1 Les ensembles $\mathbb{N}$ et $\mathbb{Z}$

$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ est l'ensemble des entiers naturels.
$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$ est l'ensemble des entiers relatifs.
$\mathbb{N}^* = \mathbb{N} \setminus \{0\}$ (entiers strictement positifs) et $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ (entiers relatifs non nuls).

Dans ce chapitre, entier sera synonyme d'entier relatif.

Remarque 4.1.1
Si a et b sont des entiers tels que $a < b$ alors $a \leq b - 1$ (et, de façon équivalente, $a + 1 \leq b$).
Par exemple, si $n > 0$ alors $n \geq 1$.

Propriété 4.1.2
Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.

4.2 Divisibilité dans $\mathbb{Z}$

4.2.1 Diviseurs et multiples

Définition 4.2.1
*Soient a et b deux entiers. On dit que a **divise** b s'il existe un entier k tel que $b = ka$. On note $\boldsymbol{a|b}$. On dit également que a est un **diviseur** de b ou que b est un **multiple** de a.*

Exemples 4.2.2
• 3 *divise* 6 *car* $6 = 2 \times 3$. -3 *divise également* 6 *car* $6 = (-2) \times (-3)$.
De façon générale, si $\boldsymbol{b|a}$ *alors* $\boldsymbol{(-b)|a}$.
• *Pour tout* $n \in \mathbb{Z}$, $n+1$ *divise* $n^2 - 1$ *car* $n^2 - 1 = (n-1)(n+1)$.

Diviseurs particuliers.
• Tout entier a divise 0 car $0 = 0.a$, mais 0 ne divise aucun entier $b \neq 0$.
• Tout entier n admet $1, -1, n$ et $-n$ comme diviseurs car $n = 1 \times n = (-1) \times (-n)$.
• Les seuls diviseurs de 1 sont 1 et -1.

4.2.2 Propriétés

Soient a, b, c des entiers relatifs.

Propriété 4.2.3
Si $b \neq 0$ *et* a *divise* b, *alors* $|a| \leq |b|$. *En particulier, tout entier non nul* a *un nombre fini de diviseurs.*

Preuve
On suppose dans un premier temps que a et b sont positifs. a divise b donc il existe un entier k tel que $b = ka$. Comme $b \neq 0$, on a $a \neq 0$ et $k \neq 0$. Comme il s'agit d'entiers naturels, $a \geq 1$ et $k \geq 1$. On a $b - a = a(k-1) \geq 0$ car $a \geq 1$ et $k - 1 \geq 0$. Donc $b - a \geq 0$. On a donc $1 \leq a \leq b$, autrement dit $a \in \{1, 2, \ldots, b\}$ qui est un ensemble fini.
On considère maintenant a et b des entiers relatifs. a divise b donc $|a|$ divise $|b|$. Par ce qui précède $1 \leq |a| \leq |b|$, autrement dit $a \in \{-|b|, \ldots, -1, 1, 2, \ldots, |b|\}$ qui est un ensemble fini.

Propriété 4.2.4
Si a *divise* b *et* b *divise* a, *alors* $a = b$ *ou* $a = -b$.

Preuve
a divise b donc il existe $k \in \mathbb{Z}$ tel que $b = ka$. b divise a donc il existe $k' \in \mathbb{Z}$ tel que $a = k'b$. On a alors $a = kk'a$. Si $a \neq 0$ alors $kk' = 1$, ce qui implique que k et k' sont tous les deux égaux à 1 ou à -1, et par conséquent $a = b$ ou $a = -b$. Si $a = 0$, alors $b = ka = 0$.

Propriété 4.2.5
Si a *divise* b *et* b *divise* c *alors* a *divise* c.

Preuve
Par hypothèse, il existe des entiers k, k' tels que $b = ka$ et $c = k'b$. On a alors $c = kk'a$, donc $\boldsymbol{a|c}$.

Propriété 4.2.6
Si a divise b et c, alors, pour tous entiers n et m, a divise $nb + mc$.

Preuve
Par hypothèse, il existe des entiers k et k' tels que $b = ka$ et $c = k'a$. Donc $nb + mc = (nk + mk')a$ est un multiple de a.

Conséquences : si a divise b et c, alors a divise nb (on prend $m = 0$), a divise $(b + c)$ (on prend $n = m = 1$), a divise $(b - c)$ (on prend $n = 1$, $m = -1$).

La propriété 4.2.6 se généralise sans difficulté à 3 termes ou plus.

Exemples 4.2.7

• *Pour tout $n \in \mathbb{Z}$, 3 divise $3n - 6$ car $\mathbf{3|3}$ et $\mathbf{3|6}$.*

• *Montrons que pour tout $n \in \mathbb{N}$, 9 divise $u_n = 4^n + 6n - 1$. On montre le résultat par récurrence*[1] *sur n.*
– *Initialisation : $u_0 = 0$ est divisible par 9.*
– *On suppose que 9 divise u_n. On écrit*

$$u_{n+1} = 4 \cdot 4^n + 6(n+1) - 1 = 4(u_n - 6n + 1) + 6(n+1) - 1 = 4u_n - 18n + 9 \ .$$

9 divise u_n (hypothèse de récurrence), et 9 divise 18 et 9, donc 9 divise $u_{n+1} = 4u_n + 18n - 9$.
– *Conclusion : 9 divise u_n pour tout $n \in \mathbb{N}$.*

4.3 Nombres premiers

4.3.1 Reconnaître un nombre premier

Définition 4.3.1
*On dit qu'un entier naturel n est **premier** s'il a exactement 2 diviseurs positifs distincts : 1 et n.*

[1] Un raisonnement par récurrence comporte toujours 3 étapes :
– Initialisation : on vérifie la propriété pour $n = n_0$.
– Passage de n à $n+1$: on suppose que la propriété est vraie au rang $n \geq n_0$, on en déduit qu'elle est vraie au rang $n + 1$.
– Conclusion : la propriété est vraie pour tout $n \in \mathbb{N}$, $n \geq n_0$.

Remarque 4.3.2
L'entier 1 *n'est pas premier, il a un seul diviseur positif, qui est* 1.
L'entier 0 *n'est pas premier, il a une infinité de diviseurs.*

Exemple 4.3.3
$2, 3, 5, 7$ *sont des nombres premiers.*

Lemme 4.3.4
Soit n un entier, $n \geq 2$. Son plus petit diviseur positif différent de 1 *est un nombre premier.*
En particulier, tout entier $n \geq 2$ a au moins un diviseur premier.

Preuve
L'ensemble des diviseurs positifs de n différents de 1 est non vide car il contient n. Donc il admet un plus petit élément qu'on note p (propriété 4.1.2). Soit d un diviseur positif de p distinct de 1. On a $d \leq p$ (propriété 4.2.3). De plus, $d|n$ (propriété 4.2.5 avec $d|p$ et $p|n$), donc $d \geq p$ par choix de p. Donc $d = p$. On en déduit que p a un unique diviseur positif différent de 1, donc p est un nombre premier.

Propriété 4.3.5
Soit n un entier, $n \geq 2$. Si n n'est divisible par aucun nombre premier $p \leq \sqrt{n}$, alors n est un nombre premier.

Preuve
Soit $n \geq 2$. On suppose que n n'est pas premier. Soit p le plus petit diviseur positif de n différent de 1. Par le lemme 4.3.4, p est premier. On écrit $n = pq$, avec $q \in \mathbb{N}^*$. Si $q = 1$ alors $n = p$ est premier, ce qui est exclu, donc $q \geq 2$. Comme q est un diviseur positif de n différent de 1, $q \geq p$ par choix de p. Donc $n = pq \geq p^2$, autrement dit $p \leq \sqrt{n}$.
On vient de montrer que si n n'est pas premier alors n est divisible par un nombre premier $p \leq \sqrt{n}$. Par contraposée[2], on en déduit que si n n'est divisible par aucun nombre premier $p \leq \sqrt{n}$, alors n est premier.

Application.
On considère $n = 29$. On a $\sqrt{29} \simeq 5,4$. Les nombres premiers inférieurs à $\sqrt{29}$ sont $2, 3, 5$. Aucun ne divise 29, donc 29 est premier.

[2]Raisonnement par contraposée : on veut montrer que si la propriété P est vraie, alors la propriété Q est vraie aussi ; il est équivalent de montrer que si la propriété Q est fausse, alors la propriété P est fausse aussi.

4.3.2 Ensemble des nombres premiers

Théorème 4.3.6
Il existe une infinité de nombres premiers.

Preuve
Faisons une preuve par l'absurde[3]. Supposons qu'il n'y ait qu'un nombre fini de nombres premiers, notons-les $p_1, \ldots, p_n$. On pose $N = p_1 p_2 \cdots p_n + 1$. $N > 1$ donc N a au moins un diviseur premier p (lemme 4.3.4), et p est nécessairement égal à p_i pour un certain $i \in \{1, \ldots, n\}$. Donc p divise $p_1 p_2 \cdots p_n$. Or p divise également N, donc p divise $N - p_1 p_2 \cdots p_n = 1$ (propriété 4.2.6). C'est impossible.

4.3.3 Décomposition en produit de facteurs premiers

Théorème 4.3.7
Tout entier $n \geq 2$ peut s'écrire de façon unique

$$n = p_1 p_2 \cdots p_r,$$

où $r \in \mathbb{N}^*$ et $p_1, p_2, \ldots, p_r$ sont des nombres premiers tels que

$$p_1 \leq p_2 \leq \cdots \leq p_r \ .$$

Remarque 4.3.8
• *Si $r = 1$, le produit est réduit à un facteur : $n = p_1$.*
• *Si les p_i ne sont pas ordonnés, la décomposition n'est pas unique. Par exemple, $6 = 2 \times 3 = 3 \times 2$.*

Preuve
Existence de la décomposition.
Montrons par récurrence sur n que tout entier $n \geq 2$ peut s'écrire

$$n = p_1 p_2 \cdots p_r \ ,$$

avec $p_1 \leq p_2 \leq \cdots \leq p_r$ des nombres premiers.
• $n = 2$ est premier, on a la décomposition voulue avec $p_1 = 2$ et $r = 1$.
• Soit $n \geq 3$. Supposons que la propriété est vraie pour tout entier k tel que $2 \leq k \leq n - 1$. Par le lemme 4.3.4, le plus petit diviseur positif de n différent de 1 est un nombre premier. On le note p_1. On pose $m = \dfrac{n}{p_1} \in \mathbb{N}^*$.
On distingue deux cas :

[3]Raisonnement par l'absurde : on suppose que la propriété P est fausse, on en déduit un résultat impossible, on conclut que la propriété P est vraie.

– Si $m = 1$ alors $n = p_1$ et on a la décomposition voulue ($r = 1$).
– Si $m \geq 2$, on peut appliquer l'hypothèse de récurrence à m car $m = \dfrac{n}{p_1} \leq \dfrac{n}{2} < n$. On écrit $m = p_2 \cdots p_r$ avec $p_2 \leq \cdots \leq p_r$ des nombres premiers ($r \geq 2$ parce qu'il y a au moins un facteur dans la décomposition de m et qu'on a numéroté à partir de 2). On a alors $n = p_1 m = p_1 p_2 \ldots p_r$. Les nombres premiers $p_2, \ldots, p_r$ divisent n. Comme p_1 est le plus petit diviseur positif de n différent de 1, on a $p_1 \leq p_2 \leq \cdots p_r$. On a donc la décomposition voulue.

• En conclusion, tout entier $n \geq 2$ a une décomposition de la forme voulue.

Unicité de la décomposition.
Nous verrons la preuve de l'unicité après le théorème de Gauss (section 4.6).

La preuve de l'existence de la décomposition en produit de facteurs premiers donne la méthode pour trouver en pratique cette décomposition.

Exemple 4.3.9
$180 = 2 \times 90 = 2 \times 2 \times 45 = 2 \times 2 \times 3 \times 15 = 2 \times 2 \times 3 \times 3 \times 5$.

Quand on a déjà un produit, il suffit de décomposer les facteurs. Exemple : $15 \times 10 = (3 \times 5) \times (2 \times 5) = 2 \times 3 \times 5 \times 5$.

Définition 4.3.10
Soit $n \in \mathbb{N}^*$ et p un nombre premier.
• *Si p divise n, on dit que p est un* ***facteur premier*** *de n*
• *Le plus grand entier k tel que p^k divise n s'appelle* ***l'exposant de*** *p* ***dans*** *n.*

Dans la décomposition en facteurs premiers, on regroupe les nombres premiers identiques et on écrit

$$\boldsymbol{n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}}$$

où $p_1, \ldots, p_s$ sont des nombres premiers tels que $p_1 < p_2 < \cdots < p_s$ et $\alpha_1, \ldots, \alpha_s$ sont des entiers strictement positifs.
L'exposant de p_i dans n est α_i. Si p n'apparaît pas dans la décomposition, son exposant est 0.

Exemple 4.3.11
L'entier n^2 n'a que des exposants pairs car $n^2 = p_1^{2\alpha_1} p_2^{2\alpha_2} \cdots p_s^{2\alpha_s}$.
L'entier $180 = 2^2 \times 3^2 \times 5$ n'est pas un carré. Enfin l'entier $2^2 \times 7^6 = (2 \times 7^3)^2$ est un carré.

Application à la divisibilité :

Théorème 4.3.12
Soient a et b des entiers strictement positifs. Pour tout nombre premier p, notons $\alpha(p)$ l'exposant de p dans a et $\beta(p)$ l'exposant de p dans b. Alors a divise b si et seulement si pour tout nombre premier p on a $\alpha(p) \leq \beta(p)$.

Preuve
Si a divise b alors il existe un entier q tel que $b = aq$. La décomposition en facteurs premiers de b est obtenue en multipliant la décomposition de a par celle de q, donc $\beta(p) \geq \alpha(p)$ pour tout nombre premier p.
Réciproquement, supposons que $\alpha(p) \leq \beta(p)$ pour tout nombre premier p. Soit $p_1, \ldots, p_r$ l'ensemble des facteurs premiers de a et de b. On écrit

$$a = p_1^{\alpha(p_1)} p_2^{\alpha(p_2)} \cdots p_r^{\alpha(p_r)} \text{ et } b = p_1^{\beta(p_1)} p_2^{\beta(p_2)} \cdots p_r^{\beta(p_r)}.$$

On a alors $b = aq$ avec $q = p_1^{\beta(p_1)-\alpha(p_1)} p_2^{\beta(p_1)-\alpha(p_2)} \cdots p_r^{\beta(p_r)-\alpha(p_r)}$ (q est bien un entier car $\beta(p_i) - \alpha(p_i) \geq 0$ par hypothèse). Donc a divise b.

Exemples 4.3.13
• $15 = 3 \times 5 = 2^0 \times 3^1 \times 5^1$ *divise* $180 = 2^2 \times 3^2 \times 5^1$.
• $25 = 5^2$ *ne divise pas* 180.
• $20 = 2^2 \times 5$, *donc les diviseurs positifs de* 20 *sont de la forme* $2^\alpha 5^\beta$ *avec* $\alpha = 0$, 1 *ou* 2 *et* $\beta = 0$ *ou* 1.

4.3.4 Crible d'Ératosthène

Le crible d'Ératosthène[4] est un algorithme pour trouver tous les nombres premiers inférieurs à un entier N fixé.
– On écrit tous les entiers de 1 à N. On barre 1 qui n'est pas premier.
– Le premier entier non barré est 2, il est premier. On barre tous ses multiples sauf lui-même.
– Le premier entier non barré est 3, il est premier. On barre tous ses multiples sauf lui-même.
– On répète l'opération. À chaque étape, le premier entier non barré est premier (car il n'est divisible par aucun nombre premier plus petit). On s'arrête au moment où on considère un nombre premier $p > \sqrt{N}$ (les entiers n avec $\sqrt{N} < n \leq N$ qui ne sont pas encore barrés sont premiers car ils ne sont divisibles par aucun nombre premier $p \leq \sqrt{n}$).
– L'ensemble des nombres premiers inférieurs à N est alors l'ensemble des entiers non barrés.

[4]Ératosthène est un mathématicien et philosophe grec du IIIe siècle avant J.C.

Exemple avec $N = 100$.

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Remarque 4.3.14
Quand on considère le nombre premier p, il suffit de barrer les multiples kp avec $k \geq p$ car les multiples plus petits ont déjà été barrés à une étape précédente.

4.4 Division euclidienne

Théorème 4.4.1
Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Alors il existe des entiers q et r tels que $a = bq + r$ et $0 \leq r < b$. De plus, q et r sont uniques.

Preuve

Existence de q et r.
Supposons pour commencer que $a \in \mathbb{N}$. Comme $b \geq 1$, l'ensemble des $n \in \mathbb{N}$ tels que $bn > a$ est non vide, donc il a un plus petit élément $k \in \mathbb{N}$. Si $k = 0$ alors $a < 0 = kb$, ce qui est exclu, donc $k \geq 1$. Par conséquent, $k - 1 \in \mathbb{N}$ et $b(k-1) \leq a$ par choix de k (k est le plus petit entier n tel que $bn > a$, donc $n = k - 1$ ne vérifie pas cette inégalité). Posons $q = k - 1$. On a : $qb \leq a < (q+1)b = qb + b$. Si on pose $r = a - bq$, on a alors $0 \leq r < b$. Conclusion : $a = bq + r$ avec $0 \leq r < b$.

Supposons maintenant $a \in \mathbb{Z}$, $a < 0$. Posons $a' = -a > 0$. Par ce qui précède, il existe des entiers q' et r' tels que $a' = bq' + r'$ avec $0 \leq r' < b$.
• Si $r' = 0$, $a = -a' = -q'b$. On pose $q = -q'$ et $r = 0$, et on a bien $a = bq + r$.
• Si $r' > 0$, on écrit $a = (-q'b - r') - b + b = b(-q' - 1) + (b - r')$. On pose $q = -q' - 1$ et $r = b - r'$. On a $a = bq + r$ et comme $0 < r' < b$, on a $0 < r < b$. C'est l'écriture recherchée.

Unicité de q et r.
Supposons que $a = bq_1 + r_1 = bq_2 + r_2$ avec $0 \leq r_1 < b$ et $0 \leq r_2 < b$. On a

$b(q_1 - q_2) = r_2 - r_1$, donc $r_2 - r_1$ est un multiple de b. Si $r_2 - r_1 \neq 0$, alors $b \leq |r_2 - r_1|$ (propriété 4.2.3). Or $-b < r_2 - r_1 < b$, et donc $|r_2 - r_1| < b$. Par conséquent, $r_2 - r_1 = 0$, autrement dit $r_1 = r_2$. Comme $b \neq 0$, l'égalité $b(q_1 - q_2) = 0$ entraîne $q_1 - q_2 = 0$, soit $q_1 = q_2$. D'où l'unicité des entiers q et r.
Le théorème ci-dessus nous conduit à la définition suivante.

Définition 4.4.2
*Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Effectuer la **division euclidienne** de a par b, c'est trouver les entiers q et r tels que $a = bq + r$ avec $0 \leq r < b$. q est le **quotient** et r est le **reste** de la division euclidienne de a par b.*

La division euclidienne est la division avec reste qu'on apprend à l'école primaire. Si $a \geq 0$ alors $q \geq 0$.

Exemple 4.4.3
$a = 100$, $b = 7$.

$$\begin{array}{r|l} 100 & 7 \\ \underline{-7} & \underline{14} \\ 30 & \\ \underline{-28} & \\ 2 & \end{array}$$

Le quotient est $q = 14$, le reste est $r = 2$.

Remarque 4.4.4
Le reste de la division euclidienne de a par b est nul si et seulement si b divise a.

Propriété 4.4.5
Soient $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$ et $a = bq + r$ avec $0 \leq r < b$. Alors $q = \left[\frac{a}{b}\right]$ (partie entière de $\frac{a}{b}$).

Preuve
$\frac{a}{b} = \frac{bq + r}{b} = q + \frac{r}{b}$. $0 \leq \frac{r}{b} < 1$, donc $q \leq \frac{a}{b} < q + 1$. Comme $q \in \mathbb{Z}$, q est la partie entière de $\frac{a}{b}$.

Les restes possibles de la division euclidienne de n par b sont $0, 1, 2, \ldots, b-1$. En prenant $b = 2$, on voit que tout entier n peut s'écrire sous la forme $n = 2q$ ($r = 0$) ou $n = 2q + 1$ ($r = 1$).
De même, tout entier n peut s'écrire sous la forme $n = 3k$ ou $n = 3k + 1$ ou $n = 3k + 2$ (en prenant $b = 3$).

Exemple 4.4.6
Soit $n \in \mathbb{Z}$. Montrons que $n(n+1)$ est multiple de 2. On écrit $n = 2k + r$ avec $r = 0$ ou $r = 1$.
– Cas 1 : $r = 0$. $n = 2k$ donc $n(n+1) = 2k(n+1)$.
– Cas 2 : $r = 1$. $n = 2k + 1$ donc $n(n+1) = n(2k+2) = 2n(k+1)$.
Dans les deux cas, $n(n+1)$ est un multiple de 2.

4.5 PGCD et PPCM

4.5.1 Plus Grand Commun Diviseur

Soient a et b deux entiers non nuls. L'entier 1 divise a et b donc a et b ont au moins un diviseur commun. Comme a et b ont un nombre fini de diviseurs, ils ont un nombre fini de diviseurs communs. Ceci justifie la définition suivante.

Définition 4.5.1
Soient $a, b \in \mathbb{Z}^*$. Le plus grand entier qui divise à la fois a et b s'appelle le ***plus grand commun diviseur*** *ou* ***pgcd*** *de a et b. On le note* $\mathbf{pgcd}(a, b)$.

Exemple 4.5.2
$\mathbf{pgcd}(6, 9) = 3$ *car les diviseurs positifs de 6 sont $1, 2, 3, 6$ et les diviseurs positifs de 9 sont $1, 3, 9$.*

Remarques 4.5.3
• $\mathbf{pgcd}(a, b) \geq 1$ *car 1 est un diviseur commun à a et b.*
• $\mathbf{pgcd}(a, b) = \mathbf{pgcd}(b, a)$.
• $\mathbf{pgcd}(a, b) = \mathbf{pgcd}(|a|, |b|)$*, car un nombre et son opposé ont les mêmes diviseurs. On peut donc toujours se ramener à des entiers strictement positifs.*

Propriété 4.5.4
Soient $a, b \in \mathbb{N}^*$. Si a divise b alors $\mathbf{pgcd}(a, b) = a$.

Preuve
Tout diviseur de a est un diviseur de b, et a est le plus grand diviseur de a.

Application de la décomposition en facteurs premiers au calcul de pgcd :

Théorème 4.5.5
Soient $a, b \in \mathbb{N}^*$ et p un nombre premier. Soit $\alpha(p)$ l'exposant de p dans a et $\beta(p)$ l'exposant de p dans b. Alors l'exposant de p dans $\mathbf{pgcd}(a, b)$ *est* $\min(\alpha(p), \beta(p))$.

Preuve
Soit d un diviseur positif commun à a et b. Pour tout nombre premier p, notons $\gamma(p)$ l'exposant de p dans d. d divise a donc $\gamma(p) \leq \alpha(p)$. De même, $\gamma(p) \leq \beta(p)$ car d divise b. Donc $\gamma(p) \leq \min(\alpha(p), \beta(p))$. Réciproquement, tout entier positif dont les exposants sont inférieurs ou égaux à $\min(\alpha(p), \beta(p))$ est un diviseur commun à a et b. Le plus grand diviseur commun est donc obtenu quand pour tout nombre premier p, l'exposant est le plus grand possible, c'est-à-dire égal à $\min(\alpha(p), \beta(p))$.

Exemple 4.5.6

$$\begin{array}{lll} a & = 2^4 \times 5 \times 7^2 & = 2^4 \times 3^0 \times 5^1 \times 7^2 \ ; \\ b & = 2^2 \times 3 \times 5^2 & = 2^2 \times 3^1 \times 5^2 \times 7^0 \ ; \\ d'où & \mathbf{pgcd}(a,b) & = 2^2 \times 3^0 \times 5^1 \times 7^0 = 20 \ . \end{array}$$

4.5.2 Algorithme d'Euclide

Remarque 4.5.7 (Un peu d'histoire)
Euclide est un célèbre mathématicien grec du IIIe siècle avant J.C. Les éléments d'Euclide (traité d'arithmétique et de géométrie) est le premier ouvrage reposant sur des démonstrations.

Lemme 4.5.8 (lemme d'Euclide)
Soient $a, b \in \mathbb{Z}^*$. S'il existe des entiers q et r avec $r \neq 0$ tels que $a = bq + r$ alors les diviseurs communs à a et b sont exactement les diviseurs communs à b et r, et $\mathbf{pgcd}(a,b) = \mathbf{pgcd}(b,r)$.

Preuve
Soit d un diviseur commun à a et b. d divise a et b, donc d divise $a - bq = r$. Donc d est un diviseur commun à b et r.
Réciproquement, si d' un diviseur commun à b et r, alors d' divise $bq + r = a$. Donc d' est un diviseur commun à a et b.
On en déduit que les diviseurs communs à a et b sont exactement les diviseurs communs à b et r. En prenant le plus grand diviseur commun, on obtient $\mathbf{pgcd}(a,b) = \mathbf{pgcd}(b,r)$.

Exemple 4.5.9
Calculons $d = \mathbf{pgcd}(273, 12)$.
On fait la division euclidienne de 273 par 12 :

$$273 = 22 \times 12 \ + \ 9 \ .$$

et donc $d = \mathbf{pgcd}(12, 9)$. *Puis on fait la division euclidienne de* 12 *par* 9 *:*

$$12 = 9 + 3 \ .$$

Donc $d = \mathbf{pgcd}(9, 3)$ *et comme* 3 *divise* 9, *on obtient* $d = 3$.

