Notes du cours de “Calcul Formel pour les physiciens” L1PC 2012. Version 3

G. H. E. DUCHAMP *

02.12.07 07h40

Table des matières

* Prière de signaler les erreurs à ADRIAN TANASA ou à moi-même.

1 Préambule

Ce cours est commun aux étudiants originaires des filières Physique et chimie. Il est conçu de façon à permettre aux étudiants des deux sensibilités de pouvoir s'entraîner tant au niveau de la programmation (TP - TD - libre service) qu'au niveau conceptuel : outils analytiques, numériques et symboliques de l'informatique &/ou utilisés en informatique moderne (sécurité,

simulation, algorithmique rapide). Les T.D. se font en maple, mais le contenu de l'enseignement est indépendant du langage.

Le poly correspond à un programme maximal. Seule une partie de celui-ci sera traitée cette année. Les exercices qui sont là pour aider à la compréhension du cours.
II se peut que vous ne compreniez pas certains énoncés, dans ce cas choisissez que les questions que vous êtes capables d'aborder ... et contactez-moi rapidement pour le décodage.
Ceci vaudra aussi lorsque vous vous exercerez sur annales.

Les parties en petits caractères sont des suppléments et ne sont pas obligatoires.

2 Introduction

Le *Calcul Symbolique* est l'art de manipuler (scientifiquement) les symboles (exacts : $4/7, \pi^2/6, \sqrt{10}$ ou bien littéraux x,y,z,t,u,v) selon certaines règles dites "de calcul" (ou bien de dérivation[1]).
En fait, cette activité est très ancienne et remonte à la numération puisque celle-ci consiste à symboliser des quantités par des symboles et que les quatre opérations arithmétiques ne sont autres que le calcul symbolique attaché à des problèmes concrets (ajout ou retrait de quantités, calcul de longueur, de surface, de volume, mesure d'une grandeur) et donnent lieu aux alogorithmes de l'arithmétique élémentaire.
De même que la mathématique (quand elle n'est pas autogène) développe des modèles pour les sciences de la nature (équations de la physique, lois ..), de même l'Informatique Théorique a développé des modèles et des concepts pour les ordinateurs (machines de Turing, calculabilité, automates, séries génératrices, complexité, grammaires..).
Le *Calcul Formel*[2] est né dès que l'on a essayé de traiter automatiquement certains calculs trop compliqués ou fastidieux pour être élaborés à la main[3]. Il se démarque du *Calcul Numérique* en ceci qu'il est un calcul exact (c'est à dire sans perte d'information due aux erreurs d'arrondi). Par exemple, si l'on veut faire mécaniquement les quatre opérations avec les fractions et $\sqrt{2}$, il faut utiliser la structure de donnée $a + b\sqrt{2};\ a,b \in \mathbb{Q}$, il n'y a pas là d'arrondi. Le problème principal du Calcul Formel est l'explosion des données en cours de calcul (c'est le prix à payer pour l'exactitude). Ansi toute l'arithmétique et ses applications[4] nécessite le calcul exact, en effet une erreur d'un digit même sur un nombre de 250 chiffres peut transformer un nombre pair en nombre impair ! Ceci est génant pour les tests de parité, par exemple dans les modems : le *bit de parité*, une forme très rudimentaire de code détecteur d'erreurs.
Le Calcul Symbolique peut ici être vu comme la science qui va traiter à la fois des structures de donnés du Calcul Formel et du comportement de ceux-ci (cf infra, la méthode Symbolique en complexité).

Pour résumer, le voisinage scientifique du Calcul Symbolique se compose ainsi :

- le calcul scientifique exact
- le calcul formel (et, concrètement, les systèmes de Calcul Formel)
- l'informatique théorique

1. On parle de *règle de dérivation* en logique formelle ou en réécriture et d'*arbre de dérivation* dans les théories des grammaires et des systèmes formels
2. Computer Algebra en anglais.
3. En anglais : hand and paper computation.
4. comme le codage, décodage, cryptage, la sécurité des transmissions par exemple..

– les systèmes formels
– la combinatoire

les sciences voisines sont l'informatique, les mathématiques, la physique et, depuis peu, la chimie et la biologie.

3 Systèmes de Calcul Formel et structures de données

4 Présentation générale et screenshots (captures d'écran)

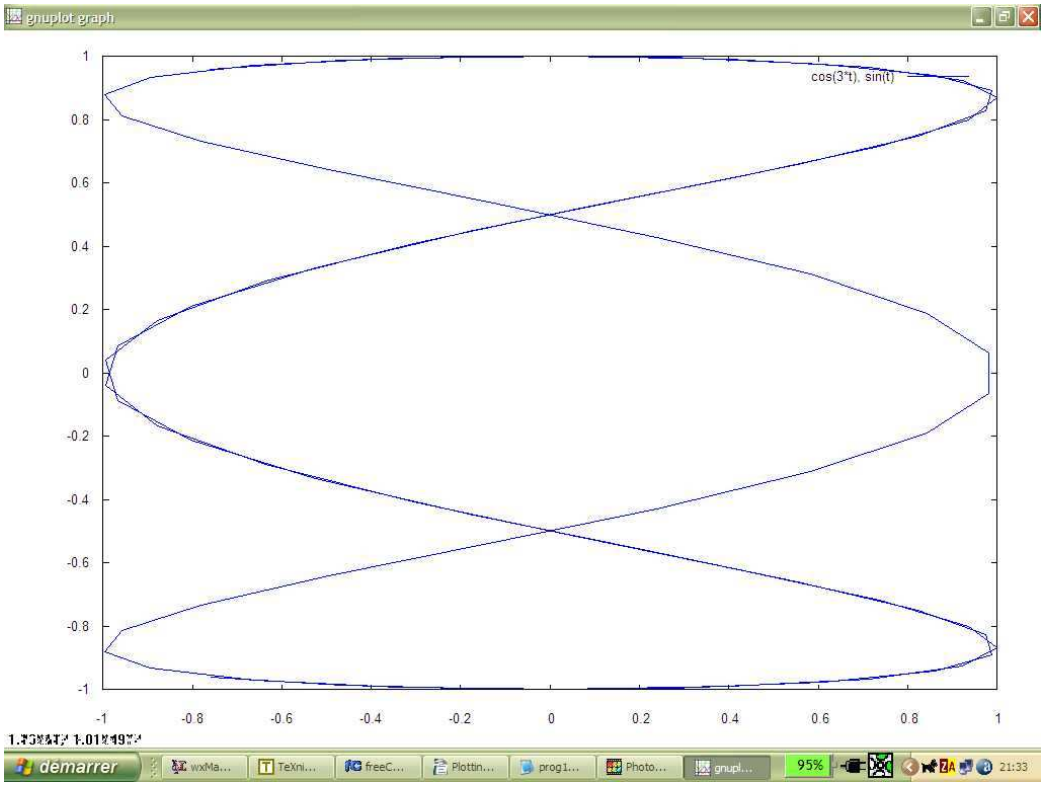


Fig 1. — *Une courbe paramétrique* $(x(t),y(t)) = (cos(3t),sin(t))$.

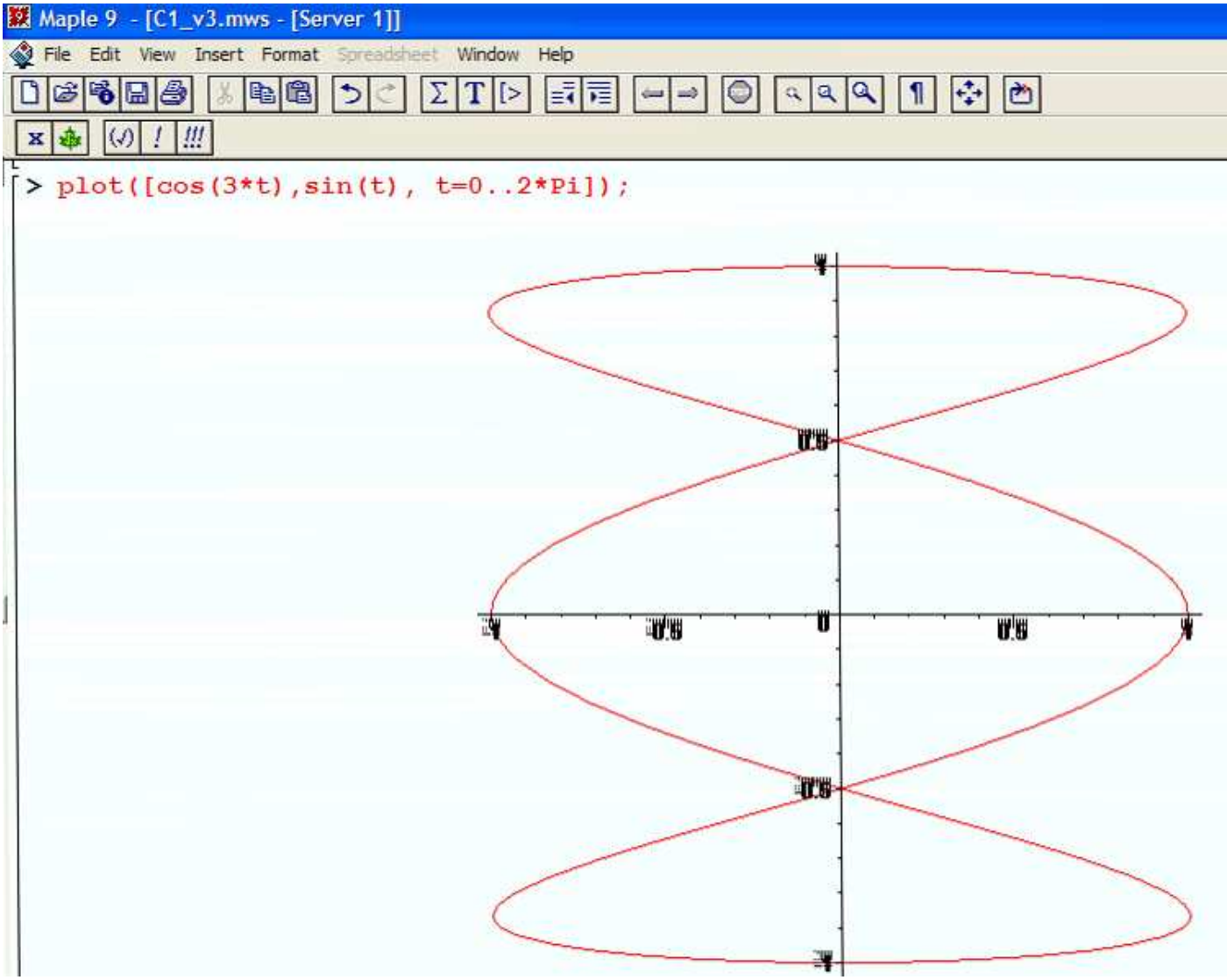


Fig 1a. — *La même en Maple* $(x(t),y(t)) = (cos(3t),sin(t))$.

wxMaxima HTML export - Mozilla Firefox

Fichier Édition Affichage Historique Marque-pages Outils ?

file:///C:/Ens/Paris7/07_08/screen1.html

Free Yahoo! Gmail Google Google Scholar MathWorld HAL arXiv.org Wikipédia (FR) Wikipedia (EN) Amazon.fr Amazon.com

```
/* wxMaxima 0.7.2 http://wxmaxima.sourceforge.net
Maxima 5.12.0 http://maxima.sourceforge.net
Using Lisp GNU Common Lisp (GCL) GCL 2.6.8 (aka GCL)
Distributed under the GNU Public License. See the file COPYING.
Dedicated to the memory of William Schelter.
This is a development version of Maxima. The function bug_report()
provides bug reporting information.

(%i1) M: matrix([41, 2, 3, 4], [1, 42, 3, 2], [1, 2, 43, 4], [1, 2, 3, 43])$
f(x, y) := float (M [?round(x), ?round(y)])$
plot3d (f, [x, 1, 4], [y, 1, 4], ['grid, 4, 4])$

(%i4) M: matrix([100, 2, 3, 4], [1, 200, 3, 2], [1, 2, 300, 4], [1, 2, 3, 400])$
f(x, y) := float (M [?round(x), ?round(y)])$
plot3d (f, [x, 1, 4], [y, 1, 4], ['grid, 4, 4])$
```

Created with wxMaxima.

Fig 2. — *Matrices de données.*

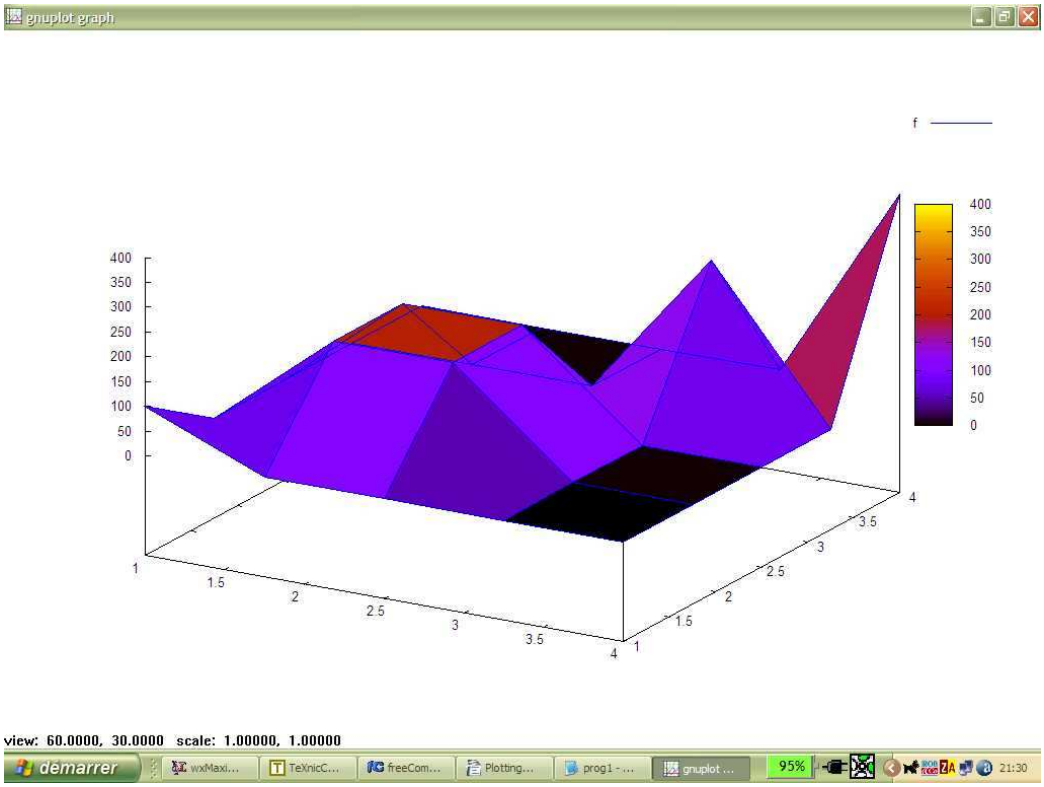


Fig 3. — *Visualisation d'une matrice.*

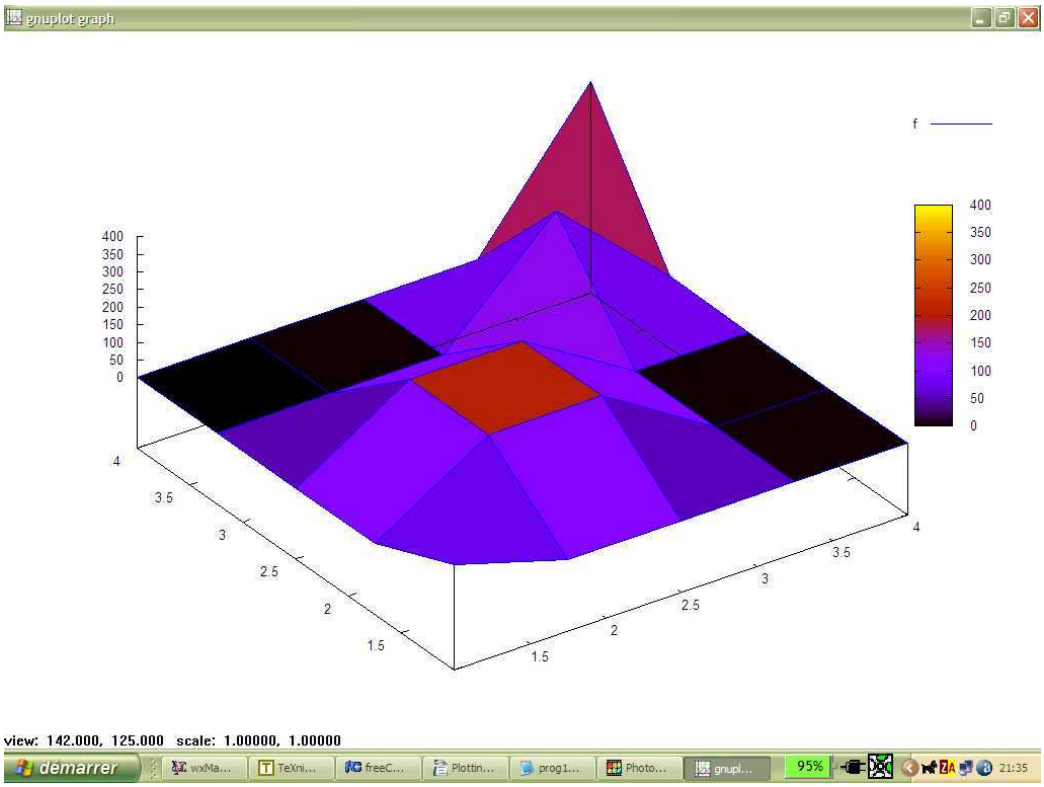


Fig 4. — *Le même diagramme après rotation.*

4.1 Numération

Il est bon, avant d'attaquer, de maîtriser la numération en base quelconque. Voici quelques exercices.

Entiers positifs en base quelconque. —

$$N = \sum_{j=0}^{m} a_j B^j \tag{1}$$

où $B \geq 2$ est un entier (la base) et N est suffsament grand. On peut rajouter des zéros devant ($q_j = 0$ pour $j > m$) cela ne change pas la valeur. On note le résultat

$$N = (a_m a_{m-1} \cdots a_0)_B \tag{2}$$

Par exemple $(101122)_3 = 287$, mais $(101122)_5 = 3287$ et $(101122)_7 = 17215$.
Pour des nombres "fractionnaires", on utilise une représentation avec chiffres après la virgule.

$$N = \sum_{j=-n}^{m} a_j B^j \ . \tag{3}$$

Ce nombre se représente

$$N = (a_m a_{m-1} \cdots a_0 \, , a_{-1} \cdots a_{-n})_B \tag{4}$$

Il se peut que, pour être exact, le développement doive avoir une infinité de chiffres après la virgule (on se limite ici à $B = 10$ et l'on appelle cela un DDI ou Développement Décimal Illimité). On connait tous

$$1/3 = 0{,}333333333333333333333333\cdots \tag{5}$$

mais on a aussi

$$22/7 = 3{,}142857142857142857142857142857142857142857\cdots = 3{,}(142857)^{\infty} \ . \tag{6}$$

En fait un DDI $(a_m a_{m-1} \cdots a_0 \, , a_{-1} \cdots)$ (j va de m à $-\infty$) représente le réel

$$x = lim_{n\to\infty}\Big(\sum_{j=-n}^{m} a_j 10^j \Big) \ . \tag{7}$$

Tout réel admet un DDI (et même un DDI propre, c'est à dire ne se terminant pas par $(9)^{\infty}$). On peut monter que

Proposition 4.1 *Soit $x > 0$ un réel admettant un DDI $x = a_m a_{m-1} \cdots a_0 \, , a_{-1} \cdots$, on a l'équivalence suivante*

$$(\text{Le DDI de } x \text{ est ultimement périodique}) \Longleftrightarrow (x = p/q \text{ avec } p,q \in \mathbb{N} \setminus \{0\})$$

Parties entières. —
C'est ce qu'il y a *devant la virgule*. En informatique, on utilise deux parties entières. La *partie entère haute* `ceiling` (plafond, en anglais) $\lceil x \rceil$, c'est le plus petit entier naturel supérieur à x

et la *partie entère basse* `floor` (plancher, an anglais) $\lfloor x \rfloor$). On a Lorsque x n'est pas entier, on a

$$\lfloor x \rfloor = \begin{cases} \lceil x \rceil \text{ si } x \in \mathbb{N} \\ \lceil x \rceil - 1 \text{ si } x \notin \mathbb{N} \end{cases}, \tag{8}$$

$\lfloor x \rfloor$ est donc le plus grand entier inférieur (ou égal) à x.

Fractions continues. —

Pour $x > 0$ donné, on peut imaginer le procédé de calcul suivant.

```
frac_cont:=proc(x,n)
local res,an,xn,i;
xn:=x:an:=floor(x):res:=an:
for i to n while xn<>floor(xn)
do
xn:=1/(xn-an):an:=floor(xn): res:=res,an
od
:[res]
end;
```

4.1.1 Quelques exercices

Objectifs : Il faut que les étudiants soient maîtres (papier crayon et programmation) des conversions entre bases (avec virgule) et du passage (fraction $\leftrightarrow$ développement périodique). La commande maple pour vérifier les conversions est à chercher dans `convert`, celle pour les développement illimités dans `evalf` (attention à la variable d'environnement `Digits`).

1) Mettre les nombres binaires suivants sous forme décimale
a) $(101101)_2$ b)$(101101101)_2$ c) $(\underbrace{101\cdots101}_{3n \text{ chiffres}})_2$ (pour le (c), on montrera que la réponse dépend de la conversion d'un nombre plus simple)
2) Mettre les fractions suivantes sous forme décimale
a) $(0{,}615)_8$ b) $(12{,}321)_5$ c) $(0,\underbrace{7777777777}_{10 \text{ chiffres}})_8$
3) Calculer
a) $a_n = (0,\underbrace{5\cdots5}_{n \text{ chiffres}})_8$ b) $b_n = (12,\underbrace{1212\cdots12}_{2n \text{ chiffres}})_8$ c) $c_n = (12,\underbrace{2112\cdots2112\cdots}_{n \text{ chiffres}})_8$
d) $f_1 = (0{,}(54321)^\infty)_8$
e) le développement décimal illimité de
i) $23/7$ ii) $7/22$ iii) $1/99999$

4) Conversions Fraction $\leftrightarrow$ Développements illimités en base b (les résultats seront toujours donnés en base dix sauf pour les points c,e).
a) $12{,}(345)^\infty;\ b = 10$ b) $12{,}(345)^\infty;\ b = 8$
c) $BA/CA;\ b = 16$ d) $22/132;\ b = 10$ e) $BA{,}(CA)^\infty;\ b = 16$

4.2 Les systèmes de Calcul Formel

4.2.1 Présentation

Un système de CF est composé de

- un noyau
- des bibliothèques

Les objets manipulés sont:

1. Toutes les structures de données classiques :
   arbres, listes, permutations, graphes, ensembles, intervalles, tables, tableaux, mots, partitions, compositions,partitions, endofonctions.
2. Les quantités du calcul scientifique :
   nombres, radicaux, polynômes, fractions rationnelles, matrices, vecteurs, tenseurs, fonctions, séries.
3. Les opérateurs pour ces structures :

   (a) Pour les structures de données : Manipulation d'arbres (sous arbres, etc...), retirer ou ajouter un élément dans une liste ou un ensemble, un sommet ou une arête dans un graphe, concaténer ou simplifier des mots (fusion, réunion, contraction etc...).

   (b) Pour les quantités du calcul scientifique : dérivation, intégration et sommation symboliques. équations différentielles, développements limités ou en série.

4. Résolution des équations posées dans le cadre précédent.

Bien entendu, un système de calcul formel comprend aussi des interfaces graphiques, texte etc....
On peut représenter toutes sortes de formules et on est très vite confronté aux problèmes d'égalité (i.e. reconnaître les doubles représentations). Par exemple on a

$$\sqrt{2}+\sqrt{3}+\sqrt{5}=\sqrt{10+2\sqrt{10}+2\sqrt{3}\sqrt{7+2\sqrt{10}}} \tag{9}$$

comment le système peut-il s'en appercevoir ? Plus difficile, comment le système peut-il donner la premier membre à partir du second ? (problèmes $A = B$, $A \to B$, voir les fonctions `convert(??,parfrac), rationalize, normal, collect`) ($\hookrightarrow$ forme normale, canonique, simplification automatique).
: Remarquer que:

```
> A := sqrt(7+2*sqrt(10));
```

$$A := \sqrt{7+2\sqrt{10}}$$

```
> simplify(A);
```

$$\sqrt{2}+\sqrt{5}$$

Mais

```
> B := sqrt(10+2*sqrt(10)+2*sqrt(3)*sqrt(7+2*sqrt(10))): simlify(B);
```

$$\sqrt{10+2\sqrt{2}\sqrt{5}+2\sqrt{3}\sqrt{5}+2\sqrt{3}\sqrt{2}}$$

Vaut-il mieux représenter une fraction sous la forme $\frac{p}{q}$ ou par son développement décimal (qui est complètement représentable en machine parce que périodique à partir d'un certain rang) ?
Comment passer d'une représentation à l'autre ?

Combinatoire. —
C'est l'art de manipuler ls structures de données discrètes.

Exercice 4.2 *i) Bijections $\mathbb{N}^2 \to \mathbb{N}$ et écriture explicite du couple de rang n.*
ii) Arbre de Wilf
iii) Fractions continues.

4.2.2 Exemples de sessions

Interpréteur (cf [3] p17). —

```
> c:= [1,2,3,u,v];
```

$$c := [1, 2, 3, u, v]$$

```
> nops(c);
```

$$5$$

```
> op(4,c);
```

$$u$$

```
> c[4];
```

$$u$$

```
> d:=[2,5*u,4*v];
```

$$d := [2, 5\,u, 4\,v]$$

```
> e:=[op(c),op(d)];
```

$$e := [1, 2, 3, u, v, 2, 5\,u, 4\,v]$$

```
> map(x->x^2,c);
```

$$[1, 4, 9, u^2, v^2]$$

La formule de Rodrigues pour les polynomes d'Hermite est

$$H_n(x) := (-1)^n e^{x^2} \frac{d^n}{dx^n}(e^{-x^2})$$

On peut les calculer en repetant une même commande à l'aide de `diff`. Soit

```
> n:=0:c:=[n,exp(-x^2)];
```

$$c := [0, e^{(-x^2)}]$$

```
> n:=n+1:c:=[n,factor(diff(c[2],x))];
```

$$c := [1, -2\,x\,e^{(-x^2)}]$$

```
> n:=n+1:c:=[n,factor(diff(c[2],x))];
```

$$c := [2, 2\,e^{(-x^2)}\,(-1+2\,x^2)]$$

```
> n:=n+1:c:=[n,factor(diff(c[2],x))];
```

$$c := [3, -4\,x\,e^{(-x^2)}\,(-3+2\,x^2)]$$

```
> for i to 7 do n:=n+1:c:=[n,factor(diff(c[2],x))]:  od : print(c);
```

$$[10, 32\,e^{(-x^2)}\,(-945+9450\,x^2-12600\,x^4+5040\,x^6-720\,x^8+32\,x^{10})]$$

```
> f:=1/(1+x^4);
```

$$f := \frac{1}{1+x^4}$$

```
> int(f,x);
```

$$\frac{1}{8}\sqrt{2}\ln\left(\frac{x^2+x\sqrt{2}+1}{x^2-x\sqrt{2}+1}\right)+\frac{1}{4}\sqrt{2}\arctan(x\sqrt{2}+1)+\frac{1}{4}\sqrt{2}\arctan(x\sqrt{2}-1)$$

```
> with(combinat);
Warning, the protected name Chi has been redefined and unprotected
```

[Chi, *bell*, binomial, *cartprod*, *character*, *choose*, *composition*, *conjpart*, *decodepart*, *encodepart*, *fibonacci*, *firstpart*, *graycode*, *inttovec*, *lastpart*, *multinomial*, *nextpart*, *numbcomb*, *numbcomp*, *numbpart*, *numbperm*, *partition*, *permute*, *powerset*, *prevpart*, *randcomb*, *randpart*, *randperm*, *stirling1*, *stirling2*, *subsets*, *vectoint*]

```
> fibonacci(43);
```

> 433494437;

Exercice 4.3 *On considère la suite des nombres de Fibonacci* $F_0 = 0$, $F_1 = 1$, $F_{n+2} = F_n + F_{n+1}$.

a) Montrer que

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^n = \begin{pmatrix} F_n & F_{n+1} \\ F_{n+1} & F_{n+2} \end{pmatrix} \tag{10}$$

b) En déduire que, pour $n \geq 2$*, on a*

$$F_n = \begin{pmatrix} 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{n-2} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{11}$$

c) En déduire une méthode rapide de calcul des F_n*.*

d) Évaluer la complexité, en nombre d'opérations arithmétiques, de la méthode naïve (fenêtre glissante) et de la méthode proposée en (b).

e) Indiquer comment on peut encore réduire la complexité en remarquant une propriété de symétrie sur les matrices $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^n$.

Taylor: Exemple de $((1-x)/(1+x))^{1/2}$

$> f := ((1+x)/(1-x))^{(1/2)};$

$$\frac{\sqrt{1+x}}{\sqrt{1-x}}$$

$> taylor(f, x = 0, 20);$

$$(1 + x + \frac{1}{2}x^2 + \frac{1}{2}x^3 + \frac{3}{8}x^4 + \frac{3}{8}x^5 + \frac{5}{16}x^6 + \frac{5}{16}x^7 + \frac{35}{128}x^8 + \frac{35}{128}x^9 + \frac{63}{256}x^{10} + \frac{63}{256}x^{11} + \frac{231}{1024}x^{12} + \frac{231}{1024}x^{13} + \frac{429}{2048}x^{14} + \frac{429}{2048}x^{15} + \frac{6435}{32768}x^{16} + \frac{6435}{32768}x^{17} + \frac{12155}{65536}x^{18} + \frac{12155}{65536}x^{19} + O\left(x^{20}\right))$$

$> f1 := f/(1+x);$

$> taylor(f1, x = 0, 20);$

$$(1 + \frac{1}{2}x^2 + \frac{3}{8}x^4 + \frac{5}{16}x^6 + \frac{35}{128}x^8 + \frac{63}{256}x^{10} + \frac{231}{1024}x^{12} + \frac{429}{2048}x^{14} + \frac{6435}{32768}x^{16} + \frac{12155}{65536}x^{18} + O\left(x^{20}\right))$$

$> f2 := (1-x)^{(-1/2)};$

$$(1 + \frac{1}{2}x + \frac{3}{8}x^2 + \frac{5}{16}x^3 + \frac{35}{128}x^4 + \frac{63}{256}x^5 + \frac{231}{1024}x^6 + \frac{429}{2048}x^7 + \frac{6435}{32768}x^8 + \frac{12155}{65536}x^9 + \frac{46189}{262144}x^{10} + \frac{88179}{524288}x^{11} + \frac{676039}{4194304}x^{12} + \frac{1300075}{8388608}x^{13} + \frac{5014575}{33554432}x^{14} + \frac{9694845}{67108864}x^{15} + \frac{300540195}{2147483648}x^{16} + \frac{583401555}{4294967296}x^{17} + \frac{2268783825}{17179869184}x^{18} + \frac{4418157975}{34359738368}x^{19} + O\left(x^{20}\right))$$

$> f3 := subs(x = 4 * x, f2);$

$> taylor(f3, x = 0, 20);$

$$(1 + 2\,x + 6\,x^2 + 20\,x^3 + 70\,x^4 + 252\,x^5 + 924\,x^6 + 3432\,x^7 +$$
$$12870\,x^8 + 48620\,x^9 + 184756\,x^{10} + 705432\,x^{11} + 2704156\,x^{12} + 10400600\,x^{13} + 40116600\,x^{14} +$$
$$155117520\,x^{15} + 601080390\,x^{16} + 2333606220\,x^{17} + 9075135300\,x^{18} + 35345263800\,x^{19} + O\left(x^{20}\right))$$

$> cb := proc(n)\ binomial(2 * n, n)\ end;$

$$proc(n)\ binomial(2 * n, n)\ end$$

$> cb(17);$

$$2333606220$$

$> cb(19);$

$$35345263800$$

$> sum(binomial(2 * n, n) * x^n, n = 0..infinity);$

$$\frac{1}{\sqrt{1 - 4x}}$$

Solutions approchées de $(x = arctan(2x))$

$> read\ flot;$

$f := proc(n)$

$\ local x, y;$

$\ x := 1;$

$\ y := 2;$

$\ while\ evalf(y - x, n) <> 0\ do\ x := y; y := evalf(2 * arctan(x), n)\ od$

$\ end;$

$> f(10);$

$$2.331122370$$

$> f(20);$

$$2.3311223704144226136$$

$> f(100);$

$$2.331122370414422613667835955917121338269077695386114575109737293393230817432716673842154257104393014$$

Exercice 4.4 *Les séries $log(1 + h)$ et $exp(X)$ étant connues. On pose,*

$$(1 + h)^\alpha := exp(\alpha.log(1 + h))$$

pour $\alpha \in \mathbb{C}$. D'autre part, pour tout complexe α, on définit

$$\left(\begin{array}{c} \alpha \\ k \end{array} \right) := \frac{\alpha(\alpha - 1) \cdots (\alpha - k + 1)}{k!}$$

i) En utilisant le développement de Taylor, montrer que

$$(1+h)^\alpha = \sum_{k=0}^{\infty} \left(\begin{array}{c} \alpha \\ k \end{array} \right) h^k$$

ii) En déduire la formule

$$\sum_{n\geq 0} \left(\begin{array}{c} 2n \\ n \end{array} \right) x^n = \frac{1}{\sqrt{1-4x}}$$

Programmation. —
Le produit de facteurs

$$\prod_{\epsilon_i \in \{-1,1\},\ i=1..3} (X + \epsilon_1\sqrt{2} + \epsilon_2\sqrt{3} + \epsilon_3\sqrt{5})$$

qui peut servir à montrer l'équation (9).

```
pol2 :=
proc()
local res,i,j,k;
res := 1;
for i from -1 by 2 to 1 do
for j from -1 by 2 to 1 do
for k from -1 by 2 to 1 do
res:= res*(X - i * 2^(1/2) - j * 3^(1/2) - k * 5^(1/2))
od
od
od;
res
end;
```

$> pol2();$

$$\left(X+\sqrt{2}+\sqrt{3}+\sqrt{5}\right)\left(X+\sqrt{2}+\sqrt{3}-\sqrt{5}\right)\left(X+\sqrt{2}-\sqrt{3}+\sqrt{5}\right)\left(X+\sqrt{2}-\sqrt{3}-\sqrt{5}\right)$$
$$\left(X-\sqrt{2}+\sqrt{3}+\sqrt{5}\right)\left(X-\sqrt{2}+\sqrt{3}-\sqrt{5}\right)\left(X-\sqrt{2}-\sqrt{3}+\sqrt{5}\right)\left(X-\sqrt{2}-\sqrt{3}-\sqrt{5}\right)$$

$> expand(");$

$$-960\,X^2 + 352\,X^4 - 40\,X^6 + X^8 + 576$$

$> subs(seq(X^{(2*i)} = x^i, i = 1..4),");$

$$-960\,x + 352\,x^2 - 40\,x^3 + x^4 + 576$$

$> [solve(")];$

$$[10 + 2\sqrt{10} + 2\sqrt{3}\sqrt{7+2\sqrt{10}}, 10 + 2\sqrt{10} - 2\sqrt{3}\sqrt{7+2\sqrt{10}},$$
$$10 - 2\sqrt{10} + 2\sqrt{3}\sqrt{7-2\sqrt{10}}, 10 - 2\sqrt{10} - 2\sqrt{3}\sqrt{7-2\sqrt{10}}]$$

$> op(1,");$

$$10 + 2\sqrt{10} + 2\sqrt{3}\sqrt{7+2\sqrt{10}}$$

4.2.3 Histoire succinte des Systèmes de Calcul Formel

Voici, à gros traits, des éléments de l'histoire récente (nous ne parlons pas de la machine arithmétique de Pascal) des Systèmes de Calcul Formel.

1953 : Premier système de dérivation (en LISP).
1958 : LISP (John Mc Carthy au MIT).
1960-70 : SAC-1 (G. Collins) manipulations de polynômes en Fortran.
ALPAK aux Bell Labs (polynômes et fractions rationnelles).
FORMAC à IBM.
Premier programme d'intégration en LISP.
MATHLAB au MIT (utilisation interactive, affichage bidimentionnel).
REDUCE (en Lisp) à Standford.
1970-80 : MACSYMA (En lisp au MIT).
SCRATCHPAD (chez IBM).
1980-90 : MAPLE à Waterloo (en C).
SMP par S. Wolfram.
SCRATCHPAD II (chez IBM).
Systèmes dédiés MACAULAY, GAP, CAYLEY, PARI,...
1990-.. : MATHEMATICA (S. Wolfram), AXIOM (Version commercialisée de SCRATCHPAD I),
MuPAD (Développé par des universitaires européens).
http://mupad.sourceforge.net/

Quelques commentaires..

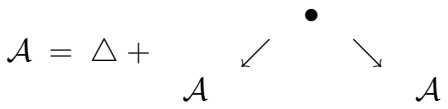
AXIOM, demande une grosse station de travail I.B.M.
MACSYMA, développé au MIT, commercialisé par Symbolics.
REDUCE de Anthony C. Hearn, disponible chez Softworld.
MATHEMATICA, très convivial mais pas toujours très fiable.
muMATH, peut fonctionner sur de petits ordinateurs.
SCRATCHPAD, développé par IBM, langage fortement typé.
CAYLEY, manipule les groupes.
MACAULAY, développé par David Bayer et Michel Stillman, résout bien les systèmes d'équations algébriques.
MAPLE, développé à l'université de Waterloo (Canada), disponible chez Softworld.
PARI Comporte les meilleurs algorithmes actuels de théorie des nombres (développé à Bordeaux).
SYMMETRICA Comporte les meilleurs algorithmes sur la combinatoire du groupe symétrique, les polynômes symétriques, les algèbres de Hecke et leurs représentations.
MuPAD Système généraliste qui a des commandes similaires a Maple, mais la communication avec C et C++ est plus simple.

4.3 Introduction à Maple : T.D.

4.4 Quelques structures de données

4.4.1 Arbres binaires complets

L'ensemble $\mathcal{A}$ des arbres binaires est construit par la grammaire **(G1)**



Il y a trois notions de *taille* classiques : le nombre de nœuds, le nombre de sommets, la profondeur.

Exercice 4.5 *1) Montrer que pour toutes ces notions de taille, le nombre d'arbres d'une taille donnée est fini.*
2) Donner la série génératrice des arbres binaires complets par nombre de nœuds.
3) Donner la grammaire qui engendre les arbres binaires dont les feuilles sont indexées par un ensemble F fini donné. Donner les premiers éléments pour $F = \{a,b\}$.

Éléments pour la solution (s'entraîner à rédiger l'exercice précédent). —
On peut adopter une notation typographiquement plus rapide : un arbre différent de $\bullet$ sera donc noté $\mathcal{A} = (\mathcal{A}_g,\mathcal{A}_d)$ où $\mathcal{A}_g$ (resp. $\mathcal{A}_d$) est le sous-arbre gauche (resp. droit). La taille (ici nombre de nœuds) peut se définir récursivement par

$$\tau(\bullet) = 1;\ \tau((\mathcal{A}_g,\mathcal{A}_d)) = \tau(\mathcal{A}_g) + \tau(\mathcal{A}_d) + 1 \tag{12}$$

ce qui donne l'équation pour la SGO $\sum_{k\geq 0} a_k x^k$ (où a_k est le nombre d'arbres binaires à k nœuds).

$$T = x + xT^2 \tag{13}$$

soit $xT^2 - T + x = 0$ on résout (13) par la méthode habituelle. Le discriminant est $\Delta = 1 - 4x^2$ et les racines possibles sont

$$T_1 = \frac{1-\sqrt{1-4x^2}}{2x};\ T_2 = \frac{1+\sqrt{1-4x^2}}{2x} \tag{14}$$

T_2 ayant un terme de plus bas degré en $1/x$ ne peut pas être retenue. On a donc $T = T_1$. Vérifions ce résultat.
On sait que

$$(1+X)^\alpha = \sum_{k\geq 0} \left(\begin{array}{c} \alpha \\ k \end{array} \right) X^k \tag{15}$$

avec

$$\left(\begin{array}{c} \alpha \\ k \end{array} \right) := \frac{(\alpha)(\alpha-1)\cdots(\alpha-k+1)}{k!} \tag{16}$$

ceci qui donne

$$\sqrt{1-4x^2} = \sum_{k\geq 0} \left(\begin{array}{c} 1/2 \\ k \end{array} \right) (-4x^2)^k \tag{17}$$

à l'aide de (16), on a, pour $k \geq 1$

$$\left(\begin{array}{c} 1/2 \\ k \end{array} \right) = \frac{(1/2)(1/2-1)(1/2-2)\cdots(1/2-k+1)}{k!} = \frac{(-1).(-3)\cdots(3-2k)}{2^k k!} = \tag{18}$$

$$\frac{(-1)^{k-1}1.3.\cdots(2k-3)}{2^k k!} = \frac{(-1)^{k-1}(2k-2)!}{2^{2k-1}k!(k-1)!} \tag{19}$$

en remplaçant ce résultat dans (17) puis dans (14), il vient

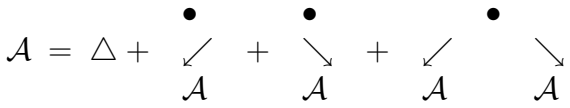
$$T = \sum_{k\geq 1} \frac{\binom{2k-2}{k-1}}{k} x^{2k-1} = \tag{20}$$

$$x + x^3 + 2x^5 + 5x^7 + 14x^9 + 42x^{11} + 132x^{13} + 429x^{15} \cdots \tag{21}$$

Exercice 4.6 *Reprendre l'exercice précédent avec le nombre de sommets comme taille.*

4.4.2 Arbres binaires incomplets

L'ensemble $\mathcal{A}$ des arbres binaires est construit par la grammaire **(G2)**

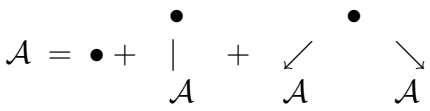


De même que précédemment, il y a trois notions de *taille* classiques : le nombre de nœuds, le nombre de sommets, la profondeur.

Exercice 4.7 *Reprendre l'exercice précédent pour ce type d'arbres.*

4.4.3 Arbre 1-2

Pour les arbres 1-2, on a la grammaire



Exercice 4.8 *1) Peut -on énumérer ces arbres par nombre de feuilles, par profondeur ?*
2) Reprendre les exercices précédents pour le nombre de nœuds.

Éléments pour la solution (s'entrainer à rédiger l'exercice précédent). —

Par nombre (total) de nœuds on a

$$T = x + xT + xT^2 \text{ soit } xT^2 + (x-1)T + x = 0 \tag{22}$$

on obtient

$$T = \frac{1 - x - \sqrt{1 - 2x - 3x^2}}{2x} = x + x^2 + 2x^3 + 4x^4 + 9x^5 + 21x^6 + 51x^7 + 127x^8 + \cdots \tag{23}$$

4.4.4 Arité variable

Cette fois, chaque nœud peut avoir un nombre arbitraire de fils. La grammaire en notation symbolique est

$$\mathcal{A} = \bullet + \sum_{k\geq 1} \underbrace{(\mathcal{A}, \mathcal{A}, \cdots, \mathcal{A})}_{k \text{ fois}} \tag{24}$$

Exercice 4.9 *Écrire et résoudre la série génératrice de ces arbres.*

4.4.5 Expressions arithmétiques

Une expression arithmétique, impliquant les quatre opérations $(+, \times, -, /)$ est un arbre dont les nœuds sont marqués avec ces opérateurs. Les deux premières opérations (associatives) sont d'arité variable et les deux dernières (non associatives) d'arité deