le cnam

UTC 501

Outils mathématiques pour l'informatique

Didier Alquié

Version 1.0 du 02/01/2024

Chapitre 1

Théorie des ensembles. Éléments de logique. Techniques de démonstration

1.1 Introduction

L'objectif de ce chapitre est de donner ou de rappeler un vocabulaire et une base méthodologique très générale sur la notion d'ensemble, d'élément, de propositions, et d'opérations logiques.

1.2 Rappels de théorie des ensembles

On suppose le lecteur familier avec les notions d'élément d'intersection, de réunion, etc. ainsi qu'avec les fonctions (applications, injections, surjections, bijections) d'un ensemble vers un autre. On les rappelle ici brièvement afin de fixer les définitions et notations une fois pour toutes.

Ensembles

1. l'appartenance d'un élément x à un ensemble E est notée $x \in E$ ou $E \ni x$
2. l'inclusion de A dans E est notée $A \subset E$ ou $E \supset A$
3. l'intersection et la réunion de A et B sont notées $A \cap B$ et $A \cup B$
4. lorsque la réunion $A \cup B$ est *disjointe*, i.e. $A \cap B = \emptyset$, elle est parfois notée $A \sqcup B$.
5. la différence de A et B est notée $A - B$ ou $A \backslash B$. C'est l'ensemble des éléments de A qui ne sont pas dans B. Il n'est pas nécessaire de supposer que $B \subset A$.
6. la différence symétrique de A et B est l'ensemble des éléments qui sont dans l'un exclusivement des deux ensembles A et B. À ce titre, l'appellation *union exclusive* serait plus appropriée. Elle est notée $A \Delta B$. On a la propriété (élémentaire)

$$A \Delta B = (A - B) \sqcup (B - A) = (A \cup B) - (A \cap B)$$

Fonctions

1. une fonction $f : \ E \to F$ est un objet qui à tout élément de départ associe 0 ou 1 élément image dans F
2. l'ensemble de définition de f est l'ensemble des points de E ayant exactement une image par f
3. l'ensemble image $f(E)$ est l'ensemble des points de F ayant au moins un antécédent dans E
4. application : tout point de E a exactement une image
5. injection : application + tout point de F a au plus un antécédent
6. surjection : application + tout point de F a au moins un antécédent
7. bijection : application + tout point de F a exactement un antécédent

Propriétés

Pour deux ensembles E et F **quelconques**

1. Il existe toujours soit une injection de E dans F, soit une injection de F dans E.
2. Il existe un injection de E dans F si et seulement s'il existe une surjection de F dans E
3. (Théorème de cantor-Bernstein) s'il existe une injection de E dans F et une injection de F dans E alors il existe une bijection de E vers F

Rappelons maintenant quelques propriétés sur le caractère fini ou infini des ensembles, la notion de "grosseur" et le lien avec les applications, injections and co. La notion de "grosseur" d'un ensemble n'est pas évidente *a priori* car la relation d'inclusion est une relation d'ordre partiel : il est en général faux qu'étant donnés deux ensembles, l'un soit inclus dans l'autre.

La bonne manière de comparer les grosseurs de deux ensembles et de regarder lequel "s'injecte" dans l'autre. Dans le cas fini, les propriétés qui suivent montrent que cela revient à comparer les cardinaux, ce qui rejoint l'intuition.

Ensembles finis. Cardinal

1. un ensemble est *fini* s'il est en bijection avec $\{1, \ldots, n\}$ pour un certain n entier naturel, qui est alors appelé son cardinal.
2. si E et F sont finis, $\#E \leq \#F$, alors il existe une injection de E dans F (et donc une surjection de F dans E) : E est "moins gros" que F.
3. deux ensembles finis sont en bijection si et seulement s'ils ont le même cardinal : ils sont "de même grosseur"

Dans le cas infini, la bonne façon de comparer les grosseurs est toujours par construction d'une injection de l'un dans l'autre. En revanche, il y a des implications un peu contre intuitives

Ensembles infinis

1. un ensemble infini est *dénombrable* s'il est en bijection avec $\mathbb{N}$
2. s'il existe une injection de E dans $\mathbb{N}$, alors E est fini ou dénombrable
3. si E est infini, alors il existe toujours une injection de $\mathbb{N}$ dans E. En termes vulgarisés, le dénombrable est le plus "petit" infini.
4. si E est dénombrable et F est (infini) non dénombrable, alors il existe une injection de E dans F
5. deux ensembles dénombrables sont toujours en bijection entre eux, même lorsque l'un est une partie stricte de l'autre.

Exemples :

— l'ensemble $2\mathbb{N}$ des nombres pairs est dénombrable, donc en bijection avec $\mathbb{N}$ alors qu'il est strictement inclus.

— $\mathbb{Z}$ et $\mathbb{Q}$ sont dénombrables

— $\mathbb{R}$ n'est pas dénombrable

1.3 Assertions, prédicats and co.

1.3.1 Les basiques

Définitions

1. une *assertion* est un énoncé de la forme la plus basique, i.e. ne contenant pas de variable ni de symbole, et qui est vrai ou faux. Par exemple

"5 est un entier naturel impair" (vrai)
"9 est un nombre premier" (faux)

2. un *prédicat* est un énoncé faisant intervenir une variable. Il peut donc être soit vrai soit faux en fonction de la valeur assignée à la variable.
3. les quantificateurs "quel que soit" et "il existe" sont notés $\forall$ et $\exists$
4. les connecteurs logiques "et", "ou" et "non" sont notés $\wedge, \vee$ et $\neg$;
5. le connecteur logique "ou exclusif" est noté $\oplus$ ou $\veebar$

1.3.2 Implications

On s'attarde maintenant un peu sur les connecteurs "implique" et "est équivalent à"

Définitions

1. $P \Rightarrow Q$ a la même vérité que $\neg P \vee Q$. Autrement dit, $P \Rightarrow Q$ est vrai dès que :
   — P est faux, que Q soit vrai ou faux
   — ou Q est vrai, que P soit vrai ou faux
2. $P \Longleftrightarrow Q$ est vrai lorsque P et Q sont toutes deux vraies ou toutes deux fausses

Ces propriétés méritent une mention spéciale. D'une part, la validité de l'implication ou de l'équivalence entre P et Q ne dit rien de systématique sur la validité de P et Q elles-mêmes, et d'autre part, conduisent à des affirmations un peu étonnantes lorsque ramenées à des contextes courants avec des formulations textuelles. Par exemple les implications

" tous les entiers impairs sont premiers $\Rightarrow$ 5 est premier"
" tous les entiers impairs sont premiers $\Rightarrow$ 9 est premier"
" $1 + 1 = 1 \Rightarrow$ je suis le pape"

sont exactes, bien que chacune des propositions de gauche et de droite soit parfois notoirement fausse, et/ou que la phrase résultante soit un peu fantaisiste.

1.3.3 Négation d'une proposition

Si la négation des propositions simples, c'est-à-dire ne comportant que peu de termes et peu de variables, ne pose pas de difficulté ni de piège, la situation se complique lorsque la proposition devient plus élaborée. La présence de quantificateurs, en particulier s'il y en a plusieurs en cascade, induit parfois des confusions et amène à des affirmations erronées.

Règle Négation d'une proposition

Pour écrire la négation d'une proposition, il faut :
— modifier les quantificateurs $\forall$ en $\exists$ et *vice versa*,
— puis nier la dernière partie de la proposition.

Exemple 1

Considérons un ensemble de lycées dont on étudie les propriétés de mixité des classes, et la proposition

P : "Dans tous les lycées, il existe une classe dans laquelle il n'y a que des filles"

Quelle est l'exacte négation de cette proposition ? Pour la formuler, nous réécrivons P avec des symboles mathématiques

P : "$\forall L$ lycée , $\exists C$ classe $\in L$, $\forall x \in C$, x est une fille"

La négation donne, selon la règle,

$\neg P$: "$\exists L$ lycée , $\forall C$ classe $\in L$, $\exists x \in C$, x n'est pas une fille"

ou encore, en langage naturel

$\neg P$: "Il y a (au moins) un lycée dans lequel toutes les classes contiennent (au moins) un garçon".

Exemple 2
Une fonction f est continue en un point x_0 si, par définition

$$\forall \varepsilon \in \mathbb{R}_+^*,\ \exists \delta \in \mathbb{R}_+^*,\ \forall x \in]x_0-\delta, x_0+\delta[,\ |f(x)-f(x_0)| < \varepsilon$$

Ainsi, f n'est pas continue en x_0 si

$$\exists \varepsilon \in \mathbb{R}_+^*,\ \forall \delta \in \mathbb{R}_+^*,\ \exists x \in]x_0-\delta, x_0+\delta[,\ |f(x)-f(x_0)| \geq \varepsilon$$

1.4 Techniques de démonstration

1.4.1 Par déduction directe

C'est la manière la plus courante d'écrire une preuve en mathématique. On passe des hypothèses à la conclusion par un certain nombre d'étapes, de sorte que chacune des étapes s'appuie soit sur un axiome, soit sur un résultat découlant de manière naturelle des axiomes ou suffisamment classique, soit sur un résultat démontré plus avant dans la théorie sous forme d'un lemme ou d'un théorème, soit enfin sur une étape précédente du raisonnement lui-même.
Outre qu'il faut parfois être astucieux, persévérant voire inventif pour trouver une preuve valide, l'un des pièges majeurs dans lequel on ne doit pas tomber est le *cercle vicieux*, ou la *pétition de principe*. Cette erreur parfois très subtilement cachée consiste à utiliser (inconsciemment et en toute bonne foi) une propriété soit-disant déjà connue mais qui est en réalité une conséquence du résultat que l'on cherche à démontrer.

1.4.2 Par contraposée

Le raisonnement par *contraposée* est un outil qui vise à démontrer un résultat de type implication. La contraposée s'appuie sur le fait la véracité de $P \Rightarrow Q$ est la même que celle de $\neg Q \Rightarrow \neg P$. L'intérêt de la méthode est que l'implication $\neg Q \Rightarrow \neg P$ est parfois plus naturelle à énoncer et à appréhender.

Exemple
Considérons l'implication

Si n est impair alors n n'est pas multiple de 10

Elle est vraie (ce n'est pas très dur à prouver) mais sa formulation contraposée

Si n est multiple de 10 alors n est pair

est plus naturelle à énoncer et parait encore plus "évidente" à démontrer.

Attention Ne pas confondre contraposée et réciproque
La *réciproque* de l'implication $P \Rightarrow Q$ est l'implication $Q \Rightarrow P$. La réciproque d'une implication valide n'a aucune raison d'être elle-même valide.

1.4.3 Par l'absurde

Le raisonnement *par l'absurde* consiste à démontrer une propriété en exhibant que la négation de cette dernière amène à une *contradiction*, c'est-à-dire une impossibilité ou une incompatibilité flagrante avec les d'un des axiomes, l'un des résultats déjà connus de la théorie ou encore l'une des déductions intermédiaires du raisonnement.

Dans le cas où la propriété à démontrer est une implication $P \Rightarrow Q$, le raisonnement par l'absurde est une variante du raisonnement par contraposée : plutôt que de montrer $\neg Q \Rightarrow \neg P$, on montre que $P \wedge \neg Q \Rightarrow$ contradiction

Deux exemples célèbres de démonstrations par l'absurde :
- la suite des nombres premiers est infinie
- le nombre réel $\sqrt{2}$ est irrationnel

1.4.4 Par récurrence

La méthode de *démonstration par récurrence* vise à prouver des propriétés portant sur les entiers naturels.

La version de base

La preuve est en deux temps :

— *Initialisation* : on vérifie que $P(0)$ est vraie

— *Hérédité* : on vérifie que pour tout $n \geq 0$, $P(n) \Rightarrow P(n+1)$

Exemple
Soit à démontrer la propriété

$$P(n) \ : \forall n \in \mathbb{N},\ 0 + \cdots + n = \frac{n(n+1)}{2}$$

— Initialisation : $P(0)$ car il est vrai que $0 = \dfrac{0(0+1)}{2}$

— Hérédité : on fixe $n \geq 0$, on suppose que $P(n)$ est vraie (c'est ce que l'on appelle l'*hypothèse de récurrence*), et on montre qu'alors P(n+1) est vraie aussi. En effet

$$\begin{aligned} 0 + \cdots + (n+1) &= (0 + \ldots n) + (n+1) \\ &= \frac{n(n+1)}{2} + (n+1) && \text{par hypothèse de récurrence} \\ &= (n+1)\left(\frac{n}{2} + 1\right) && \text{factorisation immédiate} \\ &= (n+1)\frac{(n+2)}{2} \\ &= \frac{[n+1]([n+1]+1)}{2} \end{aligned}$$

ce qui prouve $P(n+1)$ est vraie.

Les subtilités

L'initialisation
L'oublier peut avoir de lourdes conséquences, car l'hérédité peut être parfaitement valide et la propriété fausse pour certaines (voire toutes les) valeurs de n. Considérons

$$P(n) : \ 2n + 1 \text{ est un entier pair}$$

Fixons $n \in \mathbb{N}$, et supposons que $P(n)$ est vraie. Alors

$$2(n+1) + 1 = 2n + 3 = (2n+1) + 2$$

Par hypothèse de récurrence, $2n+1$ est pair et comme 2 l'est aussi, $2(n+1)+1$ qui est leur somme est encore pair, ce qui prouve que $P(n+1)$ est vraie. L'hérédité est donc démontrée. Mais aucune initialisation n'est possible, car il est évident que la propriété n'est vraie pour aucune valeur de n.

Synchronisation de l'initialisation et de l'hérédité
L'hérédité doit être assurée au moins à partir du rang de l'initialisation et alors la validité de la proposition est vraie à partir de ce même rang.

1. La combinaison
   — $P(3)$ est vraie
   — $\forall n \geq 3,\ P(n) \Rightarrow P(n+1)$
   assure $\forall n \geq 3,\ P(n)$ est vraie. Mais attention : elle ne dit rien sur $P(0), P(1), P(2)$ qu'il faudra étudier à part.
2. La combinaison
   — $P(3)$ est vraie
   — $\forall n \geq 1,\ P(n) \Rightarrow P(n+1)$

assure encore $\forall n \geq 3,\ P(n)$ est vraie, et non pas $\forall n \geq 1,\ P(n)$ est vraie (il aurait fallu pour ce faire vérifier $P(1)$ vraie).

3. La combinaison
   - $P(0)$ est vraie
   - $\forall n \geq 3,\ P(n) \Rightarrow P(n+1)$

   n'assure rien du tout pour $P(n)$ (sauf pour $n = 0$), car l'hérédité ne s'appuie pas sur le bon point de départ.

Exemple 1

$P(n)\ :\ 2^n > n - 1$.

- Initialisation : $P(0)$ est vraie car $2^0 = 1 > -1 = 0 - 1$
- Fixons $n \in \mathbb{N}$ et supposons $P(n)$ vraie. Alors

$$\begin{array}{rcll} 2^{n+1} & = & 2 \times 2^n & \\ & > & 2 \times (n-1) & \text{hypothèse de récurrence} \\ & = & 2n - 2 & \\ & \geq & n & \\ & = & (n+1) - 1 & \text{pour } n \geq 2 \text{ (et pas pour } n = 0, 1) \end{array}$$

ce qui prouve l'hérédité pour $n \geq 2$. Pour terminer proprement cette récurrence, il faut donc vérifier

- $P(2)$ est vraie pour enclencher l'hérédité. Or $2^2 = 4 > 1 = 2 - 1$ donc OK
- examiner à part (hors hérédité) $P(0), P(1)$, qui en l'occurrence sont vraies aussi (vérification directe)

Exemple 2

$P(n)\ :\ n(n-3) \geq 0$

- $P(0)$ est vraie
- Soit $n \in \mathbb{N}$. Pour $n \geq 3$, on a $n + 1 > n > 0$ et $(n+1) - 3 = n - 2 > n - 3 \geq 0$, de sorte que $(n+1)((n+1)-3) > n(n-3)$, ce dernier étant ≥ 0 par hypothèse de récurrence. Ainsi $P(n+1)$ est vraie.

L'hérédité est donc assurée pour $n \geq 3$. Comme $P(3)$ est vraie, on conclut à ce niveau que $P(n)$ est vraie pour $n = 0$ (vérifié à part), et pour $n \geq 3$ (par récurrence). Mais on ne peut rien conclure pour $P(1)$ et $P(2)$. Un examen séparé montre d'ailleurs qu'elles sont fausses.

Récurrence d'ordre supérieur

Dans certaines situations, la propriété d'hérédité est plus facile à démontrer lorsqu'elle est de la forme "$P(n)$ et $P(n+1) \Rightarrow P(n+2)$". On parle alors de récurrence d'ordre 2, et il faut adapter l'initialisation vérifier non plus simplement $P(0)$, mais $P(0)$ et $P(1)$.
Cette variante se généralise à tout ordre supérieur à 2. Par exemple, pour une récurrence d'ordre 5, on montrera que

- initialisation : $P(0), P(1), P(2), P(3), P(4)$
- hérédité : $\forall n \geq 0,\ P(n)$ et $P(n+1)$ et $P(n+2)$ et $P(n+3)$ et $P(n+4) \Rightarrow P(n+5)$

Dans ces cas plus élaborés de récurrence, il faut alors redoubler de vigilance sur la synchronisation entre l'initialisation et l'hérédité.

Récurrence forte

C'est une forme plus puissante du raisonnement : dans l'étape d'hérédité, l'hypothèse de récurrence nécessaire à démontrer $P(n+1)$ est que TOUS les prédécesseurs $P(0), P(1), \ldots, P(n)$ sont vrais. Le raisonnement est alors :

- initialisation : $P(0)$ est vraie
- hérédité : $P(0), \ldots, P(n) \Rightarrow P(n+1)$

1.4.5 La descente infinie de Fermat

La descente infinie est une méthode mélangeant subtilement le raisonnement par récurrence et le raisonnement par l'absurde. Elle utilise la propriété que toute suite strictement décroissante d'entiers naturels est nécessairement finie.

On suppose fausse la propriété que l'on veut démontrer, et on montre que cela permet de construire par itérations successives une suite infinie strictement décroissante d'entiers naturels.

Exemple Irrationalité de $\sqrt{2}$
On suppose par l'absurde qu'il existe deux entiers p, q tels que $\sqrt{2} = p/q$. Alors $p^2 = 2q^2$. Ainsi p^2 est pair, ce qui implique que p est pair. On peut écrire $p = 2p_1$ pour un certain entier p_1. En remplaçant dans l'équation de départ, il vient $4p_1^2 = 2q^2$, donc $q^2 = 2p_1^2$. Ainsi q est pair et $q = 2q_1$. En remplaçant il vient maintenant $4q_1^2 = 2p_1^2$, soit $p_1^2 = 2q_1^2$ et finalement $\sqrt{2} = p_1/q_1$. En synthèse à partir de p et q vérifiant $\sqrt{2} = p/q$, on a construit p_1, q_1 vérifiant $\sqrt{2} = p_1/q_1$ avec

$$p_1 = p/2 < p, \quad q_1 = q/2 < q$$

En itérant le processus, on peut construire une suite infinie décroissante d'entiers naturels

$$p > p_1 = p/2 > p_2 = p_1/2 > \dots$$

(en fait, dans le cas de cet exemple, on en a même une deuxième $q > q_1 = q/2 > q_2 = q_1/2 > \dots$). La contradiction apportée par le raisonnement entraine que l'hypothèse initiale est fausse : il n'existe pas deux entiers p, q tels que $\sqrt{2} = p/q$, ce que nous voulions démontrer.

Chapitre 2

Relations binaires

2.1 Introduction

Une *relation* entre objets mathématiques d'un certain domaine est une propriété qu'ont, ou non, entre eux certains de ces objets. Lorsque la propriété porte sur deux objets, la relation est dite *binaire*. Des exemples classiques sont données par la relation d'ordre strict "$<$" dans l'ensemble des nombres réels, le parallélisme ou l'orthogonalité dans l'ensemble des droites du plan.

Définition

Une *relation binaire* $\mathcal{R}$ est définie par la donnée de deux ensembles E et F et d'une partie $\mathcal{G}$ de $E \times F$. On dit que que $x \in E$ est en relation avec $y \in F$, et on écrit $x\mathcal{R}y$ si et seulement si $(x, y) \in \mathcal{G}$.

Contrairement à ce que les exemples courants suggèrent, il n'est pas exigé en toute généralité que $E = F$, ni que l'on puisse facilement renverser les rôles de E et de F. C'est précisément la raison pour laquelle la définition est formulée sur le produit cartésien $E \times F$, car celui-ci est composé de couples qui, par essence, sont ordonnés.

Par ailleurs, un élément de E peut être en relation avec un nombre quelconque d'éléments de F (éventuellement aucun) et vice versa.

La *relation réciproque* $\mathcal{R}^{-1}$ est définie par

$$\forall x \in E,\ \forall y \in F,\ y\mathcal{R}^{-1}x \Leftrightarrow x\mathcal{R}y$$

Exemple

E est un ensemble de personnes {Alice, Bob, Charlie, Didier} et F un ensemble de couleurs {rouge, jaune, vert, bleu, violet}. On définit la relation "aime" $x\mathcal{R}y$ si l'individu x aime la couleur y. Dans notre cas on suppose que :

- Alice aime le rouge et le bleu
- Bob aime le jaune
- Charlie aime le jaune, le vert et le bleu
- Didier n'aime rien du tout

On peut traduire en l'ensemble exhaustif des couples caractérisant la relation :

{(Alice, rouge), (Alice, bleu), (Bob, jaune), (Charlie, jaune), (Charlie, vert), (Charlie, bleu)}

On vérifie en particulier

- une personne peut aimer aucune, une ou plusieurs couleurs
- une même couleur peut être aimée d'aucune, une ou plusieurs personnes

La relation réciproque $\mathcal{R}^{-1}$ est "être aimée par". La liste des couples qui la caractérise est

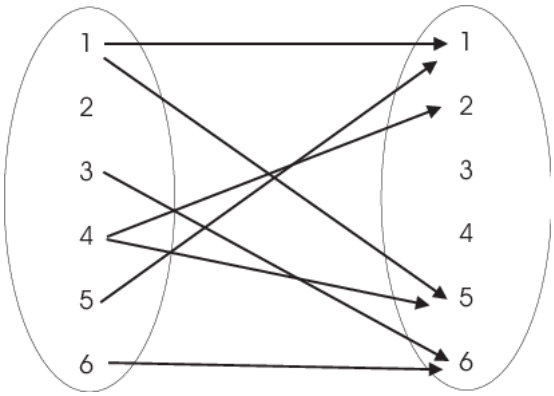
{rouge, Alice), (bleu, Alice), (jaune, Bob), etc.}

2.2 Diagramme sagittal. Représentation matricielle

Il existe deux manières classiques de représenter une relation : un diagramme sagittal et une matrice.

2.2.1 Diagramme sagittal

On dessine les deux ensembles E et F avec leurs éléments, et on trace une flèche (ou arc orienté) de $x \in E$ vers $y \in F$ si et seulement si $x\mathcal{R}y$.



Exemple de diagramme sagittal
La relation est définie en extension par :
$1\mathcal{R}1$, $1\mathcal{R}5$, $3\mathcal{R}6$, $4\mathcal{R}2$, $4\mathcal{R}5$, $5\mathcal{R}1$, $6\mathcal{R}6$

Remarques

1. Le diagramme sagittal de la relation réciproque s'obtient en re-dessinant le schéma de droite à gauche et en inversant l'orientation de chaque arc.
2. Dans le cas où $E = F$, on peut ne dessiner qu'une seule fois E, et les arêtes entre ses éléments. On obtient un graphe au sens plus commun du terme. Le digramme sagittal proposé en exemple n' pas fait ce choix de représentation.

2.2.2 Matrice d'adjacence

Il s'agit d'un tableau à deux dimensions où :

— les lignes correspondent aux éléments de E

— les colonnes correspondent aux éléments de F

— une croix apparait dans le tableau à la ligne x et colonne y lorsque $x\mathcal{R}y$.

Pour notre exemple, la matrice d'adjacence s'écrit

	rouge	jaune	vert	bleu	violet
Alice	x			x	
Bob		x			
Charlie		x	x	x	
Didier					

Dans le cas où $E = F$, la matrice est carrée. Les lignes et les colonnes sont en nombre identiques et sont indexées par les mêmes éléments. Les entrées de la matrice d'adjacence sont parfois pris comme des "0" et "1" en lieu et place de "vides" et "croix", ce qui permet d'avoir recours au calcul matriciel, utile dans certains contextes.

2.3 Réflexivité. Symétrie. Transitivité

Une relation binaire $\mathcal{R}$ définie sur un ensemble E a parfois des propriétés particulières qui jouent un rôle important dans de nombreux contextes. Nous en donnons les définitions ici.

Définitions

On dit que $\mathcal{R}$ est

- réflexive si $\forall x \in E,\ x\mathcal{R}x$
- antiréflexive si $\forall x \in E,\ \neg(x\mathcal{R}x)$.
- symétrique si $\forall x, y \in E,\ x\mathcal{R}y \Rightarrow y\mathcal{R}x$
- antisymétrique si $\forall x, y \in E,\ (\ (x\mathcal{R}y) \wedge (y\mathcal{R}x)\ ) \Rightarrow x = y$
- asymétrique si $\forall x, y \in E,\ (\ (x\mathcal{R}y) \wedge (y\mathcal{R}x)\ )$ est impossible
- transitive si $\forall x, y, z \in E,\ (\ (x\mathcal{R}y) \wedge (y\mathcal{R}z)\ ) \Rightarrow (x\mathcal{R}z)$
- antitransitive si $\forall x, y, z \in E,\ (\ (x\mathcal{R}y) \wedge (y\mathcal{R}z)\ ) \Rightarrow \neg(x\mathcal{R}z)$
- totale si $\forall x, y \in E,\ (x\mathcal{R}y) \vee (y\mathcal{R}x)$

Attention :

- “antiréflexive” n’est pas synonyme de “non réflexive”
- “antisymétrique” n’est pas synonyme de “non symétrique”
- “asymétrique” n’est pas synonyme de “non symétrique”
- “antitransitive” n’est pas synonyme de “non transitive”

2.4 Relations d’équivalence

Définition

Une relation est dite *relation d’équivalence* si elle est réflexive, symétrique et transitive.

Exemples

- Trivialement, la relation “=” sur n’importe quel ensemble
- La relation “est dans la même équipe que” sur l’ensemble des pratiquants d’un sport d’équipe
- La relation “avoir le même chiffre des unités que” sur l’ensemble des entiers.

En revanche, la relation “a un chiffre commun avec” sur l’ensemble des nombres entiers n’est pas une relation d’équivalence car elle n’est pas transitive : on a $12\mathcal{R}23$ et $23\mathcal{R}34$ et pourtant $\neg(12\mathcal{R}34)$.

2.4.1 Classes d’équivalence. Partition

On fixe x un élément de E. L’ensemble des y tels que $x\mathcal{R}y$ s’appelle la classe d’équivalence de x, notée $\mathrm{Cl}(x)$.

Propriétés

- il existe toujours au moins une classe d’équivalence
- deux classes d’équivalence sont égales ou disjointes
- dans une classe la relation est complète : tous les éléments d’une même classe sont en relation entre eux ;le graphe restreint à cette classe contient toutes les arêtes possibles
- en conséquence, l’ensemble des classes d’équivalences de $\mathcal{R}$ forment une *partition* de E, c’est-à-dire un recouvrement de E par des parties non vides 2 à 2 disjointes
- tout élément d’une classe d’équivalence donnée s’appelle un *représentant* de la classe

Dans l’exemple de la relation “=”, les classes d’équivalence sont les singletons. Dans l’exemple des sportifs, les classes d’équivalences sont les équipes. Dans l’exemple des entiers ayant le même chiffre des unités, les classes d’équivalences sont l’ensemble des entiers se terminant par 0, ceux se terminant par 1, ..., ceux se terminant par 9.

Une fois les classes d’équivalence formées, l’ensemble E peut être décrit de façon abrégée par la définition de la relation d’équivalence d’une part et d’autre part par le choix d’un représentant par classe : on parle

de *système complet de représentants*. En général, il y a plusieurs systèmes complets de représentants.

Nous venons de voir comment une relation d'équivalence induit une partition de E. Nous disposons du résultat réciproque.

Proposition

Pour toute partition de $E = C_1 \sqcup C_2 \sqcup \dots$, la relation $x\mathcal{R}y$ définie par "x et y appartiennent au même C_i" est une relation d'équivalence dont les classes sont précisément les C_i eux-mêmes.

Ainsi, les relations d'équivalence sur un ensemble et les partitions de cet ensemble sont essentiellement les mêmes objets combinatoires.

2.4.2 Congruence modulaire

Soit $\mathbb{Z}$ l'ensemble des entiers relatifs, n un entier naturel non nul. La relation de *congruence modulo* n est définie par

$$x \equiv y \bmod n \iff x - y \text{ est multiple de } n.$$

On montre sans trop de difficultés que $\equiv$ est une relation d'équivalence, et que les classes d'équivalences sont les sous-ensemble des entiers ayant le même reste dans la division euclidienne par n.

Voici par exemple l'ensemble des entiers partitionnés par leur classe de congruence modulo 10. Dans le cas d'un entier positif, la classe de congruence est celle de son chiffre des unités.

Classe	Reste de la division par 10
$\{\dots, -20, -10, 0, 10, 20, \dots\}$	0
$\{\dots, -19, -9, 1, 11, 21, \dots\}$	1
$\{\dots, -18, -8, 2, 12, 22, \dots\}$	2
$\{\dots, -17, -7, 3, 13, 23, \dots\}$	3
$\{\dots, -16, -6, 4, 14, 24, \dots\}$	4
$\{\dots, -15, -5, 5, 15, 25, \dots\}$	5
$\{\dots, -14, -4, 6, 16, 26, \dots\}$	6
$\{\dots, -13, -3, 7, 17, 27, \dots\}$	7
$\{\dots, -12, -2, 8, 18, 28, \dots\}$	8
$\{\dots, -11, -1, 9, 19, 29, \dots\}$	9

À noter que $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ et $\{1000, 241, 52, 333, 7854, 965, 20486, 357, 468128, 89\}$ sont deux systèmes complets de représentants, mais le premier parait plus naturel.

2.5 Relation d'ordre

Définition

Une relation est dite *relation d'ordre* si elle est réflexive, antisymétrique, transitive.

L'exemple stéréotypique est la relation $\leq$ sur l'ensemble des entiers, des rationnels ou des réels.
Attention : la relation $<$ n'est pas une relation d'ordre. Elle est transitive mais elle n'est ni réflexive ni antisymétrique : elle est même antiréflexive et asymétrique.

2.5.1 Ordre total ou partiel

Lorsque la relation d'ordre est totale, c'est-à-dire que deux éléments quelconques peuvent toujours être mis en relation, on parle naturellement d'*ordre total*. Dans le cas contraire, on parle d'*ordre partiel*. Par exemple,

— l'inclusion définie sur les parties d'un ensemble

— la divisibilité définie sur les entiers

sont des relations d'ordre partiel.

Voici maintenant quelques notions spécifiques aux relations d'ordre. On désigne de manière générique la relation d'ordre "est plus petit que" en gardant à l'esprit que cela peut un ordre partiel.

Théorème-Définitions

1. un *majorant* de E est un élément plus grand que tous les éléments de E.
   - il n'existe pas forcément
   - s'il existe, il n'est pas forcément dans E (ce qui sous-entend que E est alors inclus dans un ensemble plus vaste)
   - s'il existe il n'est pas forcément unique
2. la *borne supérieure*, ou *supremum* de E est le plus petit des majorants
   - il n'existe pas forcément même s'il existe un/des majorant(s)
   - s'il existe, il n'est pas forcément dans E
   - s'il existe, il est unique
3. le *maximum* de E est le plus grand élément de E
   - il n'existe pas forcément, même s'il existe un supremum ou un/des majorant(s)
   - s'il existe, il est dans E par définition
   - s'il existe, il est unique et il est aussi le supremum
4. un *élément maximal* de E est un élément qui n'est plus petit qu'aucun autre élément de E
   - il n'existe pas forcément
   - s'il existe, il est forcément dans E par définition
   - si E admet un maximum, celui-ci est l'unique élément maximal
   - si l'ordre est total, la notion d'élément maximal coïncide avec celle de maximum.
   - si l'ordre est partiel, un éventuel élément maximal n'est pas forcément le maximum de E et il n'est pas forcément unique.

On définit de manière analogue le notions de *minorant*, *borne inférieure* (ou *infimum*), *minimum*, *élément minimal*

Exemples

1. Dans $\mathbb{R}$ muni de l'ordre total $\leq$, la partie $[0,1[$
   - admet des majorants : 1, 2, 3, ...(en fait tout réel ≥ 1)
   - admet une borne supérieure : 1
   - n'admet pas de maximum (et donc pas d'élément maximal)
   - admet un minimum : 0 (qui est le seul élément minimal)
   - admet des minorants : tout réel ≤ 0
2. dans $\mathbb{Q}$ muni de l'ordre total $\leq$, et la partie $\{x \in \mathbb{Q}, 0 \leq x^2 \leq 2\}$
   - admet des majorants : tout rationnel m tel que $m^2 > 2$
   - n'admet pas de borne supérieure : on peut démontrer que pour tout m majorant, il existe un autre majorant $m' < m$. (NB : dans $\mathbb{R}$, il y a une borne supérieure qui est $\sqrt{2}$)
   - n'admet pas de maximum (et donc pas d'élément maximal)
   - admet un minimum : 0 (qui est le seul élément minimal)
   - admet des minorants : tout rationnel ≤ 0
3. dans $\mathbb{N}$ muni de l'ordre partiel "est un diviseur de", la partie $\{1, 2, 3, \ldots, 10\}$
   - admet des majorants : par exemple $10! = 3628800$
   - admet une borne supérieure : $\text{PPCM}(1, 2, 3, \ldots, 10) = 2520$
   - n'admet pas de maximum
   - admet des élément maximaux : 10,9,8,7,6

— admet un minimum : 1, qui est aussi l'unique minorant, la borne inférieure et l'unique élément minimal.

4. On enlève "1" de l'ensemble de l'exemple précédent, soit la partie $\{2, 3, \ldots, 10\}$,
   — les majorants, borne supérieure et éléments maximaux sont les mêmes que ci-dessus, et comme ci-dessus il n'y a pas de maximum
   — il y a un minorant, qui est aussi la borne inférieure : 1
   — il n'y a pas n'admet pas de minimum
   — il y a des éléments minimaux : 2, 3, 5, 7

   On observe au passage que 7 est à la fois un élément minimal et maximal. Cela peut paraitre un peu déroutant, mais cela signifie (et c'est moins déroutant ainsi) que, d'un coté, 7 n'est ni multiple ni diviseur d'un entier entre 2 et 10 (autre que lui-même bien sûr)

2.5.2 Diagramme de Hasse d'une relation d'ordre

Soit $\mathcal{G}$ le graphe d'une relation d'ordre $\prec$ définie sur E. On rappelle que :

— les sommets de $\mathcal{G}$ représentent les éléments de E

— les arêtes orientées de $\mathcal{G}$ relient x à y si $x \prec y$

Supposons E fini. On simplifie le graphe $\mathcal{G}$ afin de ne garder que les informations indispensables :

— on omet de dessiner les boucles de chaque sommet sur lui-même, puisque l'on sait que $\prec$ est réflexive

— on omet de dessiner les arêtes qui peuvent se déduire de celles déjà dessinées par transitivité. En d'autres termes, on ne conserve que les arêtes "primitives", c'est-à-dire les liens $x \prec y$ pour lesquels il n'existe aucun t tel que $x \prec t \ \wedge \ t \prec y$.

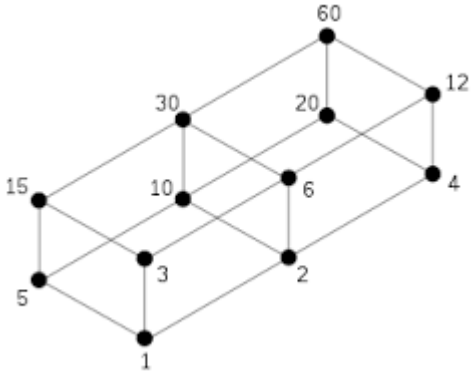
— on dessine par convention les arêtes dans le sens "montant", ce qui permet d'omettre la pointe de la flèche

Remarque

1. Dans un tel diagramme, les points "racines" - qui n'ont pas d'arête descendante - correspondent aux éléments minimaux de E. De manière analogue, les points "sommitaux" - qui n'ont pas d'arête montante - correspondent aux éléments maximaux de E.
2. Cette représentation permet à un observateur "humain" de visualiser la situation de manière synthétique.
3. Elle n'est pertinente que pour les relations d'ordre partiel. En effet, dans le cas d'un ordre total, le diagramme est simplement une colonne montante des éléments de E avec le plus petit en bas et le plus grand en haut

Exemple

L'ensemble $E = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$ des diviseurs de 60 est partiellement ordonné par la relation de divisibilité. Voici son diagramme de Hasse.



Source :Wikipedia

Chapitre 3

Arithmétique des entiers

3.1 Introduction

Contrairement à une idée reçue du grand public, l'arithmétique des entiers n'est pas le bac à sable du calcul numérique, enseigné en primaire ou au collège en attendant que les élèves apprennent les nombres rationnels, réels puis complexes. Si les mathématiques de l'ingénieur font la part belle à ces derniers, l'arithmétique des entiers présentent l'énorme avantage de proposer des calculs parfaitement exacts, sans aucun recours à la notion de précision. Cette exactitude native fait de cette branche, appelée aussi *mathématiques discrètes*, le terreau privilégié pour la modélisation et l'ingénierie de l'information numérique, c'est-à-dire l'information telle qu'elle est représentée aujourd'hui dans nos ordinateurs (essentiellement par des suites de "0 et des "1").

La théorie des codes correcteurs d'erreurs et la cryptologie sont deux applications emblématiques des mathématiques discrètes.

3.1.1 Présentation générale des anneaux

Le lecteur est probablement familier des nombres entiers depuis de nombreuses années, mais peut-être pas d'un vocabulaire un peu spécifique, inutile pour une compréhension courante mais qui est indispensable dans le cadre de ce chapitre et des objectifs qu'il poursuit.
Un *anneau commutatif* $(A, +, \times)$ est un ensemble muni de deux lois de compositions internes, possédant les propriétés suivantes :

- elles sont commutatives, associatives
- chacune a un élément neutre, noté "0" pour + et "1" pour $\times$
- tout élément x a un opposé noté $-x$
- "$\times$" est distributive par rapport à "+"

Vulgairement parlant, un anneau est un objet dans lequel on peut faire des $+, -, \times$. Bref un objet tel que l'ensemble des entiers relatifs $\mathbb{Z}$. D'ailleurs, les opérations sont très souvent appelées l'addition et la multiplication, avec les diverses notations raccourcies de cette dernière : $x \times y = x \cdot y = xy$. Pour la division, par contre, il n'est rien requis de particulier. On dit qu'un élément (non nul) est *inversible* s'il existe un élément, alors unique et noté x^{-1} (plus rarement $1/x$), tel que $x \cdot x^{-1} = 1$. On notera que dans $\mathbb{Z}$, seuls 1 et -1 sont inversibles (il se trouve qu'ils sont d'ailleurs égaux à leur propre inverse, mais ce n'est pas une propriété générale dans un anneau). Les autres entiers ne sont pas inversibles car leurs inverses sont rationnels non entiers.

Un anneau contient parfois des *diviseurs de zéro* : deux éléments (éventuellement égaux) z_1 et z_2 non nuls et tel que $z_1 z_2 = 0$. Cette situation est certainement la plus déroutante des définitions que nous rencontrerons, car elle va nous obliger à tordre le coup à une saine vérité à laquelle nous avons adhéré pendant des années :

> un produit de facteurs est nul si et seulement si l'un des facteurs est nul

Un anneau ne contenant pas de diviseurs de zéro (comme $\mathbb{Z}$) est dit *intègre*.

3.1.2 Idéal d'un anneau

De même qu'en algèbre linéaire, la notion de sous-espace vectoriel joue un rôle privilégié dans la théorie, pour les anneaux, il y a une sous-structure privilégiée : celle d'idéal.

Définition

Un idéal I dans un anneau A est une partie vérifiant les propriétés suivantes :

1. Pour tous $x, y \in I$, $x + y$ et $-x$ sont dans I
2. Pour tout $x \in I$ et tout $y \in A$, $xy \in I$

Schématiquement, un idéal est une partie

— stable par $+/-$ (en particulier qui contient "0"),

— absorbante - ce qui est plus fort que d'être stable - pour la multiplication.

— Elle ne contient pas "1", à moins d'être égale à l'anneau tout entier.

Dans $\mathbb{Z}$, on vérifie sans peine que toute partie de la forme $n\mathbb{Z}$, c'est-à-dire l'ensemble des multiples d'un certain entier n, est un idéal. En effet,

— la somme et la différence de deux multiples de n est bien un multiple de n,

— le produit de deux entiers est un multiple de n dès que l'un des deux est multiple de n

L'entier n est le *générateur* de l'idéal $n\mathbb{Z}$. En particulier, le cas

— $n = 0$ correspond à l'idéal réduit à $\{0\}$,

— $n = 1$ correspond à $\mathbb{Z}$ tout entier.

La propriété suivante énonce la réciproque :

Théorème-Définition

Les idéaux de $\mathbb{Z}$ sont **exactement** les $n\mathbb{Z}$. On dit que $\mathbb{Z}$ est un *anneau principal*

Remarque

Soit $I = n\mathbb{Z}$ un idéal. Pour qu'un produit xy soit dans I, il suffit que x ou y soit dans I (par définition-même d'un idéal). Réciproquement, on peut de demander si, lorsqu'un produit $xy \in I$, cela implique que $x \in I$ ou $y \in I$. C'est manifestement faux dans le cas général : par exemple, le produit xy est multiple de 10 sans que x ou y ne soient eux-mêmes multiples de 10. inversement si un produit xy est multiple de 7, assurément l'un au moins des deux nombres x ou y est multiple de 7. Si la réponse est oui, on dit que I est un *idéal premier*. Pour les idéaux de $\mathbb{Z}$, la proposition suivante donne l'état des lieux

Proposition

1. Si n non premier, on peut toujours trouver $x \notin n\mathbb{Z}$ et $y \notin n\mathbb{Z}$ tels que $xy \in n\mathbb{Z}$
2. Si p est premier, alors $xy \in p\mathbb{Z}$ implique que $x \in p\mathbb{Z}$ ou $y \in p\mathbb{Z}$. On dit $p\mathbb{Z}$ est un *idéal premier* de $\mathbb{Z}$

3.2 Divisibilité. Nombres premiers. PGCD, PPCM

3.2.1 Division euclidienne

Théorème

Pour tous entiers $a \in \mathbb{Z}$ (dividende) et $b \in \mathbb{N}$ (diviseur), il existe un unique couple (q, r) (quotient, reste) tels que :

— $a = bq + r$

— $0 \leq r \leq b - 1$

On trouve parfois l'écriture $a \div b = (q, r)$ ou encore $a \div b = q$ reste r. Quelle que soit la notation adoptée, le fondamental à se rappeler est que le résultat d'une division euclidienne comporte **deux** entiers.

Remarque

Si cette division est classique depuis le primaire lorsque a est positif, il faut faire un tout petit peu

attention lorsque a est négatif, et ne pas se contenter de mettre un signe "$-$" devant la division : sinon le reste r n'a plus la propriété d'être compris entre 0 et $b-1$, et cette propriété est cruciale pour l'unicité. On écrira par exemple :

— pour $32 \div 5 : 32 = 5 \times 6 + 2$

— Pour $(-32) \div 5 : -32 = 5 \times (-7) + 3$

même si dans le second cas, il est indiscutable que $-32 = 5 \times (-6) - 2$.

On dit que "a est *divisible* par b", ou que "a est un *multiple* de b" ou encore que "b divise a" si le reste de la division euclidienne de a par b est nul. Cette définition suppose implicitement que l'on travaille avec b positif, mais si b est négatif il suffit de changer b en $-b$ et la propriété de divisibilité n'est pas fondamentalement modifiée.

Un nombre entier naturel est *premier* s'il n'est divisible que par 1 et lui-même. Signalons que par convention, un nombre entier négatif qui est l'opposé d'un nombre premier est aussi premier, bien que cette convention soit en réalité totalement inusitée.

3.2.2 Théorème fondamental de l'arithmétique

Théorème Décomposition en produits de facteurs premiers (DPFP)

1. Tout nombre entier naturel n positif s'écrit
$$n = p_1^{e_1} p_2^{e_2} \dots p_s^{e_s}$$
où $p_1, p_2, \dots p_s$ sont des nombres premiers et les exposants $e_1, e_2, \dots, e_s$ des entiers > 0. Cette décomposition est unique à l'ordre près des facteurs.
2. La même propriété est vraie pour tout entier relatif à condition d'écrire la décomposition
$$n = \pm p_1^{e_1} p_2^{e_2} \dots p_s^{e_s}$$
On dit que $\mathbb{Z}$ est un *anneau factoriel*

Obtention de la décomposition

Il faut disposer d'une liste de nombres premiers $\{2, 3, 5, 7, \dots\}$. On divise si c'est possible le nombre n par 2, puis on recommence jusqu'à ce que le quotient ne soit plus divisible par 2. Le nombre de divisions que l'on a faites donnera l'exposant de 2 dans la décomposition. Puis on recommence avec 3, et ainsi de suite jusqu'à ce que le quotient soit égal à 1.

Exemple . Soit 6866640 le nombre que l'on cherche à décomposer. Les étapes sont

Valeur courante	Nombre premier	Quotient	Nombre de divisions
6866640	2	3433320	1
3433320	2	1716660	2
1716660	2	858330	3
858330	2	429165	4
429165	3	143055	1
143055	3	47685	2
47685	3	15895	3
15895	5	3179	1
3179	11	289	1
289	17	17	1
17	17	1	2

On conclut que $6866640 = 2^4 \cdot 3^3 \cdot 5^1 \cdot 11^1 \cdot 17^2$

3.2.3 PGCD, PPCM

Soient deux entiers m et n non nuls. Regardons l'ensemble $\mathcal{D}$ (resp. $\mathcal{M}$) de leurs diviseurs (resp. multiples) communs. Une habitude commode est de se limiter aux entiers naturels, ce qui n'est pas gênant pour la complétude du propos puisque, comme on l'a déjà vu, la divisibilité est "au signe près".
Il est clair que $\mathcal{D}$ (resp. $\mathcal{M}$) est non vide, puisqu'il contient 1 (resp. mn). Par ailleurs, $\mathcal{D}$ est majoré car tout entier excédant strictement m et n ne peut diviser ni m ni n. On déduit que :

— $\mathcal{D}$ possède un plus grand élément. On l'appelle le PGCD de m et n.

— $\mathcal{M}$ possède un plus petit élément. On l'appelle le PPCM de m et n.

Le cas où l'un des entiers est nul et pas l'autre, bien que la définition s'applique telle quelle, est suffisamment particulier pour justifier une définition simplifiée :

$$\forall m \neq 0,\ \mathrm{PGCD}(m,0) = m,\ \mathrm{PPCM}(m,0) = 0$$

Enfin, il n'est pas d'usage de définir ni d'utiliser $\mathrm{PGCD}(0,0)$ ni $\mathrm{PPCM}(0,0)$.

Calcul du PGCD et du PPCM avec la DPFP

On écrit les DPFP de m et de n

$$\begin{aligned} m &= p_1^{m_{p_1}} p_2^{m_{p_2}} \dots p_s^{m_{p_s}} \\ n &= q_1^{n_{q_1}} q_2^{n_{q_2}} \dots q_t^{n_{q_t}} \end{aligned}$$

Alors :

— la DPFP du PGCD s'obtient en examinant les nombres premiers apparaissant dans m ET dans n : s'il n'y en a pas, le PGCD est égal à 1. S'il y en a, à chacun d'entre eux on affecte pour exposant le minimum des deux exposants.

— la DPFP du PPCM s'obtient en conservant les nombres premiers apparaissant dans m OU dans n, et l'exposant retenu est le maximum des deux (l'un des deux exposants pouvant être nul)

Formellement, on écrit

$$\begin{aligned} \mathrm{PGCD}(m,n) &= \prod_{p \in \{p_1,\dots,p_s\} \cap \{q_1,\dots,q_t\}} p^{\min(m_p, n_p)} \\ \mathrm{PPCM}(m,n) &= \prod_{p \in \{p_1,\dots,p_s\} \cup \{q_1,\dots,q_t\}} p^{\max(m_p, n_p)} \end{aligned}$$

avec la convention qu'un produit indexé par l'ensemble vide est égal à 1.

Remarque
On généralise aisément la notion de PGCD et de PPCM à une toute collection finie d'entiers et on les calcule par la même règle.

Exemple
Soient $m = 128338749$ et $n = 6866640$. Les DFPF donnent

$$\begin{aligned} 128338749 &= 3^5 \cdot 7^1 \cdot 11^1 \cdot 19^3 \\ 6866640 &= 2^4 \cdot 3^3 \cdot 5^1 \cdot 11^1 \cdot 17^2 \end{aligned}$$

de sorte que

$$\begin{aligned} \mathrm{PGCD}(128338749, 6866640) &= 3^3 \cdot 11^1 &&= 297 \\ \mathrm{PPCM}(128338749, 6866640) &= 2^4 \cdot 3^5 \cdot 5^1 \cdot 7^1 \cdot 11^1 \cdot 17^2 \cdot 19^3 &&= 2967191876880 \end{aligned}$$

Définition

Deux entiers m et n sont *premiers entre eux* (ou *étrangers*, ou *copremiers* - de l'anglicisme *coprime*) si $\mathrm{PGCD}(m,n) = 1$.

Attention : m et n premiers entre eux n'implique pas que m et/ou n soient premiers.

Dans le cas de plus de trois entiers, on distingue deux notions :

Les entiers $n_1, \ldots, n_s$ sont
- *premiers entre eux 2 à 2* si $\forall 1 \leq i \neq j \leq s, \quad \text{PGCD}(n_i, n_j) = 1$
- *premiers entre eux dans leur ensemble* si $\text{PGCD}(n_1, \ldots, n_s) = 1$

On a "premiers entre eux 2 à 2" $\Rightarrow$ "premiers entre eux dans leur ensemble", mais la réciproque est fausse. Il se peut même que $n_1, \ldots, n_s$ soient premiers entre eux dans leur ensemble sans qu'aucune paire $\{n_i, n_j\}$ ne soit copremière.

Propriétés liées au PGCD et PPCM.

Soient a, b deux entiers

1. $\text{PGCD}(a,b) \times \text{PPCM}(a,b) = ab$. Il n'y a pas de généralisation pour le cas de plus de 3 entiers.
2. pour tour entier $k \neq 0$, $\text{PGCD}(ka, kb) = k\text{PGCD}(a,b)$ et $\text{PPCM}(ka, kb) = k\text{PPCM}(a,b)$
3. (conséquence), $\text{PGCD}\left(\frac{a}{\text{PGCD}(a,b)}, \frac{b}{\text{PGCD}(a,b)}\right) = 1$
4. si p premier divise ab alors p divise a ou p divise b.
5. si a et b sont premiers entre eux et divisent c, alors ab divise c.
6. si p est premier,
   - ou bien p divise a, ce qui équivaut à $\text{PGCD}(p,a) = p$.
   - ou bien p et a sont premiers entre eux (c'est-à-dire $\text{PGCD}(p,a) = 1$)

Les preuves sont relativement faciles en examinant les DPFP.

3.3 Théorème de Bezout. Algorithme d'Euclide

3.3.1 Nouvelle caractérisation du PGCD

Théorème Bezout (1/2)

Soient a, b deux entiers

1. $\exists u, v \in \mathbb{Z}$ tels que $\text{PGCD}(a,b) = au + bv$. Les coefficients u et v s'appellent les *coefficients de Bezout* de (a,b). Ils ne sont pas uniques (il existe même une infinité de couples (u,v))
2. (Réciproque partielle) Si $d \in \mathbb{Z}$ et $\exists u, v \in \mathbb{Z}$ $d = au + bv$, alors d est multiple de (**et non pas "est égal à"**) $\text{PGCD}(a,b)$.

Dans le cas d'entiers premiers entre eux, le théorème précédent est renforcé car la réciproque est "totale".

Théorème Bezout (2/2)

Deux entiers a et b sont premiers entre eux $\iff$ $\exists u, v \in \mathbb{Z}$ tels que $au + bv = 1$

3.3.2 Algorithme d'Euclide du calcul du PGCD

Cet algorithme alternatif de calcul du PGCD n'utilise pas les DPFP. Il est en pratique plus rapide que la méthode des DPFP, car ces dernières sont coûteuses à obtenir.

Il repose sur un enchainement de divisions euclidiennes. Son intérêt majeur, en dehors de sa rapidité, est de proposer une version étendue, appelée *algorithme d'Euclide étendu* (EEA, pour *Extended Euclid Algorithm*), qui permet de calculer non seulement le PGCD mais également et simultanément un couple de coefficients de Bezout, c'est-à-dire un couple (u,v) tel que $au + bv = \text{PGCD}(a,b)$. C'est cette version que nous présentons ici.

```
---------------------------------------------------------------
Algortihme EEA
---------------------------------------------------------------
Entrées: a > b entiers
```

```
Sorties: d, u, v, avec d = PGCD(a,b) = au+bv

Initialiser des variables
  r[-1]=a  r[0]=b
  u[-1]=1  u[0]=0
  v[-1]=0  v[0]=1

Divisions euclidiennes et mise a jour des variables
  (Tant que le nouveau reste est non nul)
  r[-1] div r[0] -> q[1], r[1] // r[1] = r[-1] - r[0]q[1]
  u[1] = u[-1]-u[0]q[1]
  v[1] = v[-1]-v[0]q[1]

  r[0] div r[1] -> q[2], r[2] // r[2] = r[0]-r[1]q[2]
  u[2] = u[0]-u[1]q[2]
  v[2] = v[0]-v[1]q[2]

  ...

  r[p-2] div r[p-1] -> q[p], r[p] // r[p] = r[p-2]-r[p-1]q[p]
  u[p] = u[p-2]-u[p-1]q[p]
  v[p] = v[p-2]-v[p-1]q[p]

  r[p-1] div r[p] -> q[p+1], r[p+1]=0 //

Terminer: d <- r[p], u <- u[p], v <- v[p]
-------------------------------------------------------------
```

Remarque
La suite (r_i) des restes est strictement décroissante (par propriété de la division euclidienne), donc elle est finie. C'est ce qui assure que la boucle "tant que" est finie, la condition d'arrêt étant précisément la nullité du reste.

Exemple calcul de PGCD(240,46)

```
-------------------------------------------------------------
This is Extended Euclid Algorithm for (a,b) = (240,46)

Step -1 (initialzation)
Value of u at this step: 1
Value of v at this step: 0
Relation r = a(u)+b(v):  240 = 240*(1)+46*(0)

Step 0 (initialzation)
Value of u at this step: 0
Value of v at this step: 1
Relation r = a(u)+b(v):  46 = 240*(0)+46*(1)

Step 1 (while loop)
Euclidean division 240 div 46   quotient: 5   remainder: 10
Value of u at this step: 1 - 5*(0) = 1
Value of v at this step: 0 - 5*(1) = -5
Relation r = a(u)+b(v):  10 = 240*(1)+46*(-5)

Step 2 (while loop)
Euclidean division 46 div 10   quotient: 4   remainder: 6
Value of u at this step: 0 - 4*(1) = -4
Value of v at this step: 1 - 4*(-5) = 21
Relation r = a(u)+b(v):  6 = 240*(-4)+46*(21)

Step 3 (while loop)
Euclidean division 10 div 6   quotient: 1   remainder: 4
Value of u at this step: 1 - 1*(-4) = 5
Value of v at this step: -5 - 1*(21) = -26
Relation r = a(u)+b(v):  4 = 240*(5)+46*(-26)
```

```
Step 4 (while loop)
Euclidean division 6 div 4   quotient: 1   remainder: 2
Value of u at this step: -4 - 1*(5) = -9
Value of v at this step: 21 - 1*(-26) = 47
Relation r = a(u)+b(v):  2 = 240*(-9)+46*(47)

Step 5 (while loop)
Euclidean division 4 div 2   quotient: 2   remainder: 0
Value of u at this step: 5 - 2*(-9) = 23
Value of v at this step: -26 - 2*(47) = -120
Relation r = a(u)+b(v):  0 = 240*(23)+46*(-120)
Gcd: 2    Bezout coefficients: (-9), (47)
------------------------------------------------------------
```

3.4 Arithmétique modulaire

L'arithmétique modulaire est la branche de l'arithmétique des entiers qui donne une structure algébrique à l'ensemble des classes d'équivalence de la relation de congruence. Étant donné un entier $n \geq 2$, le *module*, on définit une relation d'équivalence sur $\mathbb{Z}$ par "x est congru à y modulo n, et on note $x \equiv y \bmod n$. Les classes d'équivalence s'appellent les *classes de congruence* modulo n. Elles partitionnent $\mathbb{Z}$ en n sous-ensembles :

- $\{\dots, -2n, -n, 0, n, 2n, \dots\}$
- $\{\dots, -2n+1, -n+1, 1, n+1, 2n+1, \dots\}$
- $\{\dots, -2n+2, -n+2, 2, n+2, 2n+2, \dots\}$
- $\dots$
- $\{\dots, -2n+(n-2), -n+(n-2), n-2, n+(n-2), 2n+(n-2), \dots\}$
- $\{\dots, -2n+(n-1), -n+(n-1), n-1, n+(n-1), 2n+(n-1), \dots\}$

L'ensemble des classes forment un ensemble que l'on note $\mathbb{Z}/n\mathbb{Z}$. Un système complet de représentants privilégié est l'ensemble des entiers de 0 à $n-1$, qui se trouve (pas vraiment par hasard) être l'ensemble des restes possibles de la division euclidienne d'un entier par le module n. On écrira en toute rigueur

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-2}, \overline{n-1}\}$$

où $\overline{x}$ désigne la classe de l'entier x. Mais il est d'un usage assez fréquent, traditionnel et parfois plus simple d'identifier une classe et son représentant privilégié. Ainsi on pourra écrire plus simplement

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \dots, n-2, n-1\}$$

Remarque À propos de la notation mod

- Dans une égalité, le symbole " mod " est à comprendre comme la définition de la relation de congruence et on écrira indifféremment

$$x \equiv y \bmod n, \quad \overline{x} = \overline{y}, \quad x = y \text{ dans } \mathbb{Z}/n\mathbb{Z}, \quad x = y \bmod n$$

- Dans une expression isolée, la quantité $a \bmod n$ désigne le représentant privilégié de la classe de a, c'est-à-dire l'unique $r \in \{0, 1, 2, \dots, n-2, n-1\}$ tel que $a \equiv r \bmod n$.

3.4.1 Structure algébrique : l'anneau $\mathbb{Z}/n\mathbb{Z}$

Le cœur de l'arithmétique modulaire tient dans ce que l'ensemble $\mathbb{Z}/n\mathbb{Z}$ hérite des deux lois de composition $+$ et $\times$ de $\mathbb{Z}$ qui lui donnent une structure d'anneau commutatif. En d'autres termes on peut effectuer dans $\mathbb{Z}/n\mathbb{Z}$ des $+, -, \times$ et de temps en temps diviser, d'une manière compatible (cohérente)

avec la relation de congruence, le résultat étant encore dans l'ensemble $\mathbb{Z}/nZ$. Enfin, itérer la multiplication sur un même élément permet de calculer ses puissances entières : on parle d'*exponentiation modulaire*

Exemples Quelques calculs dans $\mathbb{Z}/10\mathbb{Z}$

- $14 \bmod 10 = 4$
- $(-12) \bmod 10 = 8$
- $1 + 5 = 6 \bmod 10$
- $8 - 6 = 2 \bmod 10$
- $3 + 9 = 12 = 2 \bmod 10$
- $4 \times 7 = 28 = 8 \bmod 10$
- $2^6 \bmod 10 = 2 \times \cdots \times 2 \bmod 10 = 4 \bmod 10$

La compatibilité entre les opérations et la congruence signifie qu'à tout moment du calcul on peut représenter un entier par un entier de la même classe de congruence. Illustrons sur le calcul du produit $14 \times 37 \bmod 10$.

- Méthode 1 :
$$14 \times 37 = 518 \text{ produit ordinaire } = 8 \bmod 10$$
- Méthode 2 : comme $14 = 4 \bmod 10$, et que $37 = 7 \bmod 10$, on a
$$14 \times 37 = 4 \times 7 \bmod 10 = 28 \bmod 10 = 8 \bmod 10$$

Les phénomènes inhabituels (et déroutants) dans les calculs modulo n apparaissent autour de l'inversion, notamment à cause de l'existence de diviseurs de zéro. Illustrons d'abord avec quelques exemples, encore modulo 10.

1. l'inverse d'un élément non nul, quand il existe, n'est pas une fraction ou un nombre à virgule, mais un entier modulo n. Par exemple, $3^{-1} \bmod 10$ est l'unique entier a, s'il existe, tel que $3 \times a = 1 \bmod 10$. En l'occurrence,
$$3^{-1} = 7 \bmod 10 \text{ car } 3 \times 7 = 1 \bmod 10.$$
2. tout élément non nul n'est pas forcément inversible : 2 n'est pas inversible modulo 10 car il n'existe pas de a tel que $2 \times a = 1 \bmod 10$
3. on a $4 \times 5 = 0 \bmod 10$, alors que ni 4 ni 5 ne sont nuls modulo 10. 4 et 5 sont des diviseurs de 0 dans $\mathbb{Z}/10\mathbb{Z}$.

Le théorème qui suit donne une description précise de la situation générale.

Théorème-Définition Inversibles de $\mathbb{Z}/n\mathbb{Z}$

Soit n un entier ≥ 2

1. Un élément $a \in \mathbb{Z}/n\mathbb{Z}$ est *inversible* si $\exists b \in \mathbb{Z}/n\mathbb{Z}$ tel que $ab = 1 \bmod n$.
   Dans ce cas, b est unique, noté $a^{-1} \bmod n$, lui-même inversible et d'inverse a
2. 0 n'est pas inversible (situation universelle)
3. un élément $z \in \mathbb{Z}/n\mathbb{Z}$ est un *diviseur de zéro* si $z \neq 0$ et $\exists y \neq 0$ tel que $zy = 0 \bmod n$
   Dans ce cas, y est alors aussi un diviseur de zéro.
4. Dans $\mathbb{Z}/n\mathbb{Z}$, un élément $a \neq 0 \bmod n$ est soit inversible, soit diviseur de zéro : il est
   - inversible si et seulement si $\text{PGCD}(a, n) = 1$
   - un diviseur de 0 si et seulement si $\text{PGCD}(a, n) \neq 1$
5. L'ensemble des inversibles se note $(\mathbb{Z}/n\mathbb{Z})^\times$. Il est inclus dans $\mathbb{Z}/n\mathbb{Z} - \{0\}$, mais, en général, pas égal.
6. Le nombre des inversibles est
$$\text{Card}\{a \ : 0 \leq a \leq n-1 \text{ et } \text{PGCD}(a, n) = 1\}$$

Ce nombre se note $\phi(n)$, et $\phi(.)$ s'appelle la fonction *indicatrice d'Euler*

7. Si $n = p_1^{e_1} \cdots p_s^{e_s}$ (DPFP), alors

$$\phi(n) = (p_1^{e_1} - p_1^{e_1-1}) \cdots (p_s^{e_s} - p_s^{e_s-1}) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_s}\right)$$

8. (Théorème d'Euler) Si $\text{PGCD}(a, n) = 1$, $a^{\phi(n)} = 1 \bmod n$.

3.4.2 Arithmétique modulo p premier

Le paragraphe précédent traite le cas général $n \geq 2$. Lorsque n est premier (que l'on note alors plutôt p) les définitions et manipulations générales de $+$, $-$, $\times$ s'appliquent telles quelles. En revanche, une attention particulière doit être spécifiquement portée aux inverses et aux diviseurs de 0 . Rappelons lorsque p est premier, on a l'implication

$$\forall a \in \mathbb{Z}, \text{PGCD}(a, p) \neq 1 \ \Rightarrow \ p \text{ divise } a$$

En contraposant et en observant que la réciproque est valide (c'est très facile), on a, toujours pour p premier :

$$\forall a \in \mathbb{Z}, p \text{ ne divise pas } a \ \Leftrightarrow \ \text{PGCD}(a, p) = 1$$

Or la condition $\text{PGCD}(a, p) = 1$ équivaut à "a est inversible modulo p" (point 4 du théorème-définition), c'est-à-dire inversible dans $\mathbb{Z}/p\mathbb{Z}$, tandis que "p ne divise pas a" équivaut à $a \neq 0 \bmod p$, c'est-à-dire a est non nul dans $\mathbb{Z}/p\mathbb{Z}$. Ce jeu de d'équivalences successives montre que, dans $\mathbb{Z}/p\mathbb{Z}$, contrairement au cas général, tout élément non nul est inversible. De ce point de vue, le cas p premier est plus proche de la situation des réels ou des complexes. Comme autre conséquence, $\phi(p) = p - 1$. Nous voilà prêts à reformuler le théorème-définition des inversibles dans le cas p premier.

Théorème-Définition Inversibles de $\mathbb{Z}/p\mathbb{Z}$

Soit p un entier premier

1. Dans l'anneau $\mathbb{Z}/p\mathbb{Z}$, tout élément $a \neq 0 \bmod p$ est inversible ; il n'y a pas de diviseur de 0. On dit que $\mathbb{Z}/p\mathbb{Z}$ est un *corps*. On le note aussi $\mathbb{F}_p$.
2. L'ensemble des inversibles $(\mathbb{Z}/p\mathbb{Z})^\times$ est égal $\mathbb{Z}/p\mathbb{Z} - \{0\}$
3. Le nombre des inversibles est $\phi(p) = p - 1$
4. (Petit théorème de Fermat) Si $\text{PGCD}(a, p) = 1$, $a^{p-1} = 1 \bmod p$.

Remarque Nous croyons opportun d'insister sur le fait que cette version est spécifique du cas p premier : telles qu'elles sont formulées, toutes les propriétés sont fausses pour p non premier.

3.4.3 Existence et calcul de l'inverse de a modulo n, pour $a \in \{1, \ldots, n-1\}$

Méthode 1 *Recherche exhaustive*
On calcule la liste des valeurs $a \times k \bmod n$, pour $k = 1, \ldots, n-1$, que l'on pourrait appeler la table de multiplication de a modulo n. Si l'une de ces valeurs, disons $a \times k_0$ est égale à 1 (ce sera alors la seule), c'est gagné : a est inversible et $a^{-1} \bmod n = k_0$. On observera que cette méthode permet de répondre aux deux questions (existence et calcul) en même temps.

Méthode 2 *Par Euler/Fermat*
Contrairement à la première méthode, celle-ci répond en deux temps. Il faut d'abord chercher si a est inversible en testant si $\text{PGCD}(a, n) = 1$. Puis si c'est le cas, calculer l'inverse par la formule $a^{\phi(n)-1} \bmod n$ ($a^{p-2} \bmod p$ pour $n = p$ premier)

Méthode 3 *L'algorithme d'Euclide étendu*
Comme la méthode 1, celle-ci répond aux deux questions en même temps. Exécutons l'algorithme d'Euclide étendu sur les entrées a et n. La sortie est un triplet (d, u, v), avec $d = \text{PGCD}(a, n) = au + bv$. Alors :

— si $d = 1$, alors a est inversible modulo n, et $a^{-1} \bmod n = u \bmod n$. Quitte à remplacer u par $u \bmod n$, on peut faire en sorte que $u \in \{0, \ldots, n-1\}$.

— si $d \neq 1$, alors a n'est pas inversible modulo n.

La méthode 3 est nettement plus efficace que les deux autres pour des grandes valeurs de a et n. Elle est fortement recommandée dans ce cas lorsque la rapidité de calcul est un critère important.

3.4.4 Arithmétique et algèbre modulo 2

Le cas $p = 2$ ne présente au premier abord que peu d'intérêt. En effet, il consiste à travailler dans le corps $\mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2 = \{0, 1\}$ dont les tables d'addition et de multiplication se réduisent à deux tout petits tableaux :

$+$	0	1
0	0	1
1	1	0

et

$\times$	0	1
0	0	0
1	0	1

L'égalité $1+1 = 0$ implique en particulier $1 = -1$. Autrement dit, quand on travaille modulo 2, tout signe "$-$" peut être immédiatement remplacé par un signe "$+$". Par ailleurs, les puissances avec exposants > 1 sont inutiles, puisque pour tout $e \geq 1$, on a à la fois $0^e = 0$ et $1^e = 1$.

Remarque

Afin de sous-entendre le modulo 2 en évitant toute ambiguïté, l'addition modulo 2 est parfois notée "$\oplus$".

L'intérêt majeur du corps $\mathbb{F}_2$ est de modéliser les opérations de la logique booléenne via deux "transcriptions" :

1. identifier l'alphabet booléen avec $\mathbb{F}_2$: $0 \sim$ `faux`, $1 \sim$ `vrai`
2. exprimer les fonctions booléennes telles que des connecteurs comme des polynômes à plusieurs variables à coefficients dans $\mathbb{F}_2$, pour lesquels les opérations sont $+$ et $\times$.

Exemples

On vérifiera que

1. négation : $\neg x = 1 \oplus x$
2. conjonction : $x \wedge y = xy$
3. disjonction : $x \vee y = x \oplus y \oplus xy$

L'avantage de cette transcription est que la structure de corps de $\mathbb{F}_2$ est plus riche, plus souple et plus commode à travailler que la structure de l'alphabet booléen $\{$`faux`, `vrai`$\}$; les opérations $\oplus$ et $\times$ modulo 2 sont plus parlantes que les connecteurs logiques, et enfin faire des calculs algébriques sur des polynômes à plusieurs variables est plus culturel et plus courant que faire des calculs logiques que sur des propositions à plusieurs variables.

Exemple

On définit le connecteur OU EXCLUSIF, noté XOR (de l'anglais EXCLUSIVE OR), par

$$x \text{ XOR } y = (x \wedge \neg y) \vee (\neg x \wedge y)$$

Autrement dit, la variable booléenne x XOR y est vraie si et seulement l'une exactement des deux variables x ou y est vraie. On va calculer la forme algébrique (polynomiale) correspondant à cette forme logique, en utilisant la correspondance ci-dessus. On a

$$\begin{array}{lcll}
x \text{ XOR } y & = & (x \wedge \neg y) \vee (\neg x \wedge y) & \text{par définition du XOR} \\
& = & (x \wedge (1 \oplus y)) \vee ((1 \oplus x) \wedge y) & \text{car } \neg a = 1 \oplus a \\
& = & (x(1 \oplus y)) \vee ((1 \oplus x)y) & \text{car } a \wedge b = ab \\
& = & (x \oplus xy) \vee (y \oplus xy) & \text{en développant chacune de parenthèse} \\
& = & (x \oplus xy) \oplus (y \oplus xy) \oplus (x \oplus xy)(y \oplus xy) & \text{car } a \vee b = a \oplus b \oplus ab \\
& = & x \oplus xy \oplus y \oplus xy \oplus (xy \oplus x^2y \oplus xy^2 \oplus x^2y^2) & \text{en développant} \\
& = & x \oplus xy \oplus y \oplus xy \oplus (xy \oplus xy \oplus xy \oplus xy) & \text{en utilisant } a^2 = a \\
& = & x \oplus y & \text{en appliquant } a \oplus a = 0 \text{ de manière répétée}
\end{array}$$

Ce résultat semble correct. On vérifie directement que $x \oplus y$ est 1 (vrai) si et seulement si l'une exactement des variables x et y vaut 1 (vrai) et l'autre 0 (faux) : cela se lit sur la table d'addition du + modulo 2

Chapitre 4

Calcul matriciel. Systèmes linéaires

4.1 Introduction

En algèbre, le calcul matriciel est un outil de formalisation et de représentation de tout ce qui a trait aux espaces vectoriels et aux applications linéaires. Dans le cadre de ce cours, nous n'entrerons pas dans le détail profond du lien entre ces objets. Nous nous contenterons de présenter les matrices de manière autocontenue, de donner les principales définitions, opérations et manipulations. Nous montrerons une application classique de cet outil : la résolution de systèmes linéaires.

4.2 Présentation générale des matrices

Grossièrement, une matrice est un tableau double entrée dont les coefficients sont des réels ou des complexes, que l'on appelle les *scalaires*. Les notations classiques sont les suivantes : si A est une matrice à coefficients dans K ($= \mathbb{R}$ ou $\mathbb{C}$) possédant n lignes et p colonnes, on écrit $A = [a_{i,j}]_{1 \leq i \leq n, 1 \leq j \leq p}$. Le scalaire $a_{i,j}$ est le *terme général* de la matrice, il est repéré par deux indices : le premier est l'indice de ligne, et le deuxième l'indice de colonne. Il est aussi noté $A_{i,j}$. En fait, il n'y a pas de notation unifiée standard et, dans la pratique, la plupart des notations sont assez claires et non ambigües. La représentation expansée du tableau s'écrit

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,p} \\ a_{2,1} & a_{2,2} & \dots & a_{2,p} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \dots & a_{n,p} \end{bmatrix}$$

Lorsque $n = p$, la matrice est dite *carrée*. Dans le cas général, elle est dite *rectangulaire*. Lorsque $n > p$ (resp. $n < p$), on parlera de matrice rectangulaire large (resp. rectangulaire haute)

L'ensemble des matrices n lignes p colonnes à coefficients dans K est noté $M_{n,p}(K)$. Lorsque $n = p$, on écrit indifféremment $M_n(K)$ et $M_{n,n}(K)$. On parle du *gabarit* d'une matrice pour référer ses dimensions, c'est-à-dire la largeur (nombre de colonnes) et hauteur (nombre de lignes). À noter qu'on trouve très fréquemment (en particulier dans la littérature mathématique anglo-saxone) la notation "A une matrice $n \times p$" comme raccourci de "A une matrice n lignes p colonnes".

Lorsque $n = 1$ (resp $p = 1$), la matrice est dite *uniligne* (resp. *unicolonne*), mais une tradition très répandue privilégie l'appellation *vecteur ligne* (resp. *vecteur colonne*).

Les éléments $a_{i,i}$, pour lesquels l'indice de ligne et égal à l'indice de colonne, s'appellent les *éléments diagonaux*. Lorsque la matrice est carrée, cette appellation est intuitive car les éléments forment graphiquement la diagonale du carré qui représente la matrice. On conserve l'appellation dans le cas des matrices rectangulaires, bien que cela ne corresponde pas du tout à la diagonale graphique du rectangle.

Exemple

La matrice $A \in M_{3,4}(\mathbb{R})$ définie par

$$A = \begin{bmatrix} 1 & 5 & -2 & 4 \\ 13/3 & \sqrt{2} & 8 & -\sqrt{3} \\ -2 & -3/2 & \pi & 11 \end{bmatrix}$$

a pour diagonale $(1, \sqrt{2}, \pi)$.

Définition Matrice identité

Pour tout entier $n \geq 1$, on appelle *matrice identité* ou *matrice unité* $n \times n$, notée I_n ou Id_n, la matrice carrée contenant des "1" sur la diagonale et des "0" partout ailleurs.

Définition Sous-matrice

Une *sous-matrice*, ou *matrice extraite*, de A est une matrice $n' \times p'$ obtenue à partir de A en :

— choisissant $n' \leq n$ indices de lignes $I = \{i_1, \ldots, i_{n'}\}$ et $p' \leq p$ indices de colonnes $J = \{j_1, \ldots, j_{p'}\}$

— conservant de A les éléments d'indice de ligne $\in I$ et d'indice de colonne $\in J$

Cela revient, une fois choisis les sous ensembles d'indices I et J, à effacer de A les lignes d'indice $\notin I$ et les colonnes d'indices $\notin J$.

Il n'y a pas de notation universellement adoptée pour une sous matrice. Une possibilité est de noter $A_{I,J}$

Remarques

1. Il n'est pas demandé que les indices de lignes (resp. indices de colonnes) sélectionnés soient consécutifs. Dans une matrice 10×6, on peut extraire, entre autres exemples :
   — les lignes (1,2,3) et les colonnes (3,4)
   — les lignes paires (2,4,6,8,10), et les colonnes multiples de 3 (3,6)
   — franchement irrégulièrement ; lignes (1,3,4,6,8) colonnes (2,3,5)

   Dans le dernier cas, cela donne avec un petit dessin (on met en rouge les éléments à effacer)

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} & a_{1,5} & a_{1,6} \\ a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} & a_{2,5} & a_{2,6} \\ a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} & a_{3,5} & a_{3,6} \\ a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} & a_{4,5} & a_{4,6} \\ a_{5,1} & a_{5,2} & a_{5,3} & a_{5,4} & a_{5,5} & a_{5,6} \\ a_{6,1} & a_{6,2} & a_{6,3} & a_{6,4} & a_{6,5} & a_{6,6} \\ a_{7,1} & a_{7,2} & a_{7,3} & a_{7,4} & a_{7,5} & a_{7,6} \\ a_{8,1} & a_{8,2} & a_{8,3} & a_{8,4} & a_{8,5} & a_{8,6} \\ a_{9,1} & a_{9,2} & a_{9,3} & a_{9,4} & a_{9,5} & a_{9,6} \\ a_{10,1} & a_{10,2} & a_{10,3} & a_{10,4} & a_{10,5} & a_{10,6} \end{bmatrix} \rightsquigarrow A_{\{1,3,4,6,8\},\{2,3,5\}} = \begin{bmatrix} a_{1,2} & a_{1,3} & a_{1,5} \\ a_{3,2} & a_{3,3} & a_{3,5} \\ a_{4,2} & a_{4,3} & a_{4,5} \\ a_{6,2} & a_{6,3} & a_{6,5} \\ a_{8,2} & a_{8,3} & a_{8,5} \end{bmatrix}$$

2. Lorsque I et J sont de même cardinal k, la sous-matrice est carrée $k \times k$: on l'appelle un *mineur d'ordre* k de A.
3. Lorsque $I = J$, on parle de *mineur diagonal*
4. Lorsque $I = J = \{1, \ldots, k\}$, on parle de *mineur principal*.

4.3 Opérations sur les matrices

Nous souhaitons d'ores et déjà annoncer en préambule que toutes les opérations ne sont pas possibles avec n'importe quelles matrices. Certaines opérations requièrent en effet des conditions de gabarit entre les opérandes.

4.3.1 Transposition

Définition

La *transposée* d'une matrice A $n \times p$ est la matrice $p \times n$ notée ${}^tA$ obtenue en effectuant graphiquement une symétrie miroir par rapport à la diagonale. Algébriquement, si $A = [a_{i,j}]_{1 \leq i \leq n, 1 \leq j \leq p}$, alors ${}^tA = [a_{j,i}]_{1 \leq j \leq p, 1 \leq i \leq n}$

Exemple

Si A est la même matrice que ci-dessus,

$$ {}^tA = \begin{bmatrix} 1 & 13/3 & -2 \\ 5 & \sqrt{2} & -3/2 \\ -2 & 8 & \pi \\ 4 & -\sqrt{3} & 11 \end{bmatrix} $$

4.3.2 Addition de matrices

Définition

L'addition de deux matrices A et B se fait composante à composante. Elle est possible si et seulement si A et B ont le même gabarit $n \times p$, le résultat étant aussi $n \times p$. Ainsi

$$ \forall\ 1 \leq i \leq n,\ \forall\ 1 \leq j \leq p,\ (A+B)_{i,j} = a_{i,j} + b_{i,j} $$

Exemple

Pour $A = \begin{bmatrix} 3 & 7 & -4 \\ -13 & 2 & 2 \end{bmatrix}$, $B = \begin{bmatrix} -1 & 10 & 5 \\ 9 & -8 & 5 \end{bmatrix}$, on a $A + B = \begin{bmatrix} 2 & 17 & 1 \\ -4 & -6 & 7 \end{bmatrix}$

L'opération se généralise à un nombre quelconque de matrices, pourvu qu'elles aient toutes le même gabarit. Un gabarit $n \times p$ étant donné, l'addition des matrices est une loi de composition interne :

- commutative
- associative
- admettant pour élément neutre la matrice $O_{n,p}$ dont tous les coefficients sont nuls
- et pour laquelle toute matrice A admet une matrice opposée notée $-A$

4.3.3 Multiplication par un scalaire

Définition

Soit $\lambda \in K$ et $A \in M_{n,p}(K)$. Alors la matrice λA est définie en faisant le produit de chaque composante par λ :

$$ \forall\ 1 \leq i \leq n,\ \forall\ 1 \leq j \leq p,\ (\lambda\ A)_{i,j} = \lambda a_{i,j} $$

Cette opération est possible quel que soit le gabarit de A.

Par convention, le produit matrice-scalaire $A\lambda$ est défini comme égal à λA. On a, entre autres, $0A = O_{n,p}$, $1A = A$, et aussi $-A = (-1)\ A$

4.3.4 Multiplication de deux matrices

La multiplication de deux matrices est sans doute l'opération la moins intuitive. Elle le devient un peu plus si l'on étudie en profondeur le lien entre matrices et applications linéaires d'espaces vectoriels, mais nous avons pris le parti de ne pas le faire ici.

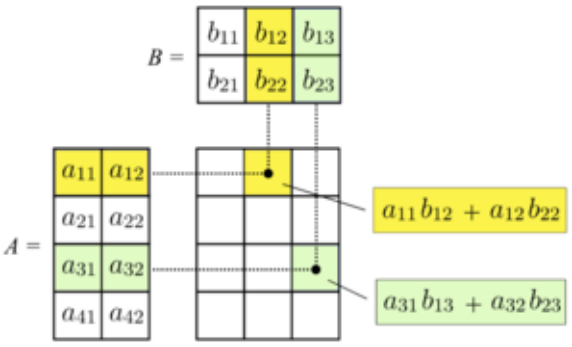
Définition

Soient A et B deux matrices de gabarit $n_A \times p_A$ et $n_B \times p_B$. Le produit AB existe si et seulement si $p_A = n_B$. Dans ce cas,

- AB a pour gabarit $n_A \times p_B$

— pour $1 \leq i \leq n_A$, $1 \leq j \leq p_B$, on a $(AB)_{i,j} = \sum_{k=1}^{p_A} a_{i,k} b_{k,j} = a_{i,1} b_{1,j} + \cdots + a_{i,p_A} b_{p_A,j}$

La figure suivante illustre tant les conditions de gabarit que le calcul des composantes du produit



Source :Wikipedia

Le produit matriciel n'est pas commutatif. Plus précisément,

— le produit AB (resp. BA) existe si $p_A = n_B$ (resp. si $p_B = n_A$). Ainsi l'un des deux produits peut exister sans que l'autre n'existe.

— Si $p_A = n_B \neq p_B = n_A$ les deux produits AB et BA existent, sont carrées mais de tailles différentes, donc ne peuvent être égaux.

— Si $p_A = n_B = p_B = n_A$ (A et B sont carrées de même taille, disons n), alors les deux produits AB et BA existent et sont aussi de taille n. Mais même dans ce cas, on a en général $AB \neq BA$.

Le produit matriciel est **associatif**.
Si A, B, C sont trois matrices de gabarits adéquats telles que les produits AB et BC existent, les produits $(AB)C$ et $A(BC)$ existent et sont égaux, ce qui permet d'omettre les parenthèses et de le noter ABC. Cette propriété se généralise au cas d'un nombre quelconque de matrices

Théorème

1. Le produit de s matrices $A_1, \ldots, A_s$ existe et est noté $A_1 \cdots A_s$, si et seulement si pour tout couple de facteurs adjacents A_i et A_{i+1} $(= 1, \ldots, s-1)$ dans le produit global, le produit $A_i A_{i+1}$ existe.
2. dans ce cas, le produit est associatif, c'est-à-dire que tous les parenthésages de l'expression $A_1 \cdots A_s$ sont possibles et donnent le même résultat.

Les matrices identités sont des éléments "partiellement neutres" (on omet volontairement les considérations et le vocabulaire rigoureux) : si A est une matrice $n \times p$, on a $I_n\ A = A\ I_p = A$ (on vérifie que ces produits existent).

4.3.5 Propriétés des opérations

Voici un pot pourri des propriétés les plus utiles. Afin de faciliter la lecture, les gabarits des matrices ne sont pas explicités, mais le lecteur pourra vérifier que chacune des formulations est compatible des gabarits implicites.

Propriétés

1. ${}^t({}^tA) = A$
2. ${}^t(A + B) = ({}^tA) + ({}^tB)$
3. ${}^t(AB) = ({}^tB)({}^tA)$
4. ${}^t(\lambda A) = \lambda({}^tA)$
5. Distributivité $A(B + C) = AB + AC$ et $(A + B)C = AC + BC$

6. Associativité généralisée (acte 1) : $(\lambda)(\mu A) = (\lambda\mu)A$
7. Associativité généralisée (acte 2) : $\lambda(AB) = (\lambda A)B = A(\lambda B)$
8. Associativité généralisée (acte final) : dans un produit mélangeant des produits matriciels et de produits scalaire-matrice, $\lambda_1 A_1 \lambda_2 A_2 \cdots \lambda_s A_s$, on peut (sans changer le résultat final)
   - adopter n'importe quel parenthésage
   - permuter, regrouper, redistribuer, etc. les scalaires pourvu qu'on ne change pas l'ordre des matrices

   Par exemple, on a $(2A)(3B)(5C) = (2 \cdot 3 \cdot 5)ABC = 30ABC = A(15B)(2C) =$ etc., mais c'est $\neq 30BAC$.
9. Distributivité généralisée (acte 1) : $(\lambda + \mu)A = \lambda A + \mu A$
10. Distributivité généralisée (acte 2) : $\lambda(A + B) = \lambda A + \lambda B$

4.4 Réduction de Gauss. Forme échelon

Définition

1. Une matrice $A \in M_{n,p}(K)$ est dite *échelonnée en lignes* si le nombre de zéros précédant la première valeur non nulle d'une ligne augmente strictement ligne par ligne jusqu'à ce qu'il ne reste éventuellement plus que des zéros.

$$\begin{bmatrix} \blacksquare & * & * & * & * & * & * & * & * \\ 0 & 0 & \blacksquare & * & * & * & * & * & * \\ 0 & 0 & 0 & \blacksquare & * & * & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & \blacksquare & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \blacksquare \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

   Le premier élément non nul d'une ligne, noté ici "■", est appelé *pivot*. Les "$*$" signifient des éléments quelconques, nuls ou pas.
2. La matrice est dite *échelonnée réduite* si elle est échelonnée et que, de plus :
   - tous les pivots sont égaux à 1
   - pour toute colonne contenant un pivot, les éléments autre que le pivot sont nuls

$$\begin{bmatrix} \boxed{1} & * & 0 & 0 & * & * & 0 & * & 0 \\ 0 & 0 & \boxed{1} & 0 & * & * & 0 & * & 0 \\ 0 & 0 & 0 & \boxed{1} & * & * & 0 & * & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \boxed{1} & * & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \boxed{1} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

On définit de manière analogue l'échelonnement en colonnes (par exemple en travaillant sur la transposée). Dans le cadre de notre cours, nous ne considérons que les échelonnement en lignes, si bien que nous omettrons la précision sans ambiguïté.

4.4.1 Réduction de Gauss

La méthode du *pivot de Gauss*, aussi connue sous le nom de *réduction de Gauss*, ou *élimination de Gauss-Jordan*, consiste à modifier une matrice en appliquant une séquence d'opérations sur les lignes, dites "opérations élémentaires" :

Type 1 permuter deux lignes : $L_i \leftrightarrow L_j$, pour $i \neq j$

Type 2 multiplier une ligne par un scalaire non nul : $L_i \leftarrow \alpha L_i, \alpha \neq 0$

Type 3 ajouter à une ligne une multiple d'une autre ligne : $L_i \leftarrow L_i + \lambda L_j$, pour $i \neq j$.

et ce afin d'amener la matrice initiale à une forme particulière, généralement échelonnée, triangulaire ou diagonale.

À noter que, contrairement à ce que suggèrent certaines habitudes, il n'est pas nécessaire de supposer $\lambda \neq 0$ dans l'opération de type 3. Si $\lambda = 0$, l'opération correspond à "ne rien faire", ce qui peut paraitre artificiel mais s'avère en fait très commode.

Algorithme Pivot de Gauss

$r \leftarrow 0$ // r est l'indice de ligne du dernier pivot trouvé
for $j = 1$ to p **do** // j décrit tous les indices de colonnes
  $i_{\max} \leftarrow \text{argmax}(i : |A[i,j]|, r+1 \leq i \leq n)$ // $A[i_{\max}, j]$ est le pivot
  if $A[i_{\max}, j] \neq 0$ **then**
    $r \leftarrow r + 1$ // r désigne l'indice de la future ligne servant de pivot
    $L_{i_{\max}} \leftarrow A[i_{\max}, j]^{-1} L_{i_{\max}}$ // Normalisation du pivot à 1
    if $i_{\max} \neq r$ **then**
      $L_{i_{\max}} \leftrightarrow L_r$ // On place la ligne du pivot en position r
    end if
    for $i = 1$ to n **do** // On s'appuie sur le pivot $A[r,j] = 1$ pour mettre à 0 les $A[i,j]$ pour $i \neq r$
      if $i \neq r$ **then**
        $L_i \leftarrow L_i - A[i,j] L_r$
      end if
    end for
  end if
end for

Remarque .
Une variante dite *légère* de la réduction de Gauss consiste à :

1. ne pas chercher comme pivot le max de la sous-colonne, mais prendre un élément quelconque non nul de la colonne
2. ne pas normaliser les pivots à 1
3. mettre des "0" seulement en-dessous des pivots et pas dans toute la colonne

Théorème Échelonnement d'une matrice

1. Toute matrice $A \in M_{n,p}(K)$ peut être transformée en une matrice échelonnée réduite (resp. en une matrice échelonnée) par la méthode (resp. la méthode légère) du pivot de Gauss.
2. Il y a plusieurs matrices échelonnées possibles, mais toutes ont le même nombre de pivots.
3. Il y a unicité de la matrice échelonnée réduite

4.5 Matrices carrées

L'ensemble des matrices $n \times n$ hérite naturellement de la loi d'addition, du produit scalaire-matrice, et de leurs propriétés respectives comme simple cas particulier des matrices quelconques. Bref, pour ces deux lois, rien de fondamentalement nouveau sous le soleil.

4.5.1 Propriétés particulières du produit matriciel

C'est du coté du produit matriciel que nous avons quelques nouveautés. À cause de la règle (générale) sur le produit et les gabarits, le produit de deux matrices $n \times n$ existe toujours et le résultat est lui-même $n \times n$. La multiplication est donc une loi de composition interne de $M_n(K)$. Nous avons déjà vu qu'elle est associative (cela découle du cas général), non-commutative et distributive par rapport à l'addition. Voici les nouveautés :

Proposition

— La matrice identité I_n est élément neutre de la multiplication matricielle :

$$\forall A \in M_n(K) \quad AI_n = I_n A = A$$

— Soit A une matrice. Sont équivalentes (ce n'est pas évident car le produit est non commutatif)

(1) il existe A' telle que $A'A = I_n$

(2) il existe A'' telle que $AA'' = I_n$

Dans ce cas, la matrice A est dite inversible, $A' = A''$, s'appelle l'*inverse* de A et est notée A^{-1}. On a ainsi : $A^{-1}A = AA^{-1} = I_n$

L'ensemble des matrices (carrées) inversibles se note $GL_n(K)$.

Remarques .

1. Si A est inversible, alors A^{-1} est aussi inversible et $(A^{-1})^{-1} = A$
2. Si A est inversible, alors ${}^tA$ est aussi inversible et ${}^t(A^{-1}) = ({}^tA)^{-1}$
3. La matrice I_n est inversible et égale à sa propre inverse.
4. La matrice nulle O_n n'est pas inversible. C'est loin d'être la seule. Nous verrons bientôt pourquoi.

4.5.2 Quelques types particuliers de matrices carrées

Définitions

Soit A une matrice $n \times n$

1. A est *symétrique* si ${}^tA = A$
2. A est *antisymétrique* si ${}^tA = -A$. En particulier, cela implique que la diagonale de A est nulle.
3. A est *diagonale* si tous ses éléments hors diagonaux sont non nuls. Sur la diagonale, les éléments sont quelconques.
4. A est *triangulaire supérieure* (TS) si les éléments sous la diagonale sont nuls, c'est-à-dire que la partie "utile" se trouve dans le triangle supérieur. Si en plus les éléments diagonaux sont nuls, A est *triangulaire supérieure stricte* (TSS)
5. On a une définition analogue pour *triangulaire inférieure* (TI) et *triangulaire inférieure stricte* (TIS)

Les classes de matrices citées dans la définition précédentes sont stables par addition et par produit scalaire-matrice - c'est presque évident à démontrer. Par ailleurs, les matrices symétriques et anti-symétriques ne sont **pas stables par multiplication** (c'est moins évident). En revanche, nous avons la

Propriété Stabilité multiplicative des matrices triangulaires

— L'ensemble des matrices TS est stable par multiplication matricielle.

— (Contrairement au cas général) : si A et B sont TS, les éléments diagonaux de AB sont les produits "position à position" des éléments diagonaux de A et de B :

$$\forall 1 \leq i \leq n, \ (AB)_{i,i} = a_{i,i}b_{i,i}$$

La propriété de stabilité multiplicative reste vraie si l'on remplace "TS" par 'TSS", "TI", "TIS" ou "diagonales"

4.5.3 Déterminant d'une matrice carrée

Définition

Le déterminant d'une matrice carrée $A = [a_{i,j}]$ est

$$\det(A) = \sum_{\sigma \in \mathcal{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{\sigma i, i}$$

où $\mathcal{S}_n$ désigne l'ensemble des permutations de $\{1, \ldots, n\}$ et, pour tout $\sigma \in \mathcal{S}_n$, $\varepsilon(\sigma)$ la *signature* de la permutation σ.

Comme cette définition n'est ni facile à manipuler, ni efficace pour réaliser le calcul concrètement, nous allons la mettre dans un joli cadre, l'accrocher au mur et ne plus y toucher. Le théorème suivant, que nous admettrons sans démonstration, peut être pris comme une définition alternative du déterminant, et permet de surcroit de réaliser les calculs de manière un peu plus agréable. Nous avons besoin d'une notation : pour $1 \leq i, j \leq n$, $A_{\neq i, \neq j}$ désigne le mineur d'ordre $(n-1) \times (n-1)$ obtenu en barrant la ligne i et la colonne j.

Théorème Définition récursive du déterminant

Soit A une matrice $n \times n$.

— si $n = 1$ $\det(A) = a_{1,1}$, l'unique coefficient de la matrice.

— si $n = 2$, $\det(A) = \det \begin{bmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{bmatrix} = \begin{vmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{vmatrix} = a_{1,1}a_{2,2} - a_{1,2}a_{2,1}$

— pour $n \geq 3$ quelconque, on a :

1. (*développement selon une colonne*) : pour tout indice de colonne j_0 fixé,

$$\det(A) = \sum_{i=1}^{n} a_{i,j_0} \times (-1)^{i+j_0} \times \det(A_{\neq i, \neq j_0})$$

2. (*développement selon une ligne*) : pour tout indice de ligne i_0 fixé,

$$\det(A) = \sum_{j=1}^{n} a_{i_0,j} \times (-1)^{i_0+j} \times \det(A_{\neq i_0, \neq j})$$

La récursivité vient de ce que le déterminant $n \times n$ à gauche dans la formule s'exprime en fonction de n déterminants $(n-1) \times (n-1)$ à droite dans la formule. On itère alors jusqu'à ce que la taille du déterminant soit 2, où la formule est donnée explicitement.

Illustrations

1. Développement selon la 2me colonne

$$\begin{vmatrix} -1 & 2 & 5 \\ 1 & 2 & 3 \\ -2 & 8 & 10 \end{vmatrix} = -2 \begin{vmatrix} 1 & 3 \\ -2 & 10 \end{vmatrix} + 2 \begin{vmatrix} -1 & 5 \\ -2 & 10 \end{vmatrix} - 8 \begin{vmatrix} -1 & 5 \\ 1 & 3 \end{vmatrix}$$
$$= -2(1 \times 10 - 3 \times (-2)) - 2(-1 \times 10 - 5 \times (-2)) - 8(-1 \times 3 - 5 \times 1)$$
$$= -2(16) + 0 - 8(-8) = -32 + 64 = 32$$

2. Développement selon la 2me ligne

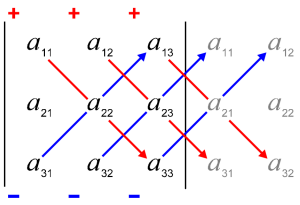
$$\begin{vmatrix} 2^{+} & -1^{-} & 2^{+} \\ 6^{-} & 3^{+} & 1^{-} \\ 4^{+} & 5^{-} & 3^{+} \end{vmatrix} = -6 \times \begin{vmatrix} 2 & -1 & 2 \\ 6 & 3 & 1 \\ 4 & 5 & 3 \end{vmatrix} + 3 \times \begin{vmatrix} 2 & -1 & 2 \\ 6 & 3 & 1 \\ 4 & 5 & 3 \end{vmatrix} - 1 \begin{vmatrix} 2 & -1 & 2 \\ 6 & 3 & 1 \\ 4 & 5 & 3 \end{vmatrix}$$
$$= -6 \times (-13) + 3 \times (-2) - 1 \times 14 = 58.$$

Remarques

1. La formule est valable quel que soit l'indice de colonne j_0 (resp. l'indice de ligne i_0) choisi.
2. Les termes de la somme sont de la forme a_{i,j_0} (resp. $a_{i_0,j}$)$\times$ un mineur d'ordre $(n-1)\times(n-1)$. Il va donc être rentable de choisir une colonne (resp. une ligne) contenant beaucoup de 0 : en effet, pour chaque a_{i,j_0} (resp. $a_{i_0,j}$) nul, on s'épargne le calcul du mineur $\det(A_{\neq i,\neq j_0})$ (resp. $\det(A_{\neq i_0,\neq j})$
3. Dans le cas $n=3$, on dispose de la règle de Sarrus,

$$\det(A) = a_{1,1}a_{2,2}a_{3,3} + a_{1,2}a_{2,3}a_{3,1} + a_{1,3}a_{2,1}a_{3,2} - a_{3,1}a_{2,2}a_{1,3} - a_{3,2}a_{2,3}a_{1,1} - a_{3,3}a_{2,1}a_{1,2}$$

dont il est plus aisé de retenir le schéma mnémotechnique :



Par exemple,

$$\det\begin{bmatrix} -1 & 2 & 5 \\ 1 & 2 & 3 \\ -2 & 8 & 10 \end{bmatrix} = (-1)\cdot 2\cdot 10 + 2\cdot 3\cdot(-2) + 5\cdot 1\cdot 8 - (-2)\cdot 2\cdot 5 - 8\cdot 3\cdot(-1) - 10\cdot 1\cdot 2 = 32$$

(on retrouve évidemment la même valeur que ci-dessus !)

Propriétés Déterminants et lois de composition

1. $\det(A) = \det({}^tA)$. (C'est cette propriété qui permet d'échanger les rôles des lignes et des colonnes).
2. Il n'y a **pas de formule générale** pour $\det(A+B)$
3. $\det(\lambda A) = \lambda^n \det(A)$
4. $\det(AB) = \det(A)\det(B)$.

Voici une deuxième liste de propriétés très couramment utilisées pour le calcul effectif.

Propriétés

1. si A est TS (ou TI, ou diagonale), $\det(A)$ = produit des éléments diagonaux
2. en particulier, $\det(I_n) = 1$
3. le déterminant est nul si la matrice contient une colonne (resp. ligne) de 0
4. si on échange deux colonnes (resp. deux lignes) sans toucher aux $(n-2)$ autres, le déterminant est multiplié par (-1) (changé en son opposé)
5. le déterminant est inchangé si on ajoute à une colonne (resp. ligne) donnée une combinaison linéaire des $(n-1)$ autres sans les changer
6. si on multiplie une colonne (resp. ligne) donnée par un scalaire α, le déterminant est multiplié par α

Ces propriétés donnent en particulier le comportement du déterminant lors d'opérations élémentaires de la réduction de Gauss. Ceci conduit à un algorithme de calcul du déterminant (génériquement la plus efficace). Partant d'une matrice, on atteint une forme TS (éventuellement diagonale) par une suite d'opérations élémentaires sur les lignes. Comme on connait le dernier déterminant (produit des éléments diagonaux) et qu'on sait à chaque étape comment le déterminant a été modifié, on en déduit la valeur du déterminant de la matrice initiale. À noter que l'utilisation de la variante légère de la réduction de Gauss est suffisante.

La proposition suivante généralise de manière très puissante le résultat sur le déterminant d'une matrice triangulaire.

Proposition Déterminant d'une matrice triangulaire de matrices

Soient $A_1, A_2, \ldots, A_s$ des matrices carrées $n_1 \times n_1, n_2 \times n_2, \ldots, n_s \times n_s$, avec $n_1, n_2, \ldots, n_s$ non nécessairement égaux entre eux. Alors on a

$$\det \begin{bmatrix} \boxed{A_1} & * & \ldots & * \\ O & \boxed{A_2} & * & \vdots \\ \vdots & \ddots & \ddots & * \\ O & \ldots & O & \boxed{A_s} \end{bmatrix} = \det(A_1)\det(A_2)\cdots\det(A_s)$$

La "grande" matrice carrée est de taille $n_1 + n_2 + \cdots + n_s$.

Le dernier théorème de cette section est un fondamental incontournable. C'est le critère le plus connu et utilisé pour tester l'inversibilité d'une matrice.

Théorème Lien entre déterminant et inversibilité

Une matrice A carrée est inversible si et seulement si $\det(A) \neq 0$. Dans ce cas, on a $\det(A^{-1}) = \dfrac{1}{\det(A)}$

4.5.4 Inversion d'une matrice carrée

Ce paragraphe décrit trois méthodes de calcul de l'inverse

Par polynôme annulateur

Pour tout polynôme $P(X) = b_s X^s + b_{s-1}X^{s-1} + \cdots + b_1 X + b_0$ à coefficients dans K et toute matrice $A \in M_n(K)$, on définit le polynôme matriciel

$$P(A) = b_s A^s + b_{s-1}A^{s-1} + \cdots + b_1 A + b_0 I_n$$

aisément calculable à l'aide des lois de composition. On dit qu'un polynôme P est un *annulateur* de la matrice A si $P(A) = O_n$. Nous avons alors un critère d'inversibilité

Proposition

1. A est inversible si et seulement s'il existe un polynôme annulateur avec terme constant non nul
2. si $P(X) = b_s X^s + b_{s-1}X^{s-1} + \cdots + b_1 X + b_0$ est un tel polynôme annulateur, alors l'inverse A^{-1} de A est donné par
$$A^{-1} = -\frac{1}{b_0}\left(b_s A^{s-1} + b_{s-1}A^{s-2} + \cdots + b_1 I_n\right)$$

En pratique, plutôt que de retenir la formule, il vaut mieux savoir dérouler la méthode sur chaque cas particulier, car c'est à la fois plus simple et plus formateur.

Exemple .
Supposons que, pour une certaine matrice A, l'on ait établi par le calcul que $A^3 - 7A^2 + 3A + 2I_n = O_n$. Alors

$$\begin{array}{rcll} A^3 - 7A^2 + 3A & = & -2I_n & \text{on isole le terme "constant"} \\ -\frac{1}{2}\left(A^3 - 7A^2 + 3A\right) & = & I_n & \text{on isole } I_n \\ \underbrace{A\left[-\frac{1}{2}\left(A^2 - 7A + 3I_n\right)\right]}_{A^{-1}} & = & I_n & \text{on factorise par } A \text{ à gauche et on identifie} \end{array}$$

L'enjeu de la méthode est donc de trouver un polynôme annulateur, ce qui n'est pas facile *a priori*. En réalité, c'est un peu un faux problème car le *théorème de Cayley-Hamilton* stipule que le polynôme caractéristique $\chi_A(X) = \det(A - XI_n)$ est un polynôme annulateur particulier. Il suffit donc de calculer ce polynôme caractéristique, ce qui, dans le faits, consiste à calculer le déterminant d'une matrice dont les éléments dépendent d'une indéterminée X. L'algorithme du pivot de Gauss n'est pas le plus efficace dans ce cas, on préfèrera un calcul par développement ligne ou colonne.

Par la comatrice

Pour rappel, $A_{\neq i,\neq j}$ désigne le mineur $(n-1)\times(n-1)$ obtenu à partir de A en barrant la ligne i et la colonne j. Ce mineur intervient dans le calcul du déterminant par la méthode du développement ligne ou colonne.

Définition

On appelle *comatrice* de A, notée $\mathrm{com}(A)$ la matrice définie par

$$\mathrm{com}(A) = \left[(-1)^{i+j}A_{\neq i,\neq j}\right] = \begin{bmatrix} A_{\neq 1,\neq 1} & -A_{\neq 1,\neq 1} & \dots & (-1)^{1+n}A_{\neq 1,\neq n} \\ -A_{\neq 2,\neq 1} & A_{\neq 2,\neq 2} & \dots & (-1)^{2+n}A_{\neq 2,\neq n} \\ \vdots & & \ddots & \vdots \\ (-1)^{n+1}A_{\neq n,\neq 1} & (-1)^{n+2}A_{\neq n,\neq 2} & \dots & A_{\neq n,\neq n} \end{bmatrix}$$

Le terme général $(-1)^{i+j}A_{\neq i,\neq j}$ est appelé le *cofacteur* d'indices (i,j).

Visuellement, la comatrice s'obtient à partir de A,

1. en remplaçant chaque coefficient $a_{i,j}$ par le mineur $A_{\neq i,\neq j}$,
2. en affublant chaque coefficient par un signe alternant tel un échiquier en partant de "+" en haut à gauche

Nous avons alors le :

Théorème Déterminant et comatrice

1. Pour toute matrice $A \in M_n(K)$, on a $A\ [{}^t(\mathrm{com}(A))] = [{}^t(\mathrm{com}(A))]A = (\det(A))I_n$
2. en conséquence, si A est inversible, $A^{-1} = \dfrac{1}{\det(A)}[{}^t\mathrm{com}(A)]$

Cette méthode nécessite le calcul des n^2 déterminants mineurs et du déterminant de A. Il est préférable de calculer d'abord le déterminant de A, car si celui-ci est nul on s'économise le calcul (devenu inutile) de tous les déterminants mineurs. En pratique, au papier-crayon, cette méthode est triviale pour $n = 2$ (car les mineurs sont réduits à un coefficient), inefficace et déconseillée pour $n \geq 4$. Pour $n = 3$, c'est un peu au choix de chacun...

Gauss encore

On va utiliser de façon opportune la panoplie constituée de la réduction de Gauss, des formes échelonnées/ triangulaires/ diagonales des matrices. Pour toute matrice A (pas forcément carrée) on appelle matrice *augmentée en ligne* (ou plus simplement *augmentée*) toute matrice $[A|B]$ où B a un gabarit compatible. Le résultat central de la section est le

Théorème Inverse et pivot de Gauss

Soit $A \in M_n(K)$. A est inversible si et seulement si la matrice augmentée $[A|I_n]$ admet pour forme échelonnée réduite une matrice de la forme $[I_n|A']$. Dans ce cas, $A^{-1} = A'$.

La méthode s'en déduit immédiatement. On applique la réduction de Gauss (version native cette fois, et pas la version légère) à la matrice augmentée en visant de faire apparaitre l'identité sur la partie gauche. Si on n'y arrive pas, c'est le signe que A n'est pas inversible. Si on y arrive, la partie droite fournit "sur un plateau" l'inverse recherché.

4.6 Rang

Théorème-Définition

Soit $A \in M_{n,p}(K)$. Les entiers suivants sont égaux

1. la dimension du sous-espace vectoriel de K^n engendré par les p vecteurs colonnes de A
2. la dimension du sous-espace vectoriel de K^p engendré par les n vecteurs lignes de A
3. la taille r maximale pour laquelle il existe une sous-matrice $r \times r$ inversible

L'entier r est appelé le rang de la matrice A, et noté $\text{rg}(A)$. Il est $\leq \min(n,p)$.

Propriétés Rang et lois de composition

1. $\text{rg}(A) = \text{rg}({}^tA)$
2. $\text{rg}(O_{n,p}) = 0$. Réciproquement, $\text{rg}(A) \geq 1$ si $A \neq O_{n,p}$
3. $\text{rg}(\lambda A) = \text{rg}(A)$ pour $\lambda \neq 0$
4. $\text{rg}(A+B) \leq \text{rg}(A) + rg(B)$
5. $\text{rg}(AB) \leq \min(\text{rg}(A), \text{rg}(B))$

Théorème Lien entre rang et inversibilité

Pour A carrée $n \times n$, $\text{rg}(A) = n \iff A$ est inversible.

4.6.1 Calcul du rang

Propriétés

1. Si A contient une colonne (resp. ligne) nulle, le rang de la sous-matrice de A obtenue en barrant cette colonne (resp. ligne) nulle est inchangé.
2. le rang est inchangé par échange de deux colonnes (resp. lignes)
3. le rang est inchangé si on ajoute à une colonne (resp. lignes) une combinaison linéaire des autres colonnes (resp. lignes)
4. le rang est inchangé si on multiplie une colonne (resp. ligne) par un scalaire non nul
5. le rang d'une matrice échelonnée est égal au nombre de pivots

Corollaire Rang et forme échelonnée

Le rang de toute matrice est égal au rang (donc au nombre de pivots) de n'importe laquelle de ses formes échelonnées.

Ce corollaire fournit naturellement l'algorithme de calcul du rang par pivot de Gauss. À noter qu'il n'est pas nécessaire d'atteindre la forme échelonnée réduite, mais une forme échelonnée, de sorte que la version légère de la réduction de Gauss est suffisante.

4.7 Résolution de système linéaire

On appelle système linéaire de n équations à p inconnues un système de la forme

$$\left\{\begin{array}{rcl} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,p}x_p &=& b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,p}x_p &=& b_2 \\ & \cdots & \\ a_{n,1}x_1 + a_{n,2}x_2 + \cdots + a_{n,p}x_p &=& b_n \end{array}\right.$$

Les $a_{i,j}$ sont les *coefficients du système*, les b_i sont les *seconds membres*. On appelle cette écriture la représentation naturelle du système.

4.7.1 Représentation matricielle

Un tel système admet la représentation matricielle

$$\underbrace{\begin{bmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,p} \\ a_{2,1} & a_{2,2} & \dots & a_{2,p} \\ \dots & & & \\ a_{n,1} & a_{n,2} & \dots & a_{n,p} \end{bmatrix}}_{A} \underbrace{\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_p \end{bmatrix}}_{X} = \underbrace{\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}}_{B}$$

La matrice $A \in M_{n,p}(K)$ est la *matrice du système*, le vecteur colonne $X \in M_{p,1}(K)$ est le *vecteur inconnu* et le vecteur colonne $B \in M_{n,1}(K)$ est le *vecteur second membre*.

La représentation matricielle compacte du système est la matrice augmentée

$$[A|B] = \left[\begin{array}{cccc|c} a_{1,1} & a_{1,2} & \dots & a_{1,p} & b_1 \\ a_{2,1} & a_{2,2} & \dots & a_{2,p} & b_2 \\ \vdots & & & & \vdots \\ a_{n,1} & a_{n,2} & \dots & a_{n,p} & b_n \end{array}\right]$$

Dans cette matrice augmentée, une ligne symbolise une équation. Il ne faut jamais oublier cette réalité car la difficulté de cette écriture et des méthodes qui l'utilisent est que les inconnues n'apparaissent plus explicitement. Il est conseillé de s'entrainer à passer couramment de l'écriture matricielle compacte à l'écriture naturelle (où les inconnues sont explicites) au moins dans un premier temps.

4.7.2 Existence et nombre de solutions

Ce sont les valeurs des rangs de la matrice du système et de la matrice augmentée qui permettent de statuer.

Théorème (Fontené-Rouché)

On se trouve toujours dans une (et une seule) des 3 situations suivantes :

1. Si $\text{rg}([A|B]) > \text{rg}(A)$ le système n'admet aucune solution
2. Si $\text{rg}([A|B]) = \text{rg}(A) = p$, le système admet une unique solution,
3. Si $\text{rg}([A|B]) = \text{rg}(A) < p$, le système admet une infinité de solutions

Remarque

On a en fait $\text{rg}([A|B]) = \text{rg}(A)$ ou $\text{rg}(A)+1$: mais cette précision, non mentionnée dans le théorème, est inutile, si ce n'est comme critère de vérification des calculs de rang.

4.7.3 Méthode de substitution

Elle travaille sur la représentation naturelle du système. Elle consiste à exprimer la variable x_1 en fonction de $x_2, \dots, x_p$ en utilisant l'une des équations, et à reporter dans toutes les autres. En isolant en tête l'équation exprimant x_1 en fonction des autres, on obtient ensuite un système de $n-1$ équations à $p-1$ équations sur lequel on itère le procédé, jusqu'à obtenir une équation comportant la seule variable x_p,

que l'on résout immédiatement. Puis on "remonte" de proche en proche pour déterminer successivement x_{p-1}, $x_{p-2}, \ldots, x_2, x_1$.
À noter qu'il n'est pas nécessaire de conserver l'ordre des variables, l'essentiel est d'en éliminer une à chaque étape de la substitution et de garder la trace de toutes les dépendances en réécrivant le système en entier à chaque étape.

Plusieurs cas peuvent se produire :

1. si les substitutions successives se passent bien et que la dernière équation ne fait intervenir que x_p, il y a une unique solution. Cela se produit lorsque $n = p$. Le système est dit de Cramer.
2. si les substitutions se passent bien et que l'on tombe sur une ou plusieurs équations ne comportant plus aucune variable, alors ces équations sans variables sont de la forme "$0 = 0$" ou "$0 = \blacksquare$". Dans le premier cas, l'équation est vraie : on la retire du système et on continue la résolution. Dans le second cas, elle est fausse : elle signe l'incompatibilité du système et donc l'absence de solutions.
3. si les substitutions ne parviennent pas à éliminer toutes les variables, la dernière équation enrôle au moins deux variables et a une infinité de solutions. Par ricochet, le système tout entier a lui même une infinité de solutions.

4.7.4 Gauss toujours

La représentation matricielle et la réduction de Gauss proposent une autre méthode de résolution.

Tout d'abord, on constate que toute opération élémentaire sur la matrice augmentée correspond à une manipulation équivalente sur les équations du système :

— $L_i \leftrightarrow L_j$ revient à échanger les équations i et j
— $L_i \leftarrow \alpha L_i,\ \alpha \neq 0$ revient à multiplier l'équation i pqr $\alpha \neq 0$
— $L_i \leftarrow L_i + \lambda L_j$ revient à ajouter λ fois l'équation j à l'équation i

Les trois types d'opérations sur les lignes correspondent donc à des opérations sur le système d'équations qui laissent inchangées l'ensemble solution.

La stratégie est d'appliquer la réduction de Gauss à la matrice augmentée jusqu'à une forme échelonnée/triangulaire/diagon
Il faut bien garder en tête que la matrice augmentée (modifiée à chaque étape) est la représentation symbolique d'un nouveau système d'équations équivalent au système initial, donc ayant les mêmes solutions. À ce titre, il est parfaitement licite, à tout moment, de revenir à la représentation naturelle du système si on le souhaite.

Au cours de la réduction de Gauss, l'apparition éventuelle de l'une des situations suivantes nécessite un traitement particulier :

— si la ligne $[0 \ldots 0|0]$ apparait, cette ligne peut être retirée de la matrice et le système ainsi réduit est équivalent au précédent : on continue donc la résolution
— si la ligne $[0 \ldots 0|\blacksquare]$ apparait, alors cette ligne matérialise l'incompatibilité du système qui n'a pas de solutions

4.7.5 Cas des systèmes carrés inversibles

Méthode matricielle

Lorsqu'il y a autant d'équations que d'inconnues, on peut avantageusement raisonner directement sur la forme matricielle. En effet, la matrice A est carrée et, si elle a le bon goût d'être inversible, on a

$$AX = B \iff X = A^{-1}B$$

c'est-à-dire que le système admet une unique solution et que celle-ci est donnée par les coordonnées du vecteur colonne $A^{-1}B$. La résolution consiste donc à calculer la matrice inverse A^{-1} puis effectuer le produit matrice-vecteur $A^{-1}B$. À noter que la condition A inversible est une condition **suffisante** à l'existence et unicité de la solution.

Gauss...

La réduction de Gauss, méthode générale, s'applique en particulier ici. Du fait que A est carrée inversible, la forme échelon réduite de $[A|B]$ sera forcément de la forme $[I_n|B']$ pour un certain vecteur colonne B'. Alors B' est l'unique solution du système, donc égal à $A^{-1}B$. Un point remarquable de la méthode est qu'elle calcule la solution $A^{-1}B$ sans isoler spécifiquement et explicitement le calcul de A^{-1}. .

Méthode de Cramer

Une méthode alternative, due à Cramer, fournit des formules explicites pour chacune des variables, pourvu que le système soit *de Cramer*, c'est-à-dire que A soit inversible. Le préalable est donc de calculer $\det(A)$. Cela peut paraitre coûteux mais cet effort de calcul n'est pas "perdu" car $\det(A)$ apparait explicitement dans les formules donnant la solution.

Théorème Formules de Cramer

Dans le cas d'un système carré inversible, dit *de Cramer*, l'unique solution est donnée par les *formules de Cramer* :

$$x_1 = \frac{\det(A_1^*)}{\det(A)}, \ldots, x_n = \frac{\det(A_n^*)}{\det(A)}$$

Les matrices A_j^*, pour $j = 1, \ldots, n$, sont les *matrices déduites*, obtenues par définition à partir de A en remplaçant la colonne j par le vecteur colonne second membre B.

En terme de temps de calcul, la compacité des formules de Cramer donne une apparence d'efficacité un peu fallacieuse. En effet, le calcul des déterminants $n \times n$ qui interviennent est loin d'être anodin en pratique. Le recours à cette méthode est déconseillé pour $n \geq 4$ par rapport à celle du pivot de Gauss pour des systèmes purement numériques. En revanche, les formules de Cramer trouvent une utilité spécifique dans le cas où les coefficients du système ne sont pas purement numériques mais paramétriques. En effet, dans ce dernier cas, la méthode de Gauss est connue pour ne plus forcément être la plus efficace.

4.7.6 Systèmes rectangulaires

Le cas des systèmes de Cramer est sympathique parce qu'il y a autant d'équations que d'inconnues, et que les équations sont *linéairement indépendantes* entre elles, c'est-à-dire qu'aucune ne s'obtient par combinaisons linéaires des autres. L'exemple suivant n'est pas de Cramer, car la troisième équation est en fait la somme des deux premières :

$$(\mathcal{S}) \begin{cases} x + 2y - 5z &= 1 \\ 2x - 3y + 4z &= 3 \\ 3x - y - z &= 4 \end{cases}$$

On peut retirer cette troisième équation car elle n'apporte aucune contrainte supplémentaire par rapport aux deux précédentes : elle est en quelque sorte "redondante". Le système $\mathcal{S}$ est alors équivalent au système réduit

$$(\mathcal{S}') \begin{cases} x + 2y - 5z &= 1 \\ 2x - 3y + 4z &= 3 \end{cases}$$

c'est-à-dire (point fondamental) a le même ensemble solution.

Concrètement, il n' y a pas à s'inquiéter *a priori* de la détection d'équations linéairement dépendantes des autres. Le phénomène apparaitra naturellement lors de la résolution (que ce soit par substitution ou par Gauss) sous la forme des "équations sans variables" $0 = 0$ ou $0 = \blacksquare$ et nous avons vu plus haut quelle procédure appliquer. La proposition récapitule les divers cas.

Proposition

1. Si les dépendances entre équations se sont manifestées par une ou plusieurs équations $0 = \blacksquare$, le système initial est incompatible. On arrête la résolution et l'ensemble solution est vide
2. Si les dépendances entre équations ne se sont manifestées que par des équations "0=0", alors
   — le système initial est compatible

— l'élimination des équations $0 = 0$ conduit à un système équivalent (donc ayant le même ensemble solution) comportant $n' \leq p$ équations indépendantes.

Dans ce cas, de deux choses l'une

(a) si $n' = p$, le système réduit est de Cramer

(b) si $n' < p$, le système réduit a une infinité de solutions ; l'ensemble solution peut être exprimé sous forme paramétrique ; on applique la *méthode des inconnues principales*

4.7.7 Méthode des inconnues principales

Soit un système de n équations **indépendantes** à p inconnues avec $n < p$. Le système est soit nativement de cette forme, soit obtenu par la réduction de la proposition précédente. Alors le système admet des (en fait une infinité de) solutions.

Définition

On appelle *ensemble d'inconnues principales* $\{x_{j_1}, \ldots, x_{j_n}\}$ tout sous-ensemble de n inconnues d'indices $j_1, \ldots, j_n$ telle que la matrice (carrée) extraite $A_{\{1,\ldots,n\},\{j_1,\ldots,j_n\}}$ est inversible.

Il peut y avoir plusieurs ensembles d'inconnues principales. De plus la recherche d'un ensemble particulier d'inconnues principales nécessite des calculs un peu longs si l'on teste l'inversibilité de matrices extraites. Heureusement, la méthode du pivot de Gauss fournit là encore un moyen efficace et systématique.

Proposition Obtention des inconnues principales

On suppose que la matrice du système (donc la matrice augmentée) a été mise sous forme échelon, et que les équations de compatibilité sont vérifiées. Alors un choix d'inconnues principales est de prendre les inconnues correspondant aux colonnes contenant les pivots. Les inconnues non principales correspondent aux colonnes ne contenant pas de pivot.

On est désormais prêts à résoudre le système

Méthode Résolution du système

1: Choisir un ensemble de n inconnues principales $\{x_{j_1}, \ldots, x_{j_n}\}$
2: Considérer les $(p - n)$ inconnues non principales $\{x_{k_1}, \ldots, x_{k_{p-n}}\}$ comme des paramètres et plus comme des inconnues // C'est là le point crucial
3: Faire passer les inconnues non principales dans les seconds membres
4: Résoudre le système (de Cramer) d'inconnues les inconnues principales $\{x_{j_1}, \ldots, x_{j_n}\}$

On obtient pour l'ensemble solution un ensemble paramétré par les inconnues non principales, donc infini. Plus précisément, c'est un sous-espace affine de dimension $p - n$.

Exemple

Reprenons le système

$$(\mathcal{S}) \begin{cases} x + 2y - 5z &= 1 \\ 2x - 3y + 4z &= 3 \\ 3x - y - z &= 4 \end{cases}$$

On écrit sous forme matricielle, on applique la réduction de Gauss et on obtient la forme échelon réduite

$$\left[\begin{array}{ccc|c} 1 & 2 & -5 & 1 \\ 2 & -3 & 4 & 3 \\ 3 & -1 & -1 & 4 \end{array}\right] \longrightarrow \ldots \longrightarrow \left[\begin{array}{ccc|c} 1 & 0 & -1 & 9/7 \\ 0 & 1 & -2 & -1/7 \\ 0 & 0 & 0 & 0 \end{array}\right] \longrightarrow \left[\begin{array}{ccc|c} 1 & 0 & -1 & 9/7 \\ 0 & 1 & -2 & -1/7 \end{array}\right]$$

d'où on déduit le système réduit

$$(\mathcal{S}') \begin{cases} x - z &= 9/7 \\ y - 2z &= -1/7 \end{cases}$$

On prend comme inconnues principales x, y, puisqu'elles correspondent aux colonnes 1 et 2 contenant les pivots. Ainsi z est inconnue non principale, donc est désormais considéré comme un paramètre et rejoint

les seconds membres

$$(\mathcal{S}')\left\{\begin{array}{lcl} x & = & z+9/7 \\ y & = & 2z-1/7 \end{array}\right.$$

On déduit finalement l'ensemble solutions :

$$\left\{\begin{pmatrix} z+9/7 \\ 2z-1/7 \\ z \end{pmatrix} : z\in\mathbb{R}\right\} = \left\{\begin{pmatrix} 9/7 \\ -1/7 \\ 0 \end{pmatrix} + z\begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix} : z\in\mathbb{R}\right\}$$

C'est le sous-espace affine passant par le point $(9/7, 1/7, 0)$ et de vecteur directeur $(1, 2, 1)$. Il est ici paramétré par l'inconnue non principale z.

Chapitre 5

Processus stochastiques

5.1 Introduction

En mathématiques, et plus particulièrement en théorie des probabilités, un *processus stochastique* ou *processus aléatoire*, est un objet qui caractérise l'évolution dans le temps d'une phénomène aléatoire, et par ricochet, d'une variable aléatoire.

Définition

Un processus stochastique est une famille $(X_t)_{t\in T}$ de variables aléatoires définies sur un même espace probabilisé. Cette famille est indexée par un paramètre t représentant le temps. Les valeurs prises par les variables aléatoires s'appellent les états du processus.

5.1.1 Discret ou continu

Un processus peut être à temps discret ou continu. Dans le premier cas on s'intéresse à l'évolution temporelle selon des "photographies instantanées" prises à intervalle régulier. La modélisation mathématique typique est de prendre pour T un espace infini dénombrable discret, comme l'ensemble des entiers naturels $\mathbb{N}$, dans lequel le "0" joue le rôle de début du processus. Dans le second cas, on s'intéresse à l'évolution permanente, et T est alors un espace infini non dénombrable "continu", typiquement $\mathbb{R}_+$, où là encore le "0" est le début du processus.

De la même manière l'espace des états peut lui-même être discret ou continu, directement hérité de l'esapce dans lequel les variables aléatoires du processus prennent leur valeur : $\mathbb{N}, \mathbb{Z}$ dans le cas discret, $\mathbb{R}$ dans le cas continu.

Considérons l'exemple de relevés météorologiques de températures. Le temps discret consiste à mesurer et collecter la température à certains instants ponctuels, par exemple toutes les heures, l'agrégation fournissant un nuage de points régulièrement séparées, alors que pour le temps continu, le thermomètre reste actif en permanence et l'agrégation des données est une courbe continue.
Un espace d'états discret correspondrait à des valeurs de températures arrondies à l'entier le plus proche. Un espace d'états continu, au contraire, signifierait de conserver la valeur exacte des températures mesurées (le thermomètre étant supposé idéal et avoir une précision de mesure infinie).

5.1.2 Processus de Markov

Intuitivement, un processus est dit *de Markov* quand son évolution future ne dépend que de l'état présent, indépendamment du passé qui y a conduit. La propriété de Markov s'énonce formellement en utilisant les probabilités conditionnelles.

Dans le cadre de ce cours, nous verrons seulement deux types de processus :

- les processus de Markov à temps discret et à espace d'états fini
- les processus de Markov à temps continu et à espace d'états discret

si bien que nous énonçons la propriété de Markov dans le cas, un peu plus facile à formuler, d'un espace d'états discret.

Propriété de Markov Espace d'états discret

1. à temps discret :

$$\forall t \geq 0, \quad \mathbb{P}(X_{t+1} = x | X_t, X_{t-1}, \ldots, X_0) = \mathbb{P}(X_{t+1} = x | X_t)$$

2. à temps continu :

$$\forall u \geq t \geq 0, \quad \mathbb{P}(X_u = x | \{X_s\}_{0 \leq s \leq t}) = \mathbb{P}(X_u = x | X_t)$$

5.2 Processus de Markov à temps discret

Lorsque le processus de Markov est à temps discret et à espaces d'états discret, on parle de *chaine de Markov*. Comme dit ci-dessus, nous étudions seulement le cas d'espace d'états fini. Parler d'une chaine de Markov à espace d'états fini revient donc, par définition, à considérer une suite de variables aléatoires $(X_t)_{t \in \mathbb{N}}$ à valeurs dans un ensemble fini $\{s_1, \ldots, s_n\}$ que nous nous empressons d'identifier à $\{1, \ldots, n\}$ par souci de simplification d'écriture.

5.2.1 Description par probabilités d'état et de transition

À chaque variable aléatoire X_t, t étant fixé, correspond une distribution de probabilité $(\mathbb{P}(X_t = i))_{i=1,\ldots,n}$, qui très concrètement prend la forme d'un vecteur ligne, noté $\mathbf{p}^{(t)}$, dont les composantes $\in [0, 1]$ et sont de somme 1. On parle de *vecteur ligne stochastique*.

Par ailleurs, et c'est là l'essence d'un processus, on s'intéresse à l'évolution entre divers instants. Les probabilités pertinentes sont les probabilités conditionnelles qui relient le futur au présent et au passé. D'après la propriété de Markov, seules sont pertinentes celles qui relient le futur au présent.

Définition

— les $\mathbb{P}(X_t = j)$ pour $t \in \mathbb{N}$ et $j \in \{1, \ldots, n\}$ sont les *probabilités d'état*.
— les $\mathbb{P}(X_{t+1} = j | X_t = i)$ pour $t \in \mathbb{N}$ et $i, j \in \{1, \ldots, n\}$ sont les *probabilités de transition*.

Lorsque les probabilités de transition ne dépendent pas du temps, la chaine de Markov est dite *homogène*. C'est une situation plutôt fréquente, que nous supposerons dorénavant.

5.2.2 Matrice et graphe de transition

Les probabilités de transition peuvent être présentées sont forme d'une matrice carrée notée $\mathbf{P}$. Comme la chaine est homogène, cette matrice ne dépend pas du temps. Le passage de l'instant t à l'instant $t+1$ se lit dans le sens "ligne vers colonne", à savoir : la probabilité de passer de l'état i (indice de ligne) à l'état j (indice de colonne) entre les instants t et $t+1$ est $\mathbf{P}_{i,j}$. La matrice dépend *a priori* du temps dans le cas général, mais pour nous n'en dépend puisque la chaîne est supposée homogène.

La formule des probabilités totales pour l'événement $\{X_{t+1} = j\}$ par rapport aux événements $\{X_t = i\}$ donne :

$$\mathbb{P}(X_{t+1} = j) = \sum_{i=1}^{n} \mathbb{P}(X_t = i)\ \mathbb{P}(X_{t+1} = j | X_t = i)$$

Nous la traduisons immédiatement par

$$\mathbf{p}_j^{(t+1)} = \sum_{i=1}^{n} \mathbf{p}_i^{(t)}\ \mathbf{P}_{i,j}$$

et nous reconnaissons le produit vecteur (ligne)-matrice : $\mathbf{p}^{(t+1)} = \mathbf{p}^{(t)}\ \mathbf{P}$. Nous voici prêts à synthétiser

Théorème-Définition Matrice de transition d'une chaîne de Markov homogène

1. La matrice de transition $\mathbf{P}$ est la matrice des probabilités de transition $(\mathbb{P}(X_{t+1} = j | X_t = i))_{i,j}$.

2. C'est une matrice stochastique (en ligne), c'est-à-dire que ses coefficients $\in [0,1]$ et que les sommes en ligne sont égales à 1.
3. Les vecteurs lignes stochastiques $\mathbf{p}^{(t)}$ vérifient

$$\forall t \geq 0,\ \mathbf{p}^{(t+1)} = \mathbf{p}^{(t)}\ \mathbf{P},\ \ \Leftrightarrow\ \ \forall t \geq 0,\ \mathbf{p}^{(t)} = \mathbf{p}^{(0)}\mathbf{P}^t$$

Remarques .

1. Le produit de deux matrices stochastiques (resp. toute puissance d'une matrice stochastique) est encore une matrice stochastique
2. Si $\mathbf{x}$ est un vecteur ligne stochastique et $\mathbf{P}$ est une matrice stochastique, alors le vecteur ligne $\mathbf{xP}$ est encore stochastique.
3. La tradition dans ce contexte est de représenter les vecteurs en ligne, ce qui amène à manipuler des produits "vecteur (ligne) - matrice". Cette tradition est contraire à l'usage courant en algèbre linéaire où les vecteurs sont représentés par des matrices unicolonnes et où on manipule plutôt des produits "matrice-vecteur (colonne)"
4. une matrice stochastique est un cas particulier de *matrice positive*, ce qui nous amène à une petite parenthèse de vocabulaire et deux définitions élémentaires :
   Définition
   Une matrice $\mathbf{A}$ est *positive* (resp. *strictement positive*) si tous ses coefficients sont positifs (resp. strictement positifs), et on écrit $\mathbf{A} \geq 0$ (resp. $\mathbf{A} > 0$).
   Remarque Pour une matrice, "strictement positive" n'est pas synonyme de "positive différente de la matrice nulle" (sauf dans le cas $n = 1$).
   On définit de manière analogue les vecteurs positifs et strictement positifs.

Définition Graphe d'une chaîne de Markov

Le graphe (orienté) d'une chaîne de Markov homogène est défini par :

— n sommets représentant les états

— des arcs orientés caractérisés par : l'arc orienté de i vers j existe si et seulement si la transition de i à j est possible, c'est-à-dire si $\mathbf{P}_{i,j} > 0$. Cette dernière probabilité est alors le label de l'arc $\overrightarrow{ij}$.

Vocabulaire . Puisque l'évolution une chaîne de Markov (homogène) est indifféremment caractérisée par sa matrice de transition (constante dans le temps) et/ou son graphe, tout adjectif qui qualifie la chaîne qualifie par extension la matrice et le graphe.

Le lien entre le graphe et la matrice de transition recèle un lemme aussi simple qu'utile. Pour tout $k \geq 1$, un chemin (orienté) de longueur k, ou k-chemin allant de i à j est un chemin comportant k arcs, donc passant par $k-1$ sommets intermédiaires.

Lemme

Soit k un entier ≥ 1, et $1 \leq i, j \leq n$

1. Il existe un k-chemin de i vers $j \Leftrightarrow\ (\mathbf{P}^k)_{i,j} > 0$
2. Il existe un chemin de longueur au plus k de i vers $j \Leftrightarrow\ ((\mathbf{I_n} + \mathbf{P})^k)_{i,j} > 0$

5.2.3 Classification des états

On suppose toujours que la chaîne de Markov est homogène à espace d'états fini.

Proposition-Définition Relation de communication

1. On dit que l'état j est *accessible* depuis l'état i, et on note $\{i \to j\}$ ou $\{j \leftarrow i\}$ si $i = j$ ou s'il existe un chemin allant de i à j.

2. On dit que i et j sont *communicants* (ou *communiquent*), et on note $\{i \leftrightarrow j\}$ si $i = j$ ou si $\{j$ est accessible depuis i et i est accessible depuis $j\}$.
3. la relation "communiquer" est une relation d'équivalence dont les classes d'équivalences sont les *classes de communication.*

Propriétés Nature des classes de communication

1. une classe est dite *récurrente* ou *finale* s'il est impossible d'en sortir une fois qu'on y est entré
2. une classe est dite *transitoire* s'il est possible d'en sortir mais dans ce cas il est impossible d'y revenir
3. une classe C' est *accessible* depuis une autre classe C, et on note $C' \leftarrow C$ si et seulement si
$$\exists i \in C,\ \exists j \in C'\ \{j \leftarrow i\} \iff \forall i \in C,\ \forall j \in C'\ \{j \leftarrow i\}$$
4. la chaîne est dite *irréductible* lorsqu'il existe une seule classe de communication (alors nécessairement récurrente). Sinon, la chaîne est dite *réductible.*

Un état est dit récurrent (resp. transitoire) s'il appartient à une classe récurrente (resp. transitoire).

Voici maintenant une notion qui interviendra dans l'étude du comportement asymptotique.

Définition Période d'un état

1. La *période* de l'état i est définie par l'un ou l'autre des énoncés suivants :
   (a) le PGCD des longueurs des chemins allant de i à i, s'il en existe. Sinon, elle est nulle par convention
   (b) l'entier PGCD$\{t \in \mathbb{N} :\ (\mathbf{P}^t)_{i,i} > 0\}$
2. un état de période 1 est dit *apériodique*
3. la chaîne est dite apériodique si tous les états sont apériodiques

Il est facile (mais pas évident !) de vérifier que tous les éléments d'une même classe de communication ont la même période. Si celle-ci est égale à 1, on parlera naturellement de *classe apériodique*

Voici enfin des critères utiles pour statuer sur l'irréductibilité et sur l'apériodicité d'une chaîne de Markov. Pour l'irréductibilité, l'un n'est pas de manière flagrante la négation de l'autre : il est donc judicieux de les avoir tous les deux à l'esprit.

Propriété Critère d'irréductibilité

Se valent :

1. $\mathbf{P}$ est irréductible
2. il existe $k \in \{1, \ldots, n-1\}$ tel que $(\mathbf{I_n} + \mathbf{P})^k > 0$
3. $(\mathbf{I_n} + \mathbf{P})^{n-1} > 0$

Propriété Critère de réductibilité

Se valent :

1. $\mathbf{P}$ est réductible
2. il existe une renumérotation des états tels que la (nouvelle) matrice de transition soit de forme triangulaire par blocs :
$$\mathbf{P}' = \left[\begin{array}{c|c} \mathbf{A}_{r\times r} & \mathbf{O}_{r\times(n-r)} \\ \hline \mathbf{B}_{(n-r)\times r} & \mathbf{C}_{(n-r)\times(n-r)} \end{array}\right]$$

Concrètement, cela signifie que l'on peut renuméroter les états et créer deux sous-ensembles $E_1 =$

$\{1,\ldots,r\}$ et $E_2 = \{r+1,\ldots,n\}$ de sorte que les états de E_1 ne peuvent jamais atteindre les états de E_2. En revanche, les états de E_2 peuvent *a priori* atteindre ceux de E_1 : lorsque tel n'est pas le cas, on a $\mathbf{B} = \mathbf{O}_{(n-r)\times r}$.

Propriété Conditions suffisantes d'apériodicité

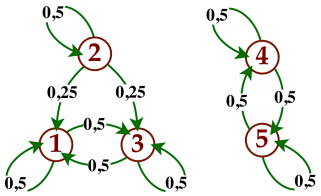
Une (matrice de transition de) chaîne de Markov est apériodique dans le cas suivants :

1. la diagonale est > 0
2. la diagonale contient au moins un élément > 0 et la chaîne est irréductible
3. la diagonale contient au moins un élément > 0 dans chaque classe de communication

5.2.4 Exemple

Considérons la chaîne de Markov à 5 états dont la matrice de transition et le graphe sont donnés par

$$P = \begin{pmatrix} 1/2 & 0 & 1/2 & 0 & 0 \\ 1/4 & 1/2 & 1/4 & 0 & 0 \\ 1/2 & 0 & 1/2 & 0 & 0 \\ 0 & 0 & 0 & 1/2 & 1/2 \\ 0 & 0 & 0 & 1/2 & 1/2 \end{pmatrix}$$



Source :Wikipedia

— Les classes de communication sont {2}, {1,3} et {4,5}. Contrairement à ce que l'on pourrait conclure par une lecture (trop) rapide du graphe , 2 ne communique ni avec 1 ni avec 3 : s'il est vrai que 1 et 3 sont accessibles depuis 2, en revanche 2 n'est accessible ni depuis 1, ni depuis 3.

— La classe {2} est transitoire, les classes {1,3} et {4,5} sont récurrentes.

— La chaîne de Markov n'est pas irréductible. Elle peut clairement être réduites en deux sous-chaînes {1,2,3} et {4,5}, qui sont totalement déconnectées. Le critère sur la forme de la matrice nous permettait d'ailleurs aussi de conclure puisque dans cet exemple, $\mathbf{P}$ est diagonale par blocs.

— La sous-chaîne composée des états {4,5} est irréductible. C'est immédiat sur le graphe mais on peut remarquer que le critère matriciel s'applique :

$$\left(\mathbf{I_2} + \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}\right)^1 = \begin{bmatrix} 3/2 & 1/2 \\ 1/2 & 3/2 \end{bmatrix} > 0$$

— La sous-chaîne composée des états {1,2,3} est réductible. En renumérotant en {1,3,2}, la sous-matrice de transition est

$$\begin{bmatrix} 1/2 & 1/2 & 0 \\ 1/2 & 1/2 & 0 \\ 1/4 & 1/4 & 1/2 \end{bmatrix}$$

qui est bien triangulaire par blocs.

— les états ont tous pour période 1 : en effet pour chaque sommet, il y a une arête (un 1-chemin) sur lui-même, a fortiori, le PGCD est égal à 1. Le critère matriciel (diagonale strictement positive) est là encore une alternative.

5.2.5 Comportement asymptotique

L'objet de ce paragraphe est d'étudier la limite si elle existe de la distribution de probabilités $\mathbf{p}^{(t)}$ lorsque $t \to +\infty$. Nous avons besoin de quelques définitions et de résultats complémentaires avant de donner les théorèmes principaux de convergence.

Théorème-Définition Vecteur stationnaire

1. Un vecteur ligne stochastique est dit *stationnaire* pour la chaîne s'il vérifie $\mathbf{xP} = \mathbf{x}$.
2. Toute matrice stochastique admet au moins un vecteur ligne stochastique stationnaire.

On dit que 1 est *valeur propre à gauche* de $\mathbf{P}$ et que $\mathbf{x}$ est un *vecteur propre à gauche*.

Définition Matrice primitive

Une matrice stochastique $\mathbf{P}$ (et par extension la chaîne et le graphe qu'elle définit) est dite *primitive* s'il existe k tel que $\mathbf{P}^k > 0$.

Propriétés

1. Si $k \in \mathbb{N}^*$ est tel que $\mathbf{P}^k > 0$, alors pour tout $\ell \geq k$ on a aussi $\mathbf{P}^\ell > 0$.
2. Strictement positive $\Rightarrow$ primitive $\Rightarrow$ irréductible. Réciproques fausses.
3. Primitive $\Leftrightarrow$ irréductible et apériodique

Voici maintenant les trois théorèmes de convergence, déclinés de l'hypothèse la plus forte à la moins forte

Théorème Vecteur stationnaire et convergence (cas primitif)

Si $\mathbf{P}$ est primitive (en particulier si $\mathbf{P} > 0$),

1. il existe un unique vecteur ligne stochastique stationnaire $\mathbf{p_s^+}$ pour $\mathbf{P}$, et on a $\mathbf{p_s^+} > 0$
2. la matrice $\mathbf{P}^t$ converge quand $t \to +\infty$ vers la matrice, notée $\mathbf{P}^\infty$, dont toutes les lignes sont égales au vecteur stationnaire $\mathbf{p_s^+}$
3. pour toute distribution de probabilité initiale $\mathbf{p}^{(0)}$, la suite $\mathbf{p}^{(t)}$ converge vers $\mathbf{p_s^+}$ quand $t \to +\infty$

Théorème Vecteur stationnaire et convergence (cas irréductible non primitif)

Si $\mathbf{P}$ est irréductible non primitive (ce qui équivaut à $\mathbf{P}$ irréductible non apériodique),

1. il existe un unique vecteur ligne stochastique stationnaire $\mathbf{p_s^+}$ pour $\mathbf{P}$, et on a $\mathbf{p_s^+} > 0$
2. la matrice $\mathbf{P}^t$ ne converge pas quand $t \to +\infty$
3. on ne peut rien dire *a priori* sur la convergence de $(\mathbf{p}^{(t)})$, sauf si $\mathbf{p}^{(0)} = \mathbf{p_s^+}$, auquel cas $(\mathbf{p}^{(t)})$ est constante
4. si $(\mathbf{p}^{(t)})$ converge, c'est nécessairement vers $\mathbf{p_s^+}$.

Ainsi, dans le passage de "primitif" à "irréductible", on conserve l'existence et l'unicité du vecteur stationnaire, mais on perd *a priori* les convergences.

Théorème Vecteur stationnaire et convergence (cas non irréductible)

Si $\mathbf{P}$ n'est pas irréductible,

1. il existe un ou plusieurs vecteur(s) ligne(s) stochastique(s) stationnaire(s) pour $\mathbf{P}$, et ils sont ≥ 0.
2. on ne peut rien dire *a priori* de la convergence de $\mathbf{P}^t$
3. on ne peut rien dire *a priori* sur la convergence de $(\mathbf{p}^{(t)})$, sauf si $\mathbf{p}^{(0)}$ est un vecteur stationnaire, auquel cas $(\mathbf{p}^{(t)})$ est constante
4. si $(\mathbf{p}^{(t)})$ converge, c'est nécessairement vers un vecteur stationnaire.

Ainsi dans le passage d' "irréductible" à "non irréductible", on perd en plus a priori l'unicité et le stricte positivité du vecteur stationnaire (mais on conserve l'existence et la positivité)

Un petit tableau nous récapitule tout cela

	Primitif	Irréductible non primitif	Non irréductible
Vecteur stationnaire			
Existence	oui > 0	oui > 0	oui ≥ 0
Unicité	oui	oui	non
Convergence			
de $\mathbf{P}^t$	oui	non	?
de $\mathbf{p}^{(t)}$	oui	?	?

5.3 Processus de Markov à temps continu

5.3.1 Introduction

Un processus de Markov à temps continu est la donnée d'une famille de variables aléatoires $(X_t)_t$ indexées par un paramètre t réel. Comme il est d'usage qu'il y ait un début au processus, on prendra $t \in \mathbb{R}_+$. Il est caractérisé par :

1. un espace d'états $E = \{1, 2, 3, \dots\}$ au plus dénombrable, qui est l'ensemble des valeurs que peuvent prendre les variables aléatoires X_t
2. une loi de probabilité initiale sur l'ensemble des états, c'est-à-dire la loi de X_0
3. une *matrice de transition* infinitésimale $Q = (q_{i,j})_{i,j}$, de taille éventuellement infinie, où
   — pour $i \neq j$, $q_{i,j} \geq 0$ matérialise la vitesse instantanée de transition de l'état i à l'état j
   — pour $i = j$, $q_{i,i} = -\sum_{j \neq i} q_{i,j}$

   de sorte que la somme (éventuellement infinie) des éléments de chaque ligne de Q est égale à 0.

5.3.2 Deux points de vue pour un processus à temps continu

Définitions

1. Point de vue "*infinitésimal*"
   Pour tous $t, h \in \mathbb{R}_+$, la variable X_{t+h} conditionnée aux $(X_s)_{s \leq t}$ ne dépend que de X_t, et on a

$$\begin{cases} \mathbb{P}(X_{t+h} = j | X_t = i) &= q_{i,j} h + o(h) & \text{si } i \neq j \\ \mathbb{P}(X_{t+h} = i | X_t = i) &= 1 + q_{i,i} h + o(h) & \text{rappelons que } q_{i,i} \leq 0 \end{cases}$$

2. Point de vue "*équation fonctionnelle*"
   On a, pour tous $t \geq s \geq 0$,

$$\mathbb{P}(X_t = j | X_s = i) = P_{i,j}(t - s)$$

   où $P(t) = [P_{i,j}(t)]_{i,j}$ est une matrice satisfaisant l'équation différentielle de *Chapman-Kolmogorov*

$$\begin{cases} P'(t) = P(t)Q \\ P(0) = Id \end{cases}$$

L'équation de Chapman-Kolmogorov se décline en un système (éventuellement infini) d'équations différentielles portant sur les fonctions scalaires $P_{i,j}(t)$:

$$\forall i, j, \quad \begin{cases} P'_{i,j}(t) &= P_{i,1}(t)q_{1,j} + P_{i,2}(t)q_{2,j} + P_{i,3}(t)q_{3,j} + \dots \\ & \qquad \left(= \sum_k P_{i,k}(t) q_{k,j} \right) \\ P_{i,j}(0) &= \mathbf{1}(i = j) \end{cases}$$

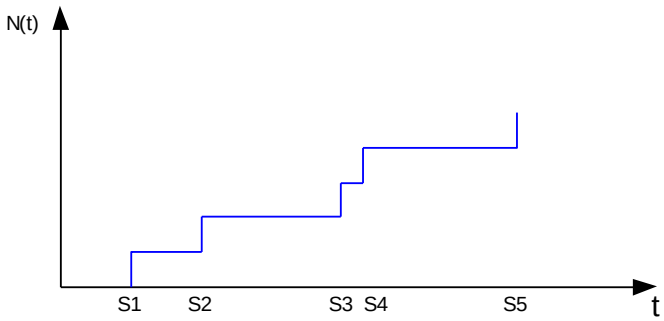
5.3.3 Processus de comptage

Un processus de comptage vise à relater l'apparition d'événements aléatoires comme des impacts de foudre, des appels téléphoniques dans un central, etc. C'est un cas particulier d'un processus de Markov pour lequel, dans la définition infinitésimale, les seules transitions possibles sont $i \to i$ et $i \to i + 1$.
Un processus de comptage présente deux points de vue complémentaires, chacun y attachant une famille de variables aléatoires.

1. On considère le nombre d'événements se produisant dans un intervalle de temps. On définit la famille de v.a. discrètes $(N_t)_{t\geq 0}$ comme le nombre d'événements s'étant produits depuis le début du processus ($t = 0$). C'est une fonction de t en escalier croissant de 1 en 1.
   On note que $N_t - N_s$ est le nombre d'événements s'étant produits dans l'intervalle $[s, t]$, pour $0 \leq s \leq t$.
2. on considère les instants où se produisent les événements, et on introduit deux suites de v.a. à densité :
   — la suite $(S_1, S_2, \dots)$ des *instants d'apparition* : S_n est l'instant d'apparition du n-ième événement.
   — la suite $(T_1, T_2, \dots)$ des *intervalles inter-événements* : T_n est l'intervalle de temps entre le $(n-1)$-ième et le n-ième événement.

   On passe des S_n aux T_n par les formules

$$S_n = T_1 + T_2 + \cdots + T_n \quad \text{pour } n \geq 1, \qquad \left\{ \begin{array}{rcll} T_1 & = & S_1 & \\ T_n & = & S_n - S_{n-1} & \text{pour } n \geq 2 \end{array} \right.$$



Processus de comptage faisant apparaitre les v.a. N_t et S_n

Les équivalences suivantes, contraposées l'une de l'autre, sont une conséquence directe des définitions et se lisent aisément sur le schéma.

$$\text{Pour } t \geq 0 \text{ et } n = 1, 2, \dots, \qquad N_t \leq n \Longleftrightarrow S_{n+1} > t, \qquad N_t > n \Longleftrightarrow S_{n+1} \leq t$$

L'intérêt de travailler avec les variables inter-événements T_n est qu'elles sont possiblement indépendantes, comme dans le cas d'un processus de Poisson que nous allons détailler ci-après. Or, la théorie des probabilités montre qu'il est plus confortable de travailler avec des v.a. indépendantes. De leur coté, les S_n, vérifiant $S_1 \leq S_2 \leq S_3 \leq \dots$, ne sont donc jamais indépendantes.

5.3.4 Processus de Poisson

Définition

Un processus est *de Poisson* s'il vérifie les trois propriétés :

1. *homogénéité* (par rapport au temps)
   la probabilité d'avoir k événements dans un intervalle ne dépend que de la longueur de l'intervalle : pour $0 \leq s \leq t$,
$$\mathbb{P}(N_t - N_s = k) = \mathbb{P}(N_{t-s} = k), \qquad // \text{ noté } p_k(t-s)$$
2. *accroissements indépendants*
   le nombre d'événements se produisant dans des intervalles disjoints sont des v.a. indépendantes : pour $0 \leq s \leq t$,
$$\begin{array}{rcl} \mathbb{P}(N_t - N_s = k, N_s = j) & = & \mathbb{P}(N_t - N_s = k)\mathbb{P}(N_s = j) \\ & & (= p_k(t-s)p_j(s) \text{ d'après la propriété 1}) \end{array}$$

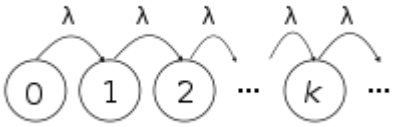
3. *rareté infinitésimale*
   il existe $\lambda > 0$, appelé intensité du processus, tel que, pour tous $t \geq 0$ et $h > 0$,

$$\mathbb{P}(N_{t+h} - N_t = k) \quad (= \mathbb{P}(N_h = k) \text{ d'après la propriété 1}) \quad = \begin{cases} 1 - \lambda h + o(h) & \text{pour } k = 0 \\ \lambda h + o(h) & \text{pour } k = 1 \\ o(h) & \text{pour } k \geq 2 \end{cases}$$

La matrice (de taille infinie) de transition infinitésimale d'un processus de comptage de Poisson est donnée par

$$\begin{bmatrix} -\lambda & \lambda & 0 & 0 & \dots \\ 0 & -\lambda & \lambda & 0 & \dots \\ 0 & 0 & -\lambda & \lambda & \dots \\ \vdots & \vdots & \vdots & \ddots & \ddots \end{bmatrix}$$

On peut comme toujours représenter le processus par un graphe, éventuellement "infini". Mais il est d'usage de ne pas faire apparaitre les transitions d'un état vers lui-même pour ne pas alourdir le dessin.



Source : Wikipedia

Le théorème suivant donne une caractérisation des processus de Poisson en fournissant les lois explicites des familles des v.a. N_t et T_n.

Théorème

Se valent :

1. le processus de comptage $(N_t)_{t\geq 0}$ est de Poisson
2. pour tout $t > 0$, la variable de comptage N_t suit une loi de Poisson de paramètre λt :

$$\mathbb{P}(N_t = k) \quad (\text{noté } p_k(t)) \quad = \frac{(\lambda t)^k}{k!} e^{-\lambda t}, \quad \text{pour } k = 0, 1, 2, \dots$$

3. les intervalles inter-événements T_n sont des v.a. à densité indépendantes de même loi exponentielle $\mathcal{E}(\lambda)$. On en rappelle la densité :

$$g_{\mathcal{E}(\lambda)}(t) = \mathbf{1}(t \geq 0) \cdot \lambda e^{-\lambda t}$$

En particulier :

— $\mathbb{E}[N_t] = \lambda t$. C'est le nombre moyen d'événements sur un intervalle de temps de longueur t.
— en faisant $t = 1$, on voit que λ est le nombre moyen d'événements par unité de temps
— $\mathbb{E}[T_n] = 1/\lambda$. C'est le temps moyen inter-événements.

5.3.5 Processus de naissance et de mort

Les processus de naissance et de mort sont un cas particulier de processus de Markov. Seules les transitions infinitésimales $i \to i$, $i \to i + 1$ (avec $i \geq 0$) et $i \to i - 1$ (avec $i \geq 1$) sont possibles.

Il est caractérisé par la donnée de deux suites réelles $(\lambda_n)_n$ et $(\mu_n)_n$ représentant *les taux instantanés de natalité et de mortalité*. On a toujours $\mu_0 = 0$.

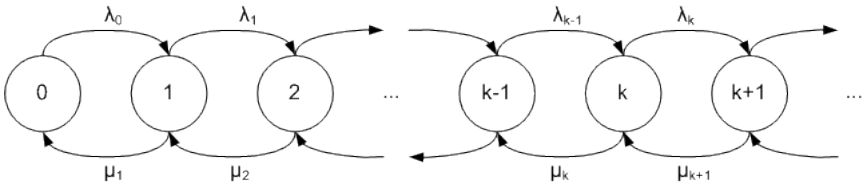
Les probabilités de transitions infinitésimales sont données par : pour $t \geq 0$ et $h > 0$,

$$\left\{\begin{array}{rcll} \mathbb{P}(X_{t+h} = i-1 | X_t = i) & = & \mu_i h + o(h) & \text{pour } i \geq 1 \\ \mathbb{P}(X_{t+h} = i | X_t = i) & = & 1 - (\lambda_i + \mu_i)h + o(h) & \text{pour } i \geq 0 \\ \mathbb{P}(X_{t+h} = i+1 | X_t = i) & = & \lambda_i h + o(h) & \text{si } i \geq 0 \\ \mathbb{P}(X_{t+h} = j | X_t = i) & = & o(h) & \text{si } |j-i| \geq 2 \end{array}\right.$$

de sorte que la matrice de transition vaut

$$Q = \begin{bmatrix} -\lambda_0 & \lambda_0 & 0 & 0 & \dots \\ \mu_1 & -(\lambda_1 + \mu_1) & \lambda_1 & 0 & \dots \\ 0 & \mu_2 & -(\lambda_2 + \mu_2) & \lambda_2 & \dots \\ \vdots & \vdots & \vdots & \ddots & \ddots \end{bmatrix}$$

Il existe là encore une représentation du processus par un graphe, analogue à celui des processus de Poisson



Source : Wikipedia

La détermination de la loi de probabilités $(\mathbb{P}(X_t = k))_{k \in \mathbb{N}}$ pour tout t demande de résoudre le système (infini) des équations différentielles de Chapman-Kolmogorov. On note

$$P(t) = (p_0(t), p_1(t), \dots) = (\mathbb{P}(X_t = 0), \mathbb{P}(X_t = 1), \dots)$$

L'équation matricielle $P'(t) = P(t)Q$ se décline en

$$\left\{\begin{array}{rcl} p_0'(t) & = & -\lambda_0 p_0(t) + \lambda_0 p_1(t) \\ p_1'(t) & = & \mu_1 p_0(t) - (\lambda_1 + \mu_1) p_1(t) + \lambda_1 p_2(t) \\ p_2'(t) & = & \mu_2 p_1(t) - (\lambda_2 + \mu_2) p_2(t) + \lambda_2 p_3(t) \\ \dots & & \end{array}\right.$$

sous la condition additionnelle $\forall t \geq 0,\ p_0(t) + p_1(t) + \dots = 1$ (loi de probabilité)

La résolution générale est très technique et au-delà de ce cours. On peut néanmoins étudier une question un peu plus simple : existe-t-il un état stationnaire ? Plus précisément, les $\mathbb{P}(X_t = k)_{k \in \mathbb{N}}$ peuvent-elles être constantes, ou bien admettent-elles une limite finie quand $t \to +\infty$?
Avec des hypothèses de régularité raisonnables pour la deuxième question, on peut résoudre ce problème en remplaçant dans les équations de Chapman-Kolmogorov les fonctions par une constante et leurs dérivées par 0. On tire alors un système d'équations, toujours infini mais numérique :

$$\left\{\begin{array}{rcl} -\lambda_0 p_0 + \lambda_0 p_1 & = & 0 \\ \mu_1 p_0 - (\lambda_1 + \mu_1) p_1 + \lambda_1 p_2 & = & 0 \\ \mu_2 p_1 - (\lambda_2 + \mu_2) p_2 + \lambda_2 p_3 & = & 0 \\ \dots & & \end{array}\right.$$

sous la condition additionnelle $p_0 + p_1 + \dots = 1$
On peut alors montrer que l'existence d'une solution au système est conditionnée par le comportement de deux séries numériques à termes positifs.

Proposition Existence d'un état stationnaire

1. Le processus admet un état stationnaire si et seulement si la série $\sum_{n \geq 1} \left(\frac{\mu_1}{\lambda_1} \frac{\mu_2}{\lambda_2} \cdots \frac{\mu_n}{\lambda_n} \right)$ est diver-

gente et la série $\sum_{n\geq 1}\left(\frac{\lambda_0}{\mu_1}\frac{\lambda_1}{\mu_2}\cdots\frac{\lambda_{n-1}}{\mu_n}\right)$ est convergente. Autrement dit,

$$\left(\frac{\mu_1}{\lambda_1}+\frac{\mu_1}{\lambda_1}\frac{\mu_2}{\lambda_2}+\cdots+\frac{\mu_1}{\lambda_1}\frac{\mu_2}{\lambda_2}\cdots\frac{\mu_n}{\lambda_n}+\cdots\right)=+\infty \quad \text{et} \quad \left(\frac{\lambda_0}{\mu_1}+\frac{\lambda_0}{\mu_1}\frac{\lambda_1}{\mu_2}+\cdots+\frac{\lambda_0}{\mu_1}\frac{\lambda_1}{\mu_2}\cdots\frac{\lambda_{n-1}}{\mu_n}+\cdots\right)<+\infty$$

2. Dans le cas où les λ_i (resp. les μ_i), sont égaux entre eux à une valeur λ (resp. μ), la condition s'écrit (très simplement) : $\lambda < \mu$.

5.4 Files d'attente

La théorie des files d'attente est une branche vouée à étudier le comportement d'un système, généralement aléatoire, dans une situation où une catégorie de personnes ou d'entités, les *clients*, viennent chercher une prestation de service auprès d'une autre catégorie de personnes ou d'entités, les *serveurs*. Lorsqu'un ou des serveurs sont disponibles, le client reçoit le service, mais si ce n'est pas le cas, il est mis en attente pour une durée souvent non prédictible.

Cette théorie recouvre une grande variété de situations de la vie quotidienne, depuis l'attente chez un professionnel sans rendez-vous, la gestion des flux de décollage et d'atterrissage des avions dans un aéroport, des requêtes informatiques (par exemple d'impression) auprès de serveurs dédiés.

5.4.1 Description

La cible est de décrire le comportement du système en caractérisant un certain nombre de grandeurs représentatives :

- nombre $X(t)$ de clients dans le système ,
- nombre $X_q(t)$ de clients dans la file d'attente,
- durée de séjour dans le système,
- durée d'attente,
- taux d'occupation des serveurs,
- durée moyenne d'activité (il existe au moins une personne dans le système),
- existence d'un régime stationnaire
- probabilité de saturation : pourcentage de clients n'ayant pu être servis

Comme l'exécution d'un service correspond à la satisfaction du client, ce dernier sort du système lorsqu'il est servi. Ainsi, pendant toute sa durée de fonctionnement, un système de file d'attente s'apparente à un processus de naissance et de mort, où chaque "naissance" correspond à un client arrivant dans le système, et chaque "mort" un départ du système après obtention du service.

5.4.2 Classification

On décrit un phénomène d'attente par 6 symboles : A/S/C/K/M/Z.

- A désigne la loi de probabilités des instants d'arrivée. Lorsque A='M' (pour "markovien"), les arrivées suivent un processus de comptage de Poisson, dont l'intensité est généralement notée λ
- S désigne la loi de probabilités des instants de service. Lorsque S='M', les services exécutés suivent un processus de comptage de Poisson, dont l'intensité est généralement notée μ
- C désigne le nombre de serveurs
- K désigne la capacité maximale du serveur, composée des C serveurs $K-C$ places dans la file d'attente.
- M désigne la taille totale de la population des clients potentiels
- Z désigne la discipline de service :
  - FIFO : First In First Out,
  - LIFO : Last In First Out (gestion de pile),
  - SIRO : Service in Random Order,

— PS : Process Sharing (chaque client reçoit une part de service),

— ...

La classification selon les trois premiers paramètres est initialement due à Kendall. Les autres paramètres ont été ajoutés après. Lorsqu'ils sont omis, K et M sont considérés comme infinis et Z est la discipline FIFO.

5.4.3 File d'attente M/M/1

La file M/M/1, d'après la classification introduite ci-dessus, répond aux principes suivants :

— l'arrivée des clients est un processus de Poisson de paramètre λ,

— le service des clients est un processus de Poisson de paramètre μ,

— il y a un seul serveur,

— la file d'attente n'est pas limitée,

— il y a une infinité de clients potentiels

— la discipline de service est FIFO.

Les taux instantanés de natalité et de mortalité sont :

— $(\lambda_n)_{n\geq 0} = (\lambda, \lambda, \lambda, \dots)$ (suite constante)

— $(\mu_n)_{n\geq 0} = (0, \mu, \mu, \dots)$ (suite constante sauf premier terme : on pose toujours $\mu_0 = 0$ par convention)

Les paramètres λ et μ s'interprètent comme suit :

— λ est le nombre moyen de clients arrivant dans le système par unité de temps

— $1/\lambda$ est le temps moyen entre deux arrivées

— μ est le nombre (potentiel) moyen de clients servis par unité de temps

— $1/\mu$ est le temps moyen de service

Les résultats qui sont maintenant présentés sont des simples cas particuliers de ceux du paragraphe "processus de naissance et de mort".

Probabilités de transitions

Forme infinitésimale : pour $t \geq 0$ et $h > 0$,

$$\begin{cases} \mathbb{P}(X_{t+h} = i-1 | X_t = i) &=& \mu h + o(h) & \text{pour } i \geq 1 \\ \mathbb{P}(X_{t+h} = i | X_t = i) &=& 1 - (\lambda+\mu)h + o(h) & \text{pour } i \geq 1 \\ \mathbb{P}(X_{t+h} = 0 | X_t = 0) &=& 1 - \lambda h + o(h) & \\ \mathbb{P}(X_{t+h} = i+1 | X_t = i) &=& \lambda h + o(h) & \text{si } i \geq 0 \\ \mathbb{P}(X_{t+h} = j | X_t = i) &=& o(h) & \text{si } |j-i| \geq 2 \end{cases}$$

Matrice de transition :

$$Q = \begin{bmatrix} -\lambda & \lambda & 0 & 0 & \dots \\ \mu & -(\lambda+\mu) & \lambda & 0 & \dots \\ 0 & \mu & -(\lambda+\mu) & \lambda & \dots \\ \vdots & \vdots & \vdots & \ddots & \ddots \end{bmatrix}$$

Graphe du processus

Source : Wikipedia

Équations de Chapman-Kolmogorov

— Forme matricielle : $P'(t) = P(t)Q$

— Forme système :

$$\left\{\begin{array}{rcl} p_0'(t) & = & -\lambda p_0(t) + \lambda p_1(t) \\ p_1'(t) & = & \mu p_0(t) - (\lambda+\mu)p_1(t) + \lambda p_2(t) \\ p_2'(t) & = & \mu p_1(t) - (\lambda+\mu)p_2(t) + \lambda p_3(t) \\ \cdots & & \end{array}\right.$$

en notant

$$P(t) = (p_0(t), p_1(t), \dots) = (\mathbb{P}(X_t = 0), \mathbb{P}(X_t = 1), \dots)$$

vérifiant de plus $\forall t \geq 0,\ p_0(t) + p_1(t) + \cdots = 1$

Régime stationnaire

Il existe si et seulement si le système d'équations numériques

$$\left\{\begin{array}{rcl} p_0 + p_1 + \dots & = & 1 \\ -\lambda p_0 + \lambda p_1 & = & 0 \\ \mu p_0 - (\lambda+\mu)p_1 + \lambda p_2 & = & 0 \\ \mu p_1 - (\lambda+\mu)p_2 + \lambda p_3 & = & 0 \\ \cdots & & \end{array}\right.$$

admet une solution. C'est équivalent à $\lambda < \mu$. On a alors

— Loi de probabilités de X, nombre de personnes dans le système :

$$\forall n \geq 0, \quad \mathbb{P}(X = n) = \left(1 - \frac{\lambda}{\mu}\right)\left(\frac{\lambda}{\mu}\right)^n$$

Le coefficient $\dfrac{\lambda}{\mu}$, parfois noté ρ, et égal à $\mathbb{P}(X \geq 1)$ s'appelle le *coefficient d'utilisation du système.*

— Loi de probabilités de X_q, nombre de clients en attente :

$$\begin{array}{rcll} \mathbb{P}(X_q = n) & = & \mathbb{P}(X = n+1) & \\ & & \left(1 - \dfrac{\lambda}{\mu}\right)\left(\dfrac{\lambda}{\mu}\right)^{n+1} & \text{pour } n \geq 1 \\ \mathbb{P}(X_q = 0) & = & \mathbb{P}(X \in \{0,1\}) & \\ & & \left(1 - \left(\dfrac{\lambda}{\mu}\right)^2\right) & \end{array}$$

$$\left\{\begin{array}{l} \mathbb{P}(X_q = 0) = \mathbb{P}(X \in \{0,1\}) = 1 - \left(\dfrac{\lambda}{\mu}\right)^2 = 1 - \rho^2 \\ \forall n \geq 1,\ \mathbb{P}(X_q = n) = \mathbb{P}(X = n+1) = \left(1 - \dfrac{\lambda}{\mu}\right)\left(\dfrac{\lambda}{\mu}\right)^{n+1} = (1-\rho)\,\rho^{n+1} \end{array}\right.$$

— Nombre moyen de clients dans le système : $L = \mathbb{E}[X] = \dfrac{\lambda}{\mu - \lambda} = \dfrac{\rho}{1-\rho}$

— Nombre moyen de clients en attente : $L_q = \mathbb{E}[X_q] = \dfrac{\lambda^2}{\mu(\mu-\lambda)} = \dfrac{\rho^2}{1-\rho}$

Pour estimer des durées (temps de ceci ou de cela), on dispose d'un lemme très puissant car il ne dépend ni de la nature des processus d'arrivées et de départ, ni de la discipline de service.

Lemme Loi de Little

Dans un système stable, le nombre moyen de clients est égal produit du débit d'arrivée par le temps moyen de séjour.

Par suite, on peut estimer typiquement :

— le temps de séjour moyen dans le système : $W = \dfrac{L}{\lambda} = \dfrac{1}{\mu - \lambda}$

— le temps moyen d'attente $W_q = \dfrac{L_q}{\lambda} = \dfrac{\lambda}{\mu(\mu - \lambda)}$

On vérifie au passage par un calcul aisé que $W = W_q + \dfrac{1}{\mu}$, ce qui est bien naturel : le temps moyen passé dans le système est égal au temps moyen d'attente ajouté au temps moyen de service.

5.4.4 La file M/M/1/K

Il y a K places dans le système, soit une place de service et $K-1$ places dans la file d'attente. Le système a donc un nombre fini d'états ($K+1$ en l'occurrence). Le système de Chapman-Kolmogorov a un nombre fini d'équations et un nombre fini d'inconnues, et on vérifie aisément par résolution qu'il y a toujours un régime stationnaire, quels que soient λ et μ. La nouveauté est qu'un client peut désormais être rejeté, c'est-à-dire ni traité ni mis en attente, précisément lorsque le système est plein $\{X = K\}$: la probabilité de rejet est ainsi $\mathbb{P}(X = K)$.

Le tableau suivant donne les formules explicites. Il convient de séparer les cas $\lambda = \mu$ et $\lambda \neq \mu$.

$\lambda \neq \mu$, (i.e. $\rho \neq 1$)	$\lambda = \mu$, (i.e. $\rho = 1$)
Loi stationnaire	
$\forall n = 0, \dots, K, \quad \mathbb{P}(X = n) = \dfrac{1 - \frac{\lambda}{\mu}}{1 - \left(\frac{\lambda}{\mu}\right)^{K+1}} \left(\dfrac{\lambda}{\mu}\right)^n = \dfrac{1-\rho}{1-\rho^{K+1}}\rho^n$	$\forall n = 0, \dots, K,\ \mathbb{P}(X = n) = \dfrac{1}{K+1}$
Probabilité de rejet	
$p_K = \dfrac{1 - \frac{\lambda}{\mu}}{1 - \left(\frac{\lambda}{\mu}\right)^{K+1}} \left(\dfrac{\lambda}{\mu}\right)^K = \dfrac{1-\rho}{1-\rho^{K+1}}\rho^K$	$p_K = \dfrac{1}{K+1}$

Table des matières