Algorithme d'Euclide.
Soient $a, b \in \mathbb{N}^*$. On cherche à déterminer $d = \mathbf{pgcd}(a, b)$. On effectue des divisions euclidiennes successives tant que le reste est non nul.

$$\begin{array}{rcll} a & = & bq_1 + r_1 & r_1 < b \qquad d = \mathbf{pgcd}(b, r_1) \\ b & = & r_1 q_2 + r_2 & r_2 < r_1 \qquad d = \mathbf{pgcd}(r_1, r_2) \\ r_1 & = & r_2 q_3 + r_3 & r_3 < r_2 \qquad d = \mathbf{pgcd}(r_2, r_3) \\ \vdots & & & \\ r_{n-2} & = & r_{n-1} q_n + r_n & r_n < r_{n-1} \qquad d = \mathbf{pgcd}(r_{n-1}, r_n) \\ r_{n-1} & = & r_n q_{n+1} + 0 & r_{n+1} = 0 \end{array}$$

La suite r_k est une suite strictement décroissante d'entiers naturels donc, au bout d'un certain temps, on tombe sur un reste nul et l'algorithme s'arrête. Si $r_{n+1} = 0$ alors r_n divise r_{n-1}, donc $\mathbf{pgcd}(r_{n-1}, r_n) = r_n$.

Théorème 4.5.10
Le pgcd de $\boldsymbol{a}$ *et* $\boldsymbol{b}$ *est le dernier reste non nul obtenu par l'algorithme d'Euclide.*

Remarque 4.5.11
Si $r_1 = 0$, *c'est que* b *divise* a, *donc* $\mathbf{pgcd}(a, b) = b$ *(l'algorithme s'arrête immédiatement).*

Théorème 4.5.12
Soient $a, b \in \mathbb{Z}^*$. *Si* d *divise* a *et* b *alors* d *divise* $\mathbf{pgcd}(a, b)$.

Preuve
On se place d'abord dans le cas où $a, b \in \mathbb{N}^*$. On reprend les notations de l'algorithme d'Euclide. Par le lemme d'Euclide, les diviseurs communs à a et b sont les diviseurs communs à b et r_1, à r_1 et r_2,..., à r_{n-1} et r_n. Comme r_n divise r_{n-1}, ce sont les diviseurs de r_n. Par conséquent, d divise r_n puisque c'est un diviseur commun à a et b. Or $r_n = \mathbf{pgcd}(a, b)$ par l'algorithme d'Euclide.
Si $a, b \in \mathbb{Z}^*$, on se ramène au cas précédent en remarquant que les diviseurs communs à a et b sont les diviseurs communs à $|a|$ et $|b|$, et que

$$\mathbf{pgcd}(a, b) = \mathbf{pgcd}(|a|, |b|) \ .$$

Propriété 4.5.13
Si $a, b, k \in \mathbb{Z}^*$, $\mathbf{pgcd}(ka, kb) = |k| \, \mathbf{pgcd}(a, b)$.

Preuve
On se place d'abord dans le cas où $a, b, k \in \mathbb{N}^*$. On note $r_1, \ldots, r_n$ et $r_{n+1} = 0$ les restes obtenus en appliquant l'algorithme d'Euclide à a et b. $a = bq_1 + r_1$ avec $0 \leq r_1 < b$, donc $ka = kbq_1 + kr_1$ avec $0 \leq kr_1 < kb$, donc kr_1 est le reste de la division euclidienne de ka par kb. De même, si on calcule le pgcd de ka et kb avec l'algorithme d'Euclide, on trouve les restes successifs $kr_1, kr_2, \ldots, kr_n$ et $kr_{n+1} = 0$. Donc $\mathbf{pgcd}(ka, kb) = kr_n = k \, \mathbf{pgcd}(a, b)$.
Si $a, b \in \mathbb{Z}^*$, il suffit de remarquer que

$$\mathbf{pgcd}(ka, kb) = \mathbf{pgcd}(|ka|, |kb|) = |k| \, \mathbf{pgcd}(|a|, |b|) = |k| \, \mathbf{pgcd}(a, b) \; .$$

Par exemple, le pgcd de 1200 et 900 se calcule ainsi :

$$\mathbf{pgcd}(1200, 900) = 100 \; \mathbf{pgcd}(12, 9) = 100 \times 3 = 300 \; .$$

4.5.3 Nombres premiers entre eux

Définition 4.5.14
Soient a et b deux entiers non nuls. On dit que a et b sont ***premiers entre eux*** *si* $\mathbf{pgcd}(a, b) = 1$. *On dit aussi que a est premier avec b.*

Exemples 4.5.15
- *15 et 26 sont premiers entre eux.*
- *Deux nombres premiers différents sont premiers entre eux.*

Propriété 4.5.16
Deux entiers strictement positifs sont premiers entre eux si et seulement si ils n'ont aucun facteur premier commun.

Preuve
C'est une conséquence du théorème 4.5.5.

Propriété 4.5.17
Soient a, b deux entiers non nuls et $d = \mathbf{pgcd}(a, b)$. Alors $\dfrac{a}{d}$ et $\dfrac{b}{d}$ sont premiers entre eux.

Preuve
Soit $e = \mathbf{pgcd}\left(\dfrac{a}{d}, \dfrac{b}{d}\right)$. Il faut montrer que $e = 1$. Comme e divise $\dfrac{a}{d}$ et $\dfrac{b}{d}$, il

existe des entiers a', b' tels que $\frac{a}{d} = a'e$ et $\frac{b}{d} = b'e$, donc $a = a'ed$ et $b = b'ed$. Mais ed est un diviseur commun à a et b, donc $ed \leq \mathbf{pgcd}(a, b) = d$. Comme $d > 0$, on peut simplifier l'inégalité : $e \leq 1$. Or $e \geq 1$ car c'est un pgcd, donc $e = 1$.

Une fraction est irréductible si le numérateur et le dénominateur sont premiers entre eux. Pour obtenir une fraction irréductible égale à $\frac{p}{q}$, il suffit de simplifier par le pgcd :
$\frac{p}{q} = \frac{p'}{q'}$ avec $p' = \frac{p}{\mathbf{pgcd}(p,q)}$ et $q' = \frac{q}{\mathbf{pgcd}(p,q)}$.
Par la proposition 4.5.17, $\mathbf{pgcd}(p', q') = 1$.

4.5.4 Plus Petit Commun Multiple

Soient a et b deux entiers non nuls. ab est un multiple commun à a et b, $|ab| > 0$ aussi. Par conséquent, a et b ont au moins un multiple commun strictement positif, ce qui rend possible la définition suivante.

Définition 4.5.18
Soient a et b deux entiers non nuls. Le plus petit entier strictement positif qui est à la fois multiple de a et b s'appelle le ***plus petit commun multiple*** *ou* ***ppcm*** *de a et b. On le note* $\mathbf{ppcm}(a, b)$.

Par exemple, on a : $\mathbf{ppcm}(4, 6) = 12$.
Le ppcm sert à mettre des fractions au même dénominateur :

$$\frac{1}{4} + \frac{1}{6} = \frac{3}{12} + \frac{2}{12} = \frac{5}{12} .$$

Remarques 4.5.19
• $\mathbf{ppcm}(a, b) = \mathbf{ppcm}(b, a)$.
• $\mathbf{ppcm}(a, b) = \mathbf{ppcm}(|a|, |b|)$ *car un nombre et son opposé ont les mêmes multiples. On peut donc toujours se ramener à des entiers strictement positifs.*

Propriété 4.5.20
Soient $a, b \in \mathbb{Z}^*$. Si c est un multiple commun à a et b, alors c est un multiple de $\mathbf{ppcm}(a, b)$.

Preuve
On note $m = \mathbf{ppcm}(a, b) \geq 1$. On fait la division euclidienne de c par m :

$$c = qm + r \text{ avec } 0 \leq r < m .$$

Maintenant a divise m et c et donc a divise $c - qm = r$. De même, b divise r. Par conséquent, r est un multiple commun à a et b avec $0 \leq r < m$. Comme m est le plus petit multiple commun strictement positif, on ne peut pas avoir $0 < r < m$. Donc $r = 0$, et c est un multiple de $m = \mathbf{ppcm}(a, b)$.

Application de la décomposition en facteurs premiers au calcul de ppcm :

Théorème 4.5.21
Soient $a, b \in \mathbb{N}^*$ et p un nombre premier. Soit $\alpha(p)$ l'exposant de p dans a et $\beta(p)$ l'exposant de p dans b. Alors l'exposant de p dans $\mathbf{ppcm}(a, b)$ *est* $\max(\alpha(p), \beta(p))$.

La preuve est analogue à celle du théorème 4.5.5.

Exemple 4.5.22

$$\begin{array}{rll} a & = 2^4 \times 5 \times 7^2 & = 2^4 \times 3^0 \times 5^1 \times 7^2 \ , \\ b & = 2^2 \times 3 \times 5^2 & = 2^2 \times 3^1 \times 5^2 \times 7^0 \ , \\ \textit{d'où} & \mathbf{ppcm}(a, b) & = 2^4 \times 3^1 \times 5^2 \times 7^2 \ . \end{array}$$

Théorème 4.5.23
Soient $a, b \in \mathbb{Z}^*$. Alors

$$\mathbf{pgcd}(a, b) \cdot \mathbf{ppcm}(a, b) = |ab| \ .$$

Preuve
On se place d'abord dans le cas où $a, b \in \mathbb{N}^*$. Soit $p_1, \ldots, p_n$ les nombres premiers qui apparaissent dans les décompositions de a et b.
On écrit $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ et $b = p_1^{\beta_1} \cdots p_n^{\beta_n}$ (avec $\alpha_i, \beta_i \in \mathbb{N}$ pour $i \in \{1, \ldots n\}$).
Par les théorèmes 4.5.5 et 4.5.21, on sait que

$$\mathbf{pgcd}(a, b) = p_1^{\gamma_1} \cdots p_n^{\gamma_n} \text{ avec } \gamma_i = \min(\alpha_i, \beta_i) \text{ pour } i \in \{1, \ldots, n\},$$

$$\mathbf{ppcm}(a, b) = p_1^{\delta_1} \cdots p_n^{\delta_n} \text{ avec } \delta_i = \max(\alpha_i, \beta_i) \text{ pour } i \in \{1, \ldots, n\}.$$

Si $\alpha_i \leq \beta_i$ alors $\gamma_i = \alpha_i$ et $\delta_i = \beta_i$. Si $\alpha_i > \beta_i$ alors $\gamma_i = \beta_i$ et $\delta_i = \alpha_i$. Dans les deux cas, $\gamma_i + \delta_i = \alpha_i + \beta_i$. Donc

$$\mathbf{pgcd}(a, b) \cdot \mathbf{ppcm}(a, b) = p_1^{\gamma_1 + \delta_1} \cdots p_n^{\gamma_n + \delta_n} = p_1^{\alpha_1 + \beta_1} \cdots p_n^{\alpha_n + \beta_n}.$$

Or $ab = p_1^{\alpha_1 + \beta_1} \cdots p_n^{\alpha_n + \beta_n}$, et donc $\mathbf{pgcd}(a, b) \cdot \mathbf{ppcm}(a, b) = ab$.

Si $a, b \in \mathbb{Z}^*$, il suffit de remarquer que

$$\mathbf{pgcd}(a,b) \cdot \mathbf{ppcm}(a,b) = \mathbf{pgcd}(|a|,|b|) \cdot \mathbf{ppcm}(|a|,|b|) = |a||b| \ .$$

Il est facile de calculer le pgcd de deux entiers grâce à l'algorithme d'Euclide. Le théorème 4.5.23 permet de calculer le ppcm à partir du pgcd.

Exemple 4.5.24
Calculons $\mathbf{ppcm}(792, 54)$. *Appliquons tout d'abord l'algorithme d'Euclide :*

$$\begin{aligned} 792 &= 54 \times 14 + 36 \\ 54 &= 36 \times 1 + 18 \\ 36 &= 18 \times 2 + 0 \end{aligned}$$

Donc $\mathbf{pgcd}(792, 54) = 18$. *On en déduit que*

$$\mathbf{ppcm}(792, 54) = \frac{792 \times 54}{18} = 2376 \ .$$

4.6 Théorèmes de Bézout et de Gauss

4.6.1 Théorème de Bézout

Remarque 4.6.1 (Un peu d'histoire)
Étienne Bézout est un mathématicien français du XVIIIe siècle.

Théorème 4.6.2 (théorème de Bézout)
Soient a et b deux entiers non nuls. Il existe des entiers relatifs u et v tels que $au + bv = \mathbf{pgcd}(a, b)$.

Preuve
Soit $E = \{au + bv \mid u \in \mathbb{Z}, v \in \mathbb{Z}, au + bv > 0\}$[5]. E un sous-ensemble de $\mathbb{N}$, et il est non vide car il contient $|a| = a \times (\pm 1) + b \times 0$. Il a donc un plus petit élément, qu'on appelle d. Comme d est un élément de E, il existe des entiers u_0 et v_0 tels que $d = au_0 + bv_0$. Nous allons montrer que $d = \mathbf{pgcd}(a, b)$.
• Montrons que d divise a. On effectue la division euclidienne de a par d : $a = qd + r$ avec $0 \leq r < d$.

$$r = a - qd = a - q(au_0 + bv_0) = a(1 - qu_0) - bqv_0,$$

[5]Notation d'un ensemble : $\{x \mid \ldots\}$ est l'ensemble des x tels que ... ("..." désigne les conditions vérifiées par x ou par les paramètres définissant x). On note également $\{x \ ; \ \ldots\}$ ou $\{x : \ldots\}$.

donc r est de la forme $au + bv$ avec $u = 1 - qu_0$ et $v = -qv_0$. Si $r > 0$, alors $r \in E$, donc $r \geq d$ (d est le plus petit élément de E). C'est impossible puisque $0 \leq r < d$. Par conséquent, $r = 0$ et d divise a.
• De façon analogue, d divise b. Par conséquent, d est un diviseur commun à a et b, donc $d \leq \mathbf{pgcd}(a, b)$.
• $\mathbf{pgcd}(a, b)$ divise a et b, donc il divise $au_0 + bv_0 = d$. Donc $\mathbf{pgcd}(a, b) \leq d$ (rappelons que $d > 0$).
• En conclusion, on a obtenu que $\mathbf{pgcd}(a, b) = d = au_0 + bv_0$.

Théorème 4.6.3 (théorème de Bézout)
Deux entiers non nuls a et b sont premiers entre eux si et seulement s'il existe des entiers u et v tels que $au + bv = 1$.

Preuve
Si $\mathbf{pgcd}(a, b) = 1$, alors par le théorème 4.6.2, il existe des entiers u et v tels que $au + bv = 1$.
Réciproquement, supposons qu'il existe des entiers u et v tels que $au+bv = 1$. Soit $d = \mathbf{pgcd}(a, b)$. d divise a et b, donc d divise $au + bv = 1$, donc $d \leq 1$. Or $d \geq 1$ (c'est un pgcd), donc $d = 1$.

Exemple 4.6.4
n^2 et $n^2 + 1$ sont premiers entre eux car

$$(n^2 + 1) \times 1 \ + \ n^2 \times (-1) = 1 \ .$$

On a ainsi obtenu la relation de Bézout avec $u = 1$ et $v = -1$.

Remarque 4.6.5
Si $au + bv = c \neq 1$, c n'est pas nécessairement égal à $\mathbf{pgcd}(a, b)$.
Par exemple, on a : $a = 4, b = 10$, $4a - b = 6$ et $\mathbf{pgcd}(a, b) = 2$.

4.6.2 Comment trouver une relation de Bézout

Trouver une relation de Bézout pour a et b, c'est trouver des entiers u et v tels que : $au + bv = \mathbf{pgcd}(a, b)$.
On applique l'algorithme d'Euclide à a et b. On part de l'égalité donnant le pgcd, et on « remonte » l'algorithme.

Exemple 4.6.6
$a = 116, b = 10$

$$\begin{array}{rcll} 116 & = & 11 \times 10 \ + \ 6 & (L1) \\ 10 & = & 1 \times 6 \ + \ 4 & (L2) \\ 6 & = & 1 \times 4 \ + \ 2 & (L3) \\ 4 & = & 2 \times 2 \ + \ 0 & \end{array} \qquad \begin{array}{rcl} a & = & 11b + r_1 \\ b & = & r_1 + r_2 \\ r_1 & = & r_2 + \mathbf{pgcd}(a, b) \end{array}$$

Par la ligne (L3), $\mathbf{pgcd}(a,b) = 2$*, et on a l'égalité :*

$$\mathbf{pgcd}(a,b) = r_1 - r_2. \quad (*)$$

On exprime r_2 *(reste avec le numéro le plus élevé) à l'aide de (L2) :*

$$r_2 = b - r_1 \ ,$$

puis on remplace dans $(*)$ *:*

$$\mathbf{pgcd}(a,b) = r_1 - (b - r_1) = 2r_1 - b. \quad (**) \ .$$

On exprime r_1 *à l'aide de (L1) :*

$$r_1 = a - 11b \ ,$$

puis on remplace dans $(**)$ *:*

$$\mathbf{pgcd}(a,b) = 2(a - 11b) - b = 2a - 23b.$$

Par conséquent, la relation $2a - 23b = 2$*, qui se réécrit sous la forme*

$$a \times 2 \ + \ b \times (-23) = 2 \ ,$$

est (appelée) **une relation de Bézout** *pour* a *et* b*, avec ici* $a = 116$*,* $b = 10$*,* $u = 2$ *et* $v = -23$*.*

Remarques 4.6.7

• *Une fois qu'on a calculé* u *et* v*, il est très facile de vérifier que*

$$au + bv = \mathbf{pgcd}(a,b) \ .$$

• u *et* v *ne sont pas uniques. Par exemple, la relation* $7a - 81b = 2$ *est une autre relation de Bézout pour* $a = 116$ *et* $b = 10$*.*

Variante de l'algorithme (plus adapté à la programmation).

On applique l'algorithme d'Euclide à a et b. On note $q_1, \ldots, q_n$ les quotients et $r_1, \ldots, r_n$ les restes obtenus, avec r_n le dernier reste non nul.

– On pose $u_0 = 0$, $v_0 = 1$, $u_1 = 1$, $v_1 = -q_1$.

– Pour $i = 2, \ldots, n$, on définit u_i et v_i par récurrence : $u_i = u_{i-2} - q_i u_{i-1}$ et $v_i = v_{i-2} - q_i v_{i-1}$.

– On a la relation de Bézout suivante : $\boldsymbol{au_n + bv_n = \mathbf{pgcd}(a,b)}$.

Cette égalité repose sur le résultat suivant, dont la preuve est laissée en exercice au lecteur.

Exercice 4.6.8

Vérifier que $au_i + bv_i = r_i$ *pour tout* $i \in \{0, \ldots, n\}$ *(pour* $i = 0$*, on prend* $r_0 = b$*).*

4.6.3 Théorème de Gauss

Remarque 4.6.9 (Un peu d'histoire)
Carl Friedrich Gauss est un célèbre mathématicien allemand – fin XVIIIe début XIXe siècle.

Théorème 4.6.10 (théorème de Gauss)
Soient a, b, c des entiers non nuls. Si a divise bc et si a est premier avec b, alors a divise c.

Preuve
Par le théorème de Bézout, il existe des entiers u et v tels que $au + bv = 1$. Donc $acu + bcv = c$ en multipliant par c. a divise bc par hypothèse, et a divise a, donc a divise $a(cu) + (bc)v = c$.

Propriété 4.6.11
Soient a_1, a_2, b des entiers tels que a_1 et a_2 sont premiers entre eux. Si a_1 et a_2 divisent b, alors le produit $a_1 a_2$ divise b.

Preuve
a_1 divise b, donc il existe un entier b' tel que $b = b'a_1$. a_2 divise $b = b'a_1$ et $\mathbf{pgcd}(a_1, a_2) = 1$, donc a_2 divise b' par le théorème de Gauss. Par conséquent, il existe b'' tel que $b' = b''a_2$, donc $b = b''a_1a_2$.

Remarques 4.6.12
• *On peut avoir $\boldsymbol{a|bc}$ avec a ne divisant ni b ni c. Par exemple, considérons :*

$$60 = 15 \times 4\ .$$

L'entier 6 divise 60 mais 6 ne divise ni 15 ni 4.
• *La propriété 4.6.11 se généralise à trois entiers ou plus :*
Si $a_1, a_2, \ldots, a_n$ sont deux à deux premiers entre eux et divisent b, alors $a_1 a_2 \cdots a_n$ divise b.
Par exemple, si $5, 6$ et 7 divisent n, alors n est un multiple de $5 \times 6 \times 7$.

4.6.4 Résoudre l'équation $ax + by = c$

On veut trouver toutes les solutions entières de l'équation :

$$ax + by = c \qquad (E)$$

où a, b, c sont des entiers donnés avec a, b non nuls, et x, y sont les inconnues.

Existence de solutions :

Théorème 4.6.13
L'équation (E) admet au moins une solution si et seulement si $\mathbf{pgcd}(a, b)$ *divise* c.

Preuve
Supposons que (E) a une solution (x, y). $\mathbf{pgcd}(a, b)$ divise a et b, donc il divise $ax + by = c$.
Réciproquement, supposons que $\mathbf{pgcd}(a, b)$ divise c ; autrement dit, il existe un entier c' tel que $c = c'\mathbf{pgcd}(a, b)$. Par le théorème de Bézout, il existe des entiers u et v tels que $au + bv = \mathbf{pgcd}(a, b)$. Alors $x_0 = c'u$ et $y_0 = c'v$ forment une solution de (E) car

$$ax_0 + by_0 = c'(au + bv) = c'\mathbf{pgcd}(a, b) = c\ .$$

La preuve du théorème 4.6.13 indique comment trouver une solution particulière de (E).

Recherche de toutes les solutions.
On suppose que (x_0, y_0) est une solution de (E). Exprimons les autres solutions en fonction de (x_0, y_0). On a les équivalences :

$$ax + by = c \Longleftrightarrow ax + by = ax_0 + by_0 \Longleftrightarrow a(x - x_0) + b(y - y_0) = 0\ .$$

Soient $X = x - x_0$ et $Y = y - y_0$. Pour résoudre (E), il est équivalent de résoudre

$$aX = -bY \quad (E')\ .$$

Soient $a' = \dfrac{a}{\mathbf{pgcd}(a, b)}$ et $b' = \dfrac{b}{\mathbf{pgcd}(a, b)}$. L'équation (E') est équivalente à

$$a'X = -b'Y\ .$$

Or a' et b' sont premiers entre eux (propriété 4.5.16) et b' divise $a'X$, donc b' divise X par le théorème de Gauss, autrement dit il existe $k \in \mathbb{Z}$ tel que $X = kb'$. On a alors $ka'b' = -b'Y$, et en simplifiant par $b' \neq 0$ on trouve $Y = -ka'$. On vient de montrer qu'une solution de (E') est nécessairement de la forme $X = kb', Y = -ka'$. On vérifie facilement que $X = kb', Y = -ka'$ est bien une solution de (E') pour tout $k \in \mathbb{Z}$. On a donc déterminé exactement les solutions de (E').
Par conséquent, l'ensemble des solutions de (E) est donné par

$$x = x_0 + kb', y = y_0 - ka'\ ,\ \text{ pour tous les } k \in \mathbb{Z}\ ,$$

et on en déduit que :

$$S = \{(x_0 + kb', y_0 - ka') \mid k \in \mathbb{Z}\}$$

avec

$$a' = \frac{a}{\mathbf{pgcd}(a,b)} \text{ et } b' = \frac{b}{\mathbf{pgcd}(a,b)} .$$

Remarque 4.6.14
Si l'équation (E) a au moins une solution, alors elle a une infinité de solutions.

Exemple 4.6.15
Trouver toutes les solutions entières positives de $116x + 10y = 20$.
On résout d'abord l'équation dans $\mathbb{Z}$. *C'est l'équation (E) avec* $a = 116$, $b = 10$ *et* $c = 20$. *On cherche ensuite les solutions vérifiant les conditions demandées.*

Solution particulière :
En b), on a vu que $\mathbf{pgcd}(116, 10) = 2$ *et que* $116 \times 2 - 10 \times 23 = 2$ *est une relation de Bézout pour a et b* ($u = 2, v = -23$)*.Par conséquent,* $c = 10 \times \mathbf{pgcd}(a, b)$ *; donc* $x_0 = 10u = 20$ *et* $y_0 = 10v = -230$ *conviennent.*

Solution générale :
La solution générale est (x, y) *où*

$$x = x_0 + k\frac{b}{\mathbf{pgcd}(a,b)} = 20 + 5k$$

et

$$y = y_0 - k\frac{a}{\mathbf{pgcd}(a,b)} = -230 - 58k ,$$

avec $k \in \mathbb{Z}$.

Solutions positives :

- $x = 20 + 5k \geq 0 \Longleftrightarrow k \geq -\frac{20}{5} = -4$.
- $y = -230 - 58k \geq 0 \Longleftrightarrow k \leq -\frac{230}{58} \approx -3,97 \Longleftrightarrow k \leq -4$ *(k est entier).*
- *x et y sont tous les deux positifs si et seulement si* $k = -4$. *Il y a donc une unique solution :* $(x, y) = (0, 2)$.

4.6.5 Unicité de la décomposition en facteurs premiers

Nous avons vu en Section 4.3 le théorème 4.3.7. Nous avons montré l'existence de cette décomposition et il restait à montrer son unicité.

Lemme 4.6.16
Soient $a_1, \ldots, a_n$ *des entiers (où* $n \in \mathbb{N}^*$*), et p un nombre premier. Si p divise le produit* $a_1 a_2 \ldots a_n$*, alors p divise au moins un des entiers* $a_1, \ldots, a_n$.

Preuve
On montre le résultat par récurrence sur $n \in \mathbb{N}^*$.
• Si $n = 1$, alors p divise a_1.
• Supposons que le résultat est vrai pour $n \in \mathbb{N}^*$ et que p divise $a_1 \dots a_n a_{n+1}$. Si p divise $a_1 \dots a_n$, alors p divise un des entiers $a_1, \dots, a_n$ par hypothèse de récurrence. Si p ne divise pas $b = a_1 \dots a_n$ alors b et p sont premiers entre eux car les seuls diviseurs positifs de p sont 1 et p. p divise ba_n, donc p divise a_{n+1} d'après le théorème de Gauss.
• Conclusion : le résultat est vrai pour tout entier $n \geq 1$.

Preuve [de l'unicité de la décomposition en facteurs premiers]
Supposons que $n = p_1 p_2 \cdots p_r = q_1 q_2 \dots, q_s$, avec $p_1 \leq \cdots \leq p_r$, $q_1 \leq \cdots \leq q_s$ des nombres premiers. Commençons par montrer que $p_1 = q_1$. p_1 divise $q_1 \cdots q_s$ donc par le lemme 4.6.16, p_1 divise q_j pour un certain entier $j \in \{1, \dots, s\}$. Si $p_1 < q_1$, alors $p_1 < q_j$, donc p_1 ne divise pas q_j (les seuls diviseurs positifs de q_j sont 1 et q_j). C'est absurde. On en déduit que $p_1 \geq q_1$. Un raisonnement analogue montre que $q_1 \geq p_1$. Donc $p_1 = q_1$.
Montrons l'unicité de la décomposition par récurrence sur r (nombre de facteurs premiers).
• Si $r = 1$ alors $n = p_1$. Or $p_1 = q_1$ donc $n = q_1$ et $s = 1$.
• Si $r > 1$, posons $n' = \dfrac{n}{p_1}$. Alors $n' = p_2 \dots p_r$ (produit de $r - 1$ facteurs premiers) et $n' = q_2 \dots q_s$. On applique l'hypothèse de récurrence à n' et on obtient : $r = s$, $p_2 = q_2, \dots, p_r = q_r$.
• Conclusion : si $n = p_1 p_2 \cdots p_r = q_1 q_2 \dots, q_s$ comme ci-dessus, alors $r = s$ et $p_1 = q_1, \dots, p_r = q_r$.

4.7 Congruences

Dans la suite, on considère un entier $n \geq 2$.

4.7.1 Définition et propriétés

Définition 4.7.1
Soient $a, b \in \mathbb{Z}$. On dit que ***a et congru à b modulo n*** *si $a - b$ est un multiple de n. On dit aussi que a et b sont congrus modulo n. On note $a \equiv b\ (n)$.*

Il y a d'autres notations : mod n et $[n]$. Notons aussi que

$a \equiv b\ (n) \iff \exists k \in \mathbb{Z}, a = b + kn$
$a \equiv 0\ (n) \iff \mathbf{n|a}$.

Propriété 4.7.2
Soit $a \in \mathbb{Z}$. Il existe un unique entier r tel que $a \equiv r\ (n)$ et $0 \leq r \leq n-1$. r est le reste de la division euclidienne de a par n.

Exemple 4.7.3
Quel jour de la semaine sera le 6 octobre 2007 ? Les jours de la semaine correspondent aux congruences modulo 7 (lundi : $1\ (n)$, mardi : $2\ (n)$, ..., vendredi : $5\ (n)$,...). Le 6 octobre 2006 est un vendredi, le 6 octobre 2007 est dans 365 jours. $5 + 365 = 370$ *et* $370 \equiv 6\ (n)$.
Donc le 6 octobre 2007 sera un samedi.

Propriétés 4.7.4
Soient $a, b, c \in \mathbb{Z}$.
- $a \equiv a\ (n)$.
- *si* $a \equiv b\ (n)$ *alors* $b \equiv a\ (n)$.
- *si* $a \equiv b\ (n)$ *et* $b \equiv c\ (n)$ *alors* $a \equiv c\ (n)$.

Preuve
Les deux premiers points sont immédiats.
Si $a \equiv b\ (n)$ et $b \equiv c\ (n)$, alors n divise $a - b$ et $b - c$, donc n divise $(a - b) + (b - c) = a - c$, donc $a \equiv c\ (n)$

Remarque 4.7.5
En raison de ces trois propriétés, on dit que la congruence modulo n est une relation d'équivalence (comme l'égalité ou le parallélisme de droites).

4.7.2 Compatibilité avec les opérations

Propriétés 4.7.6
Soient $a, b, c, d \in \mathbb{Z}$ tels que $a \equiv b\ (n)$ et $c \equiv d\ (n)$. Alors
- $a + c \equiv b + d\ (n)$.
- $ac \equiv bc\ (n)$.
- *pour tout entier $k \geq 1$,* $a^k \equiv b^k\ (n)$.

Preuve

- n divise $a - b$ et $c - d$, donc n divise $(a - b) + (c - d) = (a + c) - (b + d)$, c'est-à-dire $a + c \equiv b + d\ (n)$.
- $ac - bd = a(c - d) + ad - bd = a(c - d) + (a - b)d$. Comme $c - d$ et $a - b$ sont des multiples de n, $ac - bd$ est également multiple de n. Autrement dit, $ac \equiv bc\ (n)$.

• Du point précédent appliqué à $a \equiv b\ (n)$, on trouve $a^2 \equiv b^2\ (n)$. En réutilisant la propriété précédente, on trouve $a^3 \equiv b^3\ (n)$,..., $a^k \equiv b^k\ (n)$.

On utilise souvent les deux premières propriétés 4.7.6 sous la forme suivante : Si $a \equiv b\ (n)$ alors $a + c \equiv b + c\ (n)$ et $ac \equiv bc\ (n)$.

Remarque 4.7.7
Si $ac \equiv bc\ (n)$, on ne peut pas simplifier par c, même si $c \not\equiv 0$. Exemple : $6 \equiv 2\ (4)$ *mais* $3 \not\equiv 1\ (4)$.

Exemples 4.7.8
• *Calculer* $16^k\ (n)$ *pour tout* $k \in \mathbb{N}$. $16 \equiv -1\ (17)$. *Donc* $16^k \equiv (-1)^k\ (17)$ *pour tout* $k \geq 1$ *et t* $16^0 = 1 = (-1)^0$. *Donc* $16^k \equiv (-1)^k\ (17)$ *pour tout entier* $k \geq 0$.

• *Quelles sont les valeurs possibles de* $a^2\ (5)$ *? Peut-on avoir* $a^2 \equiv 2\ (5)$ *?*
Pour tout $a \in \mathbb{Z}$, *il existe r tel que* $a \equiv r\ (5)$ *avec* $0 \leq r < 5$. *Il y a donc cinq cas :*
– *si* $a \equiv 0\ (5)$, *alors* $a^2 \equiv 0\ (5)$.
– *si* $a \equiv 1\ (5)$, *alors* $a^2 \equiv 1\ (5)$.
– *si* $a \equiv 2\ (5)$, *alors* $a^2 \equiv 4\ (5)$.
– *si* $a \equiv 3\ (5)$, *alors* $a^2 \equiv 9 \equiv 4\ (5)$.
– *si* $a \equiv 4\ (5)$, *alors* $a^2 \equiv 16 \equiv 1\ (5)$.
Conclusion : *L'entier* a^2 *est congru à* $0, 1$ *ou* 4 *modulo* 5. *On n'a jamais* $a^2 \equiv 2\ (5)$.
Remarque :
Si $a \equiv 4\ (5)$, *alors* $a \equiv -1\ (5)$ *et* $a^2 \equiv 1\ (5)$. *De même, si* $a \equiv 3\ (5)$, *alors* $a \equiv -2\ (5)$ *et* $a^2 \equiv 4\ (5)$. *C'est un calcul déjà fait pour* $a \equiv 2\ (5)$.
Quand on fait des calculs (notamment des puissances), il peut être intéressant de prendre comme représentants des nombres (positifs ou négatifs) avec la plus petite valeur absolue.

4.7.3 Critères de divisibilité

Divisibilité par 9
$10 \equiv 1\ (9)$ donc $10^n \equiv 1^n \equiv 1\ (9)$ pour tout entier $n \geq 1$. De plus, $10^0 = 1$ donc $10^n \equiv 1\ (9)$ pour tout $n \in \mathbb{N}$.

$243 = 2 \times 10^2 + 4 \times 10^1 + 3 \times 10^0$ (c'est la définition de l'écriture en base 10). Donc
$243 \equiv 2 \times 1 + 4 \times 1 + 3 \times 1\ (9) \equiv 2 + 4 + 3\ (9) \equiv 0\ (9)$. Donc 243 est un multiplie de 9.

De façon générale, si l'entier N s'écrit $a_k a_{k-1} \dots a_1 a_0$ en base 10, alors

$$N = a_k 10^k + \dots + a_1 10^1 + a_0 10^0 \text{ et } N \equiv a_k + a_{k-1} + \dots + a_1 + a_0\ (9)\ .$$

Par conséquent, N est multiple de 9 si et seulement si la somme de ses chiffres est multiple de 9.
Par exemple, on a :

$$9764 \equiv 9+7+6+1\ (9) \equiv 26\ (9) \equiv 2+6\ (9) \equiv 8\ (9)\ ;$$

donc 9764 n'est pas multiple de 9.

Divisibilité par 3
On a $10 \equiv 1\ (3)$, donc le même raisonnement que pour 9 montre qu'un entier N est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3.

Divisibilité par 5 et par 2
$10 \equiv 0\ (5)$ donc $10^n \equiv 0\ (5)$ pour tout entier $n \geq 1$.
Si l'entier N s'écrit $a_k a_{k-1} \dots a_1 a_0$ en base 10, alors $N \equiv a_0\ (5)$. Donc N est divisible par 5 si et seulement si a_0 est divisible par 5, c'est-à-dire $a_0 = 0$ ou 5.

De même, $10 \equiv 0\ (2)$ donc $N \equiv a_0\ (2)$ et N est divisible par 2 si et seulement si a_0 est un chiffre pair.

On peut naturellement se demander pourquoi on a des critères de divisibilité pour ces valeurs-là ?

On est en base 10.On peut écrire $9 = 10-1$; c'est pour cela que $10 \equiv 1\ (9)$, ce qui conduit au critère de divisibilité par 9. Comme 3 divise 9, on a également $10 \equiv 1\ (3)$ et on a un critère analogue pour 3.
5 est un diviseur de 10, donc $10 \equiv 0\ (5)$, ce qui conduit au critère de divisibilité par 5. De même pour 2, qui est un autre diviseur de 10.

Si on était en base 16 (base utilisée en informatique), on aurait un critère de divisibilité par $15 = 16 - 1$, analogue à celui par 9 en base 10. On aurait également des critères de divisibilité pour les diviseurs de 15 et pour les diviseurs de 16.

4.8 $\mathbb{Z}/n\mathbb{Z}$

On considère un entier $n \geq 2$.

4.8.1 Définition

Définition 4.8.1
Soit $a \in \mathbb{Z}$. La ***classe de congruence modulo n*** *de a est l'ensemble $\{x \in \mathbb{Z} \mid x \equiv a\ (n)\} = \{a + kn \mid k \in \mathbb{Z}\}$. On note cette classe $\overline{a}$.*

$\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des classes de congruence modulo n :

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{a} \mid a \in \mathbb{Z}\} .$$

Propriété 4.8.2
$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$. L'ensemble $\mathbb{Z}/n\mathbb{Z}$ a n éléments.

Preuve
Par définition, $\overline{a} = \overline{b}$ si et seulement si $a \equiv b\ (n)$. Or, pour tout entier a, il existe un unique entier r tel que $a \equiv r\ (n)$ et $0 \leq r \leq n-1$. Donc $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$, et ces classes sont différentes par unicité de r, donc $\mathbb{Z}/n\mathbb{Z}$ a bien n éléments.

Remarque 4.8.3
On peut choisir d'autres représentants pour les classes de congruence. Par exemple, on a :

$$\mathbb{Z}/5\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\} = \{\overline{-2}, \overline{-1}, \overline{0}, \overline{1}, \overline{2}\}$$

car

$$4 \equiv -1\ (5)$$

et

$$3 \equiv -2\ (5) .$$

De même

$$\mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\} = \{\overline{-2}, \overline{-1}, \overline{0}, \overline{1}, \overline{2}, \overline{3}\} .$$

De façon générale, on a :

$$\mathbb{Z}/n\mathbb{Z} = \left\{\overline{-\frac{n-1}{2}}, \ldots, \overline{-1}, \overline{0}, \overline{1}, \ldots, \overline{\frac{n-1}{2}}\right\}$$

si n est impair, et

$$\mathbb{Z}/n\mathbb{Z} = \left\{\overline{-\left(\frac{n}{2}-1\right)}, \ldots, \overline{-1}, \overline{0}, \overline{1}, \ldots, \overline{\frac{n}{2}}\right\}$$

si n est impair.

4.8.2 Opérations dans $\mathbb{Z}/n\mathbb{Z}$

Soient $\alpha, \beta \in \mathbb{Z}/n\mathbb{Z}$ et $a, b \in \mathbb{Z}$ tels que $\alpha = \overline{a}$ et $\beta = \overline{b}$. On définit les opérations suivantes d'addition et de produit par :

$$\alpha + \beta = \overline{a+b}$$

et

$$\alpha\beta = \overline{ab}\ .$$

Ces opérations sont bien définies car le résultat est indépendant du choix des représentants a et b : si $\overline{a} = \overline{a'}$ et $\overline{b} = \overline{b'}$, alors $a \equiv a'\ (n)$ et $b \equiv b'\ (n)$. Or $a + b \equiv a' + b'\ (n)$ et $ab \equiv a'b'\ (n)$, donc $\overline{a+b} = \overline{a'+b'}$ et $\overline{ab} = \overline{a'b'}$.

Propriété 4.8.4
Dans $\mathbb{Z}/n\mathbb{Z}$, $\overline{0}$ est le neutre pour l'addition et $\overline{1}$ est le neutre pour la multiplication :
$\forall \alpha \in \mathbb{Z}/n\mathbb{Z}$, $\alpha + \overline{0} = \alpha$ *et* $\overline{1}\alpha = \alpha$.

Exemple 4.8.5
Voici les tables d'addition et de multiplication dans $\mathbb{Z}/6\mathbb{Z}$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Remarque 4.8.6
Si $\alpha\beta = \overline{0}$, on n'a pas nécessairement $\alpha = \overline{0}$ ou $\beta = \overline{0}$. Exemple : dans $\mathbb{Z}/6\mathbb{Z}$, $\overline{2}.\overline{3} = \overline{0}$.

4.8.3 Éléments inversibles dans $\mathbb{Z}/n\mathbb{Z}$

Si on a l'égalité $\alpha\beta = \alpha\gamma$ dans $\mathbb{Z}/n\mathbb{Z}$, on ne peut pas toujours simplifier par α.
Dans $\mathbb{R}$, simplifier c'est multiplier par l'inverse. Tout réel non nul a un inverse.
Dans $\mathbb{Z}/n\mathbb{Z}$, seuls certains éléments ont un inverse.

Théorème 4.8.7
Soit $\alpha = \overline{a} \in \mathbb{Z}/n\mathbb{Z}$. Il existe un élément $\beta \in \mathbb{Z}/n\mathbb{Z}$ tel que $\alpha\beta = \overline{1}$ si et seulement si a et n sont premiers entre eux. Si β existe, il est unique, et β et appelé l'inverse de α dans $\mathbb{Z}/n\mathbb{Z}$.

Preuve
$\alpha = \overline{a}$ est inversible si et seulement s'il existe $\beta = \overline{b} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\alpha\beta = \overline{1}$, ce qui s'écrit également $ab \equiv 1\ (n)$. Autrement dit, $\alpha = \overline{a}$ est inversible si et seulement s'il existe des entiers b et k tels que $ab = 1 + kn$.

• Si α est inversible, alors il existe b, k tels que $ab = 1 + kn$, autrement dit $ab - kn = 1$. Donc a et n sont premiers entre eux par le théorème de Bézout.

• Réciproquement, si a et n sont premiers entre eux, alors il existe u_0 et v_0 tels que $au_0 + nv_0 = 1$ (théorème de Bézout). Si on prend $b = u_0$, $\beta = \overline{b}$ et $k = -v_0$, alors $ab - kn = 1$, c'est-à-dire $\alpha\beta = \overline{1}$. Donc α est inversible.
Montrons que β est unique. L'ensemble des u, v tels que $au + bv = 1$ est $u = u_0 + nm, v = v_0 - am$, $m \in \mathbb{Z}$. Donc l'ensemble des b tels que $ab \equiv 1\ (n)$ est $b = u_0 + nm, m \in \mathbb{Z}$. Donc $b \equiv u_0\ (n)$ pour tout m, c'est-à-dire que tous les b solutions sont dans la même classe de congruence modulo n. Donc $\beta = \overline{u_0} = \overline{b}$ est l'unique inverse de α dans $\mathbb{Z}/n\mathbb{Z}$.

Éléments particuliers.
• $\overline{0}$ n'est jamais inversible.
• $\overline{1}$ est toujours inversible, d'inverse $\overline{1}$.
• $\overline{n-1} = \overline{-1}$ est toujours inversible, d'inverse $\overline{-1}$.

Remarque 4.8.8
L'inverse de $\alpha \in \mathbb{Z}/n\mathbb{Z}$ est noté α^{-1}. Mais attention avec cette notation : l'inverse de $\overline{2}$ n'est pas $\dfrac{\overline{1}}{2}$ ou $\overline{2^{-1}}$ ($2^{-1} = \dfrac{1}{2}$ n'est pas un entier !), c'est $(\overline{2})^{-1}$.

La preuve du théorème 4.8.7 indique comment calculer l'inverse de $\overline{a}$: en cherchant une relation de Bézout entre a et n. Il n'y a pas de méthode directe.

Exemple 4.8.9
On se place dans $\mathbb{Z}/9\mathbb{Z}$. 9 est premier avec $1, 2, 4, 5, 7, 8$ et n'est pas premier avec $0, 3, 6$, donc les éléments inversibles sont $\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}$. Cherchons les inverses.
• *L'inverse de $\overline{1}$ est $\overline{1}$, l'inverse de $\overline{-1} = \overline{8}$ est $\overline{-1} = \overline{8}$.*
La relation • $9 - 4 \times 2 = 1$ *est une relation de Bézout entre 9 et 2, et donc*

$$\overline{-4} \cdot \overline{2} = \overline{1}\ .$$

L'inverse de $\overline{2}$ *est* $\overline{-4} = \overline{5}$*. On en déduit que l'inverse de* $\overline{5}$ *est* $\overline{2}$*. On en déduit également* $\overline{-2}.\overline{4} = \overline{1}$*, donc* $\overline{-2} = \overline{7}$ *et* $\overline{4}$ *sont inverses l'un de l'autre.*

On a ainsi trouvé tous les inverses :

classe	*inverse*
$\overline{1}$	$\overline{1}$
$\overline{2}$	$\overline{5}$
$\overline{4}$	$\overline{7}$
$\overline{5}$	$\overline{2}$
$\overline{7}$	$\overline{4}$
$\overline{8}$	$\overline{8}$

Propriété 4.8.10
Si $\alpha = \overline{a} \in \mathbb{Z}/n\mathbb{Z}$ *est inversible alors :*
• $\forall b, c \in \mathbb{Z},\ \ ab \equiv ac\ (n) \iff b \equiv c\ (n)$.
• $\forall \beta, \gamma \in \mathbb{Z}/n\mathbb{Z},\ \ \alpha\beta = \alpha\gamma \iff \beta = \gamma$.

Preuve
On sait que $b \equiv c\ (n)$ entraîne que $ab \equiv ac\ (n)$. Montrons la réciproque. Soit $\overline{u}$ l'inverse de $\overline{a}$ dans $\mathbb{Z}/n\mathbb{Z}$, c'est-à-dire $ua \equiv 1\ (n)$. Si $ab \equiv ac\ (n)$, alors $uab \equiv uac\ (n)$, donc $b \equiv c\ (n)$.
Les égalités dans $\mathbb{Z}/n\mathbb{Z}$ s'en déduisent.

Théorème 4.8.11
Si p *est un nombre premier, tous les éléments de* $\mathbb{Z}/p\mathbb{Z}$ *sont inversibles sauf* $\overline{0}$*.*
Si n *n'est pas un nombre premier, il existe au moins un élément différent de* $\overline{0}$ *qui n'est pas inversible dans* $\mathbb{Z}/n\mathbb{Z}$*.*

Preuve
Soit p un nombre premier et $a \in \mathbb{Z}$. Si p divise a, alors $\overline{a} = \overline{0}$. Si p ne divise pas a, alors a et p sont premiers entre eux, donc $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ par le théorème 4.8.7.
Si n n'est pas premier, il existe en entier d qui divise n et tel que $1 < d < n$. $\overline{d} \neq \overline{0}$ et d n'est pas premier avec n donc $\overline{d}$ n'est pas inversible.

4.9 Résoudre l'équation $ax \equiv b\ (n)$

On veut trouver toutes les solutions entières de l'équation :

$$ax \equiv b\ (n) \qquad (E)$$

où a et b sont des entiers donnés avec a non nul, et où $x \in \mathbb{Z}$ est l'inconnue.

Cas où a et n sont premiers entre eux.
Dans ce cas, $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ (théorème 4.8.7). Soit $u \in \mathbb{Z}$ tel que $\overline{u}$ est l'inverse de $\overline{a}$. Par la propriété 4.8.10, l'équation (E) est équivalente à $uax \equiv ub\ (n)$, c'est-à-dire $x \equiv ub\ (n)$.

Conclusion :
L'ensemble des solutions de (E) est

$$\{x \in \mathbb{Z} \mid x \equiv ub\ (n)\} = \{ub + kn \mid k \in \mathbb{Z}\}\ .$$

Il y a une infinité de solutions dans $\mathbb{Z}$.

Exemple 4.9.1
Résoudre dans $\mathbb{Z}$ l'équation $2x \equiv 3\ (9)$.
Donnons la preuve. 2 et 9 sont premiers entre eux, et on a vu que l'inverse de $\overline{2}$ dans $\mathbb{Z}/9\mathbb{Z}$ est $\overline{5}$. Donc cette équation est équivalente à $x \equiv 5.3\ (9)$. Donc x est solution si et seulement si $x \equiv 6\ (9)$. Autrement dit, $S = \{6+9k \mid k \in \mathbb{Z}\}$.

Cas où a et n ne sont pas premiers entre eux.
(E) $\iff \exists k \in \mathbb{Z}, ax - b = kn$.
Soit $d = \mathbf{pgcd}(a, n)$. Si (E) admet une solution x, alors d divise n et a, donc d divise $ax - kn = b$. Dans ce cas, on peut simplifier par $d \neq 0$: on pose $a' = \dfrac{a}{d}$, $b' = \dfrac{b}{d}$, $n' = \dfrac{n}{d}$, et l'égalité $ax - b = kn$ est équivalente à $a'x - b' = kn'$.
On en déduit que (E) est équivalente à l'équation $a'x \equiv b'\ (n')$.

Conclusion :
– si $\mathbf{pgcd}(a, n)$ ne divise pas b, il n'y a pas de solution.
– si $\mathbf{pgcd}(a, n)$ divise b, on divise a, b et n par $\mathbf{pgcd}(a, n)$ et on se ramène à l'équation (E') : $a'x \equiv b'\ (n')$ avec a' et n' premiers entre eux.

Exemples 4.9.2
• *Résoudre dans $\mathbb{Z}$ l'équation (E) : $6x \equiv 3\ (9)$.*
Donnons la preuve, on a $\mathbf{pgcd}(6, 9) = 3$. Ce pgcd divise $b = 3$. Donc l'équation (E) est équivalente à (E') : $2x \equiv 1\ (3)$.
On observe maintenant que : $\overline{2} = \overline{-1}$ dans $\mathbb{Z}/3\mathbb{Z}$; donc son inverse est $\overline{-1} = \overline{2}$. L'équation (E') est donc équivalente à $x \equiv 2\ (3)$.
Conclusion :
L'ensemble des solutions de (E) est $S = \{2 + 3k \mid k \in \mathbb{Z}\}$.

• *Résoudre dans $\mathbb{Z}$ l'équation $4x \equiv 5\ (6)$.*
Pour la preuve, on observe que $\mathbf{pgcd}(4, 6) = 2$. Ce pgcd ne divise pas 5 et donc il n'y a pas de solution : $S = \emptyset$.

Équation dans $\mathbb{Z}/n\mathbb{Z}$.
On veut résoudre $\alpha X = \beta$, où $\alpha, \beta \in \mathbb{Z}/n\mathbb{Z}$ sont donnés $\alpha \neq \overline{0}$, et où $X \in \mathbb{Z}/n\mathbb{Z}$ est l'inconnue.
On se ramène à résoudre $ax \equiv b\ (n)$, avec $\alpha = \overline{a}$, $\beta = \overline{b}$ et $X = \overline{x}$.

Exemples 4.9.3
• *Résoudre $\overline{2}X = \overline{3}$ dans $\mathbb{Z}/9\mathbb{Z}$.*
Preuve : On a vu que x est solution de $2x \equiv 3\ (9)$ si et seulement si $x \equiv 6\ (9)$, autrement dit $\overline{x} = \overline{6}$.
Conclusion :
Il y a une unique solution dans $\mathbb{Z}/9\mathbb{Z}$, qui est $\overline{6}$.

• *Résoudre $\overline{6}X = \overline{3}$ dans $\mathbb{Z}/9\mathbb{Z}$.*
Preuve : On a vu que x est solution de $6x \equiv 3\ (9)$ si et seulement si $x \equiv 2\ (3)$. Quelle est la classe d'équivalence de x modulo 9 ? Si on écrit $x = 9q + r$ avec $0 \leq r \leq 8$, alors $x \equiv r\ (3)$. Comme $r \in \{0, 1, \ldots, 8\}$, $r \equiv 2\ (3)$ si et seulement si $r = 3, 5$ ou 8.
Conclusion :
Il y a 3 solutions dans $\mathbb{Z}/9\mathbb{Z}$, qui sont $\overline{2}, \overline{5}$ et $\overline{8}$.

4.10 Théorème des restes chinois

Le général Han Xing part à la bataille avec 100 soldats. Après la bataille, le général veut compter ses soldats. Il les fait mettre par rang de 3, il en reste 2. Puis il les fait mettre par rang de 5, il en reste 3. Enfin, il les fait mettre par rang de 7, il en reste 2. Combien y a-t-il de soldats ? [6]

Ce problème se traduit de la façon suivante : déterminer x sachant que x est un entier naturel inférieur à 100 tel que $x \equiv 2\ (3)$, $x \equiv 3\ (5)$ et $x \equiv 2\ (7)$.

Théorème 4.10.1 (théorème des restes chinois)
Soient n, m deux entiers positifs premiers entre eux. Pour tous entiers $a, b \in \mathbb{Z}$, le système d'équations

$$(S) \quad \begin{cases} x & \equiv & a\ (n) \\ x & \equiv & b\ (m) \end{cases}$$

a des solutions. De plus, si x_0 est une solution particulière, l'ensemble des solutions de (S) est $\{x \in \mathbb{Z} \mid x \equiv x_0\ (nm)\} = \{x_0 + knm \mid k \in \mathbb{Z}\}$.

Remarque 4.10.2 (Un peu d'histoire)
Le théorème des restes chinois figure dans un livre du mathématicien chinois Qin Jiushao du XIIIe siècle.

[6] Ce problème apparaît dans un livre chinois datant du IIIe siècle.

Preuve
Les entiers n et m sont premiers entre eux donc, par le théorème de Bézout, il existe des entiers u et v tels que $nu + mv = 1$. On commence par chercher des solutions particulières aux systèmes suivants, qu'on appelle systèmes élémentaires :

$$(S1) \quad \left\{ \begin{array}{rcl} x & \equiv & 1\ (n) \\ x & \equiv & 0\ (m) \end{array} \right. \qquad (S2) \quad \left\{ \begin{array}{rcl} x & \equiv & 0\ (n) \\ x & \equiv & 1\ (m) \end{array} \right.$$

$y_1 = mv$ est une solution de (S1) car $y_1 \equiv 1\ (n)$ (relation de Bézout), et y_1 est multiple de m donc $y_1 \equiv 0\ (m)$.
De même, $y_2 = nu$ est une solution de (S2) car y_2 est multiple de n et $y_2 \equiv 1\ (m)$ par la relation de Bézout.

Soit $x_0 = ay_1 + by_2$. Alors $x_0 \equiv a.1 + b.0\ (n) \equiv a\ (n)$ et $x_0 \equiv a.0 + b.1\ (m) \equiv b\ (m)$. Donc x_0 est une solution du système (S). Exprimons toutes les solutions de (S) en fonction de la solution particulière x_0. On a les équivalences suivantes :

$$x \text{ solution de } (S) \Longleftrightarrow \left\{ \begin{array}{rcl} x & \equiv & x_0\ (n) \\ x & \equiv & x_0\ (m) \end{array} \right. \Longleftrightarrow$$
$$\Longleftrightarrow \left\{ \begin{array}{rcl} x - x_0 & \equiv & 0\ (n) \\ x - x_0 & \equiv & 0\ (m) \end{array} \right. \Longleftrightarrow n \text{ et } m \text{ divisent } x - x_0. \qquad (*)$$

Si x est solution de (S), alors n et m divisent $x - x_0$ par $(*)$. Comme n et m sont premiers entre eux, le produit nm divise $x - x_0$ (propriété 4.6.11), donc $x \equiv x_0\ (nm)$.
Réciproquement, si $x \equiv x_0\ (nm)$, alors nm divise $x - x_0$, donc n et m divisent $x - x_0$, et par $(*)$ x est une solution de (S).
Conclusion :
L'entier $x \in \mathbb{Z}$ est solution de (S) si et seulement si $x \equiv x_0\ (nm)$.

Exemple 4.10.3
Résoudre dans $\mathbb{Z}$ le système (S) $\left\{ \begin{array}{rcl} x & \equiv & 3\ (7) \\ x & \equiv & 4\ (15) \end{array} \right.$
Preuve : L'application de l'algorithme d'Euclide à 15 et 7 donne :
$15 = 7 \times 2 + 1$
$7 = 7 \times 1 + 0$
Donc $\mathbf{pgcd}(15, 7) = 1$*, et la relation* $15 - 2 \times 7 = 1$ *est une relation de Bézout entre 15 et 7.*
Résolvons les systèmes élémentaires

$$(S1) \quad \left\{ \begin{array}{rcl} x & \equiv & 1\ (7) \\ x & \equiv & 0\ (15) \end{array} \right.$$

et

$$(S2) \quad \begin{cases} x & \equiv & 0\ (7) \\ x & \equiv & 1\ (15) \end{cases}$$

En utilisant la relation de Bézout ci-dessus, on voit que $y_1 = 15$ *est une solution particulière de (S1) car* $y_1 \equiv 1\ (7)$ *et* y_2 *est un multiple de* 15*, donc* $y_2 \equiv 0\ (15)$*. De même,* $y_2 = -2 \times 7 = -14$ *est une solution particulière de (S2). Donc* $x_0 = 3y_1 + 4y_2 = -11$ *est une solution particulière de (S). Comme* $7 \times 15 = 105$*, l'ensemble des solutions de (S) est l'ensemble des* $x \equiv -11\ (105)$*.* □

Le théorème 4.10.1 se généralise pour un système de k équations :

Théorème 4.10.4
Si $n_1, n_2, \ldots, n_k$ *sont des entiers positifs 2 à 2 premiers entre eux, alors, pour tous* $a_1, \ldots, a_k \in \mathbb{Z}$*, le système*

$$\begin{cases} x & \equiv & a_1\ (n_1) \\ x & \equiv & a_2\ (n_2) \\ & \vdots & \\ x & \equiv & a_k\ (n_k) \end{cases}$$

a des solutions et, si x_0 *est une solution particulière, l'ensemble des solutions est*
$\{x \in \mathbb{Z} \mid x \equiv x_0\ (n_1 n_2 \ldots n_k)\}$.

Pour trouver une solution particulière, on commence par résoudre les systèmes élémentaires. Par exemple, pour $k = 3$, il y a 3 systèmes élémentaires :

$$(S1) \begin{cases} x & \equiv & 1\ (n_1) \\ x & \equiv & 0\ (n_2) \\ x & \equiv & 0\ (n_3) \end{cases} \quad (S2) \begin{cases} x & \equiv & 0\ (n_1) \\ x & \equiv & 1\ (n_2) \\ x & \equiv & 0\ (n_3) \end{cases} \quad (S3) \begin{cases} x & \equiv & 0\ (n_1) \\ x & \equiv & 0\ (n_2) \\ x & \equiv & 1\ (n_3) \end{cases}$$

Comment trouver une solution particulière de (S1) ?
x est solution de (S1) si et seulement si $x \equiv 1\ (n_1)$ et x est divisible par n_2 et n_3. Or n_2 et n_3 sont premiers entre eux, donc x est divisible par n_2 et n_3 si et seulement si x est divisible par $n_2 n_3$. Donc (S1) est équivalent au système

$$(S1') \quad \begin{cases} x & \equiv & 1\ (n_1) \\ x & \equiv & 0\ (n_2 n_3) \end{cases}$$

Comme n_1 est premier avec n_2 et n_3, n_1 n'a aucun facteur premier commun avec n_2 et n_3, donc n_1 et $n_2 n_3$ sont premiers entre eux. Pour trouver une solution du système à 2 équations (S1'), on peut donc appliquer la méthode vue précédemment. On fait de même pour les systèmes (S2) et (S3).

Une fois qu'on a trouvé y_1, y_2, y_3 des solutions particulières de (S1), (S2), (S3), on vérifie facilement que $x_0 = a_1y_1 + a_2y_2 + a_3y_3$ est une solution de

$$\left\{ \begin{array}{rcl} x & \equiv & a_1 \ (n_1) \\ x & \equiv & a_2 \ (n_2) \\ x & \equiv & a_3 \ (n_3) \end{array} \right.$$

Le théorème affirme alors que l'ensemble des solutions est l'ensemble des entiers $x \equiv x_0 \ (n_1n_2n_3)$.

Exemple 4.10.5
Revenons au problème de l'armée chinoise. Le nombre de soldats est solution du système

$$(S) \quad \left\{ \begin{array}{rcl} x & \equiv & 2 \ (3) \\ x & \equiv & 3 \ (5) \\ x & \equiv & 2 \ (7) \end{array} \right.$$

Les nombres 3, 5 *et* 7 *n'ont pas de facteur premier commun et sont donc* 2 *à* 2 *premiers entre eux.*

Le premier système élémentaire est $(S1)$ $\left\{ \begin{array}{rcl} x & \equiv & 1 \ (3) \\ x & \equiv & 0 \ (5) \\ x & \equiv & 0 \ (7) \end{array} \right.$ $\iff$ $(S1')$ $\left\{ \begin{array}{rcl} x & \equiv & 1 \ (3) \\ x & \equiv & 0 \ (35) \end{array} \right.$

Cherchons une relation de Bézout entre 3 *et* 35. *L'algorithme d'Euclide donne :*

$$\left\{ \begin{array}{l} 35 = 11 \times 3 + 2 \\ 3 = 2 + 1 \ . \end{array} \right.$$

La relation de Bézout entre 3 *et* 35 *est donc :*

$$1 = 3 - 2 = 3 - (35 - 11 \times 3) = 12 \times 3 \ - \ 35 \ .$$

On en déduit que $y_1 = -35$ *est une solution de (S1'), donc de (S1).*

Le deuxième système élémentaire est $(S2)$ $\left\{ \begin{array}{rcl} x & \equiv & 0 \ (3) \\ x & \equiv & 1 \ (5) \\ x & \equiv & 0 \ (7) \end{array} \right.$ $\iff$ $(S2')$ $\left\{ \begin{array}{rcl} x & \equiv & 1 \ (5) \\ x & \equiv & 0 \ (21) \end{array} \right.$

L'algorithme d'Euclide pour 21 *et* 5 *donne :*

$$21 = 4 \times 5 \ + \ 1 \ .$$

La relation de Bézout entre 5 *et* 21 *est donc :*

$$1 = 21 \ - \ 4 \times 5 \ .$$

On en déduit que $y_2 = 21$ *est une solution de (S2).*

Le troisième système élémentaire est

$$(S3)\ \begin{cases} x & \equiv & 0\ (3) \\ x & \equiv & 0\ (5) \\ x & \equiv & 1\ (7) \end{cases} \iff (S3')\ \begin{cases} x & \equiv & 1\ (7) \\ x & \equiv & 0\ (15) \end{cases}$$

L'algorithme d'Euclide pour 15 *et* 7 *est :*

$$15 = 2 \times 7\ +\ 1\ .$$

On obtient alors la relation de Bézout entre 15 *et* 7 *:*

$$1 = 15\ -\ 2 \times 7\ .$$

On en déduit que $y_3 = 15$ *est une solution de (S3).*

$x_0 = 2y_1 + 3y_2 + 2y_3 = 23$ *est donc une solution particulière du système initial (S). L'ensemble des solutions est donc l'ensemble des* x *congrus à* 23 *modulo* 105*, (car* $3 \times 5 \times 7 = 105$*). Par conséquent, la seule solution inférieure ou égale à* 100 *est* $x = 23$*.*

Remarque 4.10.6
Une fois qu'on a trouvé y_1, y_2, y_3*, on peut résoudre sans calcul supplémentaire tous les systèmes de la forme :*

$$\begin{cases} x & \equiv & a\ (3) \\ x & \equiv & b\ (5) \\ x & \equiv & c\ (7) \end{cases}$$

Les solutions sont les $x \equiv ay_1 + by_2 + cy_3\ (105)$*.*

4.11 Petit théorème de Fermat

Remarque 4.11.1 (Un peu d'histoire)
Pierre de Fermat est un mathématicien français du XVIIe siècle.

Théorème 4.11.2 (Petit théorème de Fermat)
Soient p *un nombre premier et* x *un entier. Alors :*
- $x^p \equiv x\ (p)$*,*
- *si* p *ne divise pas* x*, alors* $x^{p-1} \equiv 1\ (p)$*.*

Lemme 4.11.3
Soit p *un nombre premier et un* k *un entier tel que* $1 \leq k \leq p-1$*. Alors* p *divise* C_p^k*.*

Preuve
$C_p^k = \dfrac{p!}{k!(p-k)!}$ donc $p! = k!(p-k)!C_p^k$. Or $p! = 1 \times 2 \times \cdots \times p$, donc p divise $k!(p-k)!C_p^k$. Comme p est premier, ceci implique que p divise soit $k!$, soit $(p-k)!$, soit C_p^k.
• Si p divise $k! = 1 \times \cdots \times k$, alors p divise un des facteurs (p est premier), autrement dit il existe $i \in \{1, \ldots, k\}$ tel que p divise i. Or $1 \leq i \leq k < p$, donc c'est impossible.
• De même, p ne peut pas diviser $(p-k)! = 1 \times \cdots \times (p-k)$ car $(p-k) < p$.
• Par conséquent, p divise C_p^k.

Preuve [du théorème de Fermat]
On traite à part le cas $p = 2$. Soit $x \in \mathbb{Z}$. Si 2 divise x alors $x \equiv 0\ (2)$ et $x^2 \equiv 0\ (2) \equiv x\ (2)$. Si 2 ne divise pas x, alors $x \equiv 1\ (2)$ et $x^2 \equiv 1\ (2) \equiv x\ (2)$. Ceci prouve le théorème pour $p = 2$.

On suppose dans la suite de la preuve que $p > 2$. Montrons par récurrence sur $x \in \mathbb{N}$ que $x^p \equiv x\ (p)$.
• Si $x = 0$, alors $x^p \equiv 0\ (p) \equiv x\ (p)$.
• Supposons que $x^p \equiv x\ (p)$ pour $x \in \mathbb{N}$. Par la formule du binôme,

$$(x+1)^p = x^p + C_p^{p-1}x^{p-1} + \cdots + C_p^k x^k + \cdots + C_p^1 x + 1.$$

Par le lemme 4.11.3, $C_p^k \equiv 0\ (p)$ pour tout $k \in \{1, \ldots, p-1\}$, donc

$$(x+1)^p \equiv x^p + 0 + \cdots + 0 + 1\ (p)\ .$$

Or $x^p \equiv x\ (p)$ par hypothèse de récurrence, donc

$$(x+1)^p \equiv x + 1\ (p)\ ,$$

ce qui est la propriété au rang $x+1$.
• Conclusion : $x^p \equiv x\ (p)$ pour tout $x \in \mathbb{N}$.

Si $x \in \mathbb{Z}$, $x < 0$, on pose $y = -x$. Comme p est premier et différent de 2, p est impair et $x^p = (-y)^p = -y^p$. Par ce qui précède, $y^p \equiv y\ (p)$, donc $x^p \equiv -y\ (p) \equiv x\ (p)$. Ceci termine la preuve du premier point du théorème.

Si x n'est pas un multiple de p, alors $\overline{x}$ est inversible dans $\mathbb{Z}/p\mathbb{Z}$ (théorème 4.8.11). Si $\overline{u}$ est son inverse dans $\mathbb{Z}/p\mathbb{Z}$, alors $ux \equiv 1\ (p)$. Par le premier point du théorème, $x^p \equiv x\ (p)$ donc, en multipliant par u, on trouve $x^{p-1} \equiv 1\ (p)$. Ceci prouve le second point du théorème.

Exercice 4.11.4
Quel est le reste de la division euclidienne de 42^{2006} *par* 5 *?*

Preuve : L'entier 2 *est le reste de la division euclidienne de* 42 *par* 5*, autrement dit* $42 \equiv 2\ (5)$*. Donc*

$$42^{2006} \equiv 2^{2006}\ (5)\ .$$

Par le théorème de Fermat, $2^4 \equiv 1\ (5)$*, donc* $2^{4k} \equiv 1\ (5)$ *pour tout entier* $k \in \mathbb{N}$*. Effectuons la division euclidienne de* 2006 *par* 4*. On a bien sûr :*

$$2006 = 4 \times 501\ +\ 2\ .$$

On en déduit que

$$2^{2006} \equiv 2^{4\times 501} \cdot 2^2\ (5) \equiv 1 \times 4\ (5)\ .$$

Donc

$$42^{2006} \equiv 4\ (5)\ ,$$

ce qui signifie exactement que 4 *est le reste de la division euclidienne de* 42^{2006} *par* 5*.*

Pour calculer $x^n\ (p)$ quand $x \not\equiv 0\ (p)$, on utilise souvent le théorème de Fermat comme dans l'exemple. Si on écrit

$$n = q(p-1) + r\ ,$$

qui n'est rien d'autre que la division euclidienne de n par $p-1$, alors

$$x^n \equiv (x^{p-1})^q \cdot x^r\ (p) \equiv x^r\ (p)$$

car

$$x^{p-1} \equiv 1\ (p)\ .$$

4.12 Cryptographie

La cryptographie désigne les méthodes de codage permettant de transmettre des messages de telle manière que seule le destinataire peut lire le message. Ainsi, si une tierce personne intercepte le message, elle ne peut pas le comprendre.

4.12.1 Cryptographie à clé secrète

Dans la cryptographie à clé secrète, l'algorithme de décodage se déduit facilement de l'algorithme de codage. L'algorithme de codage doit donc être gardé secret, il est connu uniquement de l'expéditeur et du destinataire.

Exemple élémentaire : cryptage par décalage

On remplace chaque lettre du message par la lettre suivante dans l'alphabet. Par exemple, le mot MARS devient après cryptage NBST. On décode en remplaçant chaque lettre par la lettre précédente dans l'alphabet.

Cryptage affine
On choisit des entiers a et b avec a premier avec 26. La clé est donc cette paire (a, b) que l'expéditeur et le destinataire ont à disposition.

Les opérations de codage et de décodage s'effectuent ainsi.

Codage :
On remplace chaque lettre par son rang dans l'alphabet, puis on remplace chaque entier x associé à une lettre par l'entier y tel que $y \equiv ax + b\ (26)$, avec $1 \leq y \leq 26$. y est donc la version codée de x.

Décodage :
Par hypothèse, $\overline{a}$ est inversible dans $\mathbb{Z}/26\mathbb{Z}$, on note $\overline{u}$ son inverse, c'est-à-dire $ua \equiv 1\ (26)$. Alors

$$u(y - b) \equiv uax\ (26) \equiv x\ (26)\ .$$

Pour décoder, on calcule donc $x' \equiv u(y - b)\ (26)$, en choisissant x' tel que $1 \leq x' \leq 26$. Alors $x' = x$, et on a retrouvé la lettre de départ.

Traitons à titre d'exemple le cas ou la clé secrète est : $a = 3, b = 5$.
Pour trouver u, on applique l'algorithme d'Euclide à 3 et 26 :

$$26 = 3 \times 8\ +\ 2\ ,\ 3 = 2 + 1\ .$$

On obtient la relation de Bézout entre 3 et 26 en écrivant :

$$1 = 3 - 2 = 3 - (26 - 3 \times 8) = 9 \times 3\ -\ 26\ .$$

On peut donc prendre $u = 9$.

Codage :
Prenons le mot MARS. Il correspond en utilisant le rang des lettres qui composent le mot à la suite de nombre $(13, 1, 18, 19)$. Son codage est la suite $(18, 8, 7, 10)$, correspondnant au mot RHGJ.
En effet, on a $3 \times 13\ +\ 5 \equiv 18\ (26)$, $3 \times 1\ +\ 5 \equiv 8\ (26)$, $3 \times 18\ +\ 5 \equiv 7\ (26)$, $3 \times 19\ +\ 5 \equiv 10\ (26)$,

Décodage :
On vérifie qu'en calculant $x' \equiv 9(y - 5)\ (26)$ pour chaque entier du message codé $(18, 8, 7, 10)$, on retrouve le message d'origine $(13, 1, 18, 19)$.

Dans les algorithmes à clés secrètes, le problème le plus important réside dans l'échange de la clé entre l'expéditeur et le destinataire. Si quelqu'un intercepte la clé de codage, il peut décoder n'importe quel message.

4.12.2 Cryptographie à clé publique

Dans la cryptographie à clé publique, l'algorithme de codage est connu de tout le monde. L'algorithme de décodage, connu uniquement du destinataire, ne peut pas se déduire de l'algorithme de codage.

Système de cryptographie RSA[7]
– p et q sont 2 nombres premiers différents (très grands) et $n = pq$.
– On choisit un entier positif e premier avec $m = (p-1)(q-1)$.
– On détermine un entier positif d tel que $ed \equiv 1\ (m)$ ($\overline{d}$ est l'inverse de $\overline{e}$ dans $\mathbb{Z}/m\mathbb{Z}$).

le couple (n, e) est la **clé publique** : on la communique à tout le monde.
Les entiers p, q et d sont gardés secrets par le destinataire.

Codage
Le message est un entier M avec $0 \leq M \leq n-1$
(si on veut envoyer un message plus long, on le découpe en plusieurs blocs).
L'expéditeur calcule l'entier $C \equiv M^e\ (n)$ avec $0 \leq C \leq n-1$. Il envoie le message codé C.

Décodage
Le destinataire calcule $M' \equiv C^d\ (n)$ avec $0 \leq M' \leq n-1$.

Propriété : $M' = M$.

Lemme 4.12.1
Soient p et q deux nombres premiers différents et $k \in \mathbb{N}$ tel que $k \equiv 1\ ((p-1)(q-1))$. Alors, pour tout entier $x \in \mathbb{Z}$,

$$x^k \equiv x\ (pq)\ .$$

Preuve
On écrit $k = i(p-1)(q-1)+1$. L'entier i est positif car $p-1 \geq 1, q-1 \geq 1$ et $k \geq 0$. Montrons d'abord que $x^k \equiv x\ (p)$.
• Si p divise x, alors $x \equiv 0\ (p)$ donc $x^k \equiv 0\ (p) \equiv x\ (p)$.
• Si p ne divise pas x, alors $x^{p-1} \equiv 1(p)$ par le petit théorème de Fermat. On a

$$x^k = x^{i(p-1)(q-1)+1} = (x^{p-1})^{i(q-1)} \cdot x\ ,$$

et donc

$$x^k \equiv 1^{i(q-1)} \cdot x\ (p) \equiv x\ (p)\ .$$

Pour tout $x \in \mathbb{Z}$, on a donc $x^k \equiv x\ (p)$.

[7]Le système RSA date de 1978, son vient des initiales de ses trois auteurs : Rivest, Shamir, Adleman

Le même argument montre que

$$\forall x \in \mathbb{Z},\ x^k \equiv x\ (q).$$

Ceci montre que, pour tout entier x, p et q divisent $x^k - x$. Comme p et q sont premiers entre eux, le produit pq divise $x^k - x$, autrement dit $x^k \equiv x\ (pq)$.

Preuve [de la propriété permettant le décodage de RSA]
Par définition,

$$M' \equiv C^d\ (pq) \equiv M^{ed}\ (pq)\ ,$$

et

$$ed \equiv 1\ ((p-1)(q-1))\ .$$

Par le lemme 4.12.1 (appliqué à $x = M$ et $k = ed$),

$$M^{ed} \equiv M\ (pq)\ .$$

Par conséquent,

$$M' \equiv M\ (pq)\ .$$

Or $0 \leq M < pq$ et $0 \leq M' < pq$, et donc nécessairement $M' = M$.

Pourquoi ne peut-on pas décrypter le cryptage RSA ?

L'efficacité du cryptage RSA réside dans le fait que décoder sans connaître la clé secrète demanderait des calculs beaucoup trop importants.
Pour retrouver le message initial M à partir du message codé C, on a besoin de connaître d. L'entier d se calcule facilement à partir de e si on connaît p et q (à l'aide de l'algorithme d'Euclide appliqué à e et $m = (p-1)(q-1)$). Tout le monde connaît l'entier n, donc, en théorie, on peut retrouver p et q en décomposant n en facteurs premiers. En pratique, la décomposition en facteurs premiers est très difficile et prend énormément de temps quand les entiers sont grands. À l'inverse, multiplier les entiers p et q pour obtenir n est très facile. De plus, on dispose d'algorithmes assez rapides pour trouver de grand nombres premiers.
On utilise actuellement des nombres premiers p, q d'environ 100 chiffres, le produit $n = pq$ a donc environ 200 chiffres. Même les ordinateurs les plus puissants sont incapables de mener à bien la décomposition en facteurs premiers d'un entier aussi grand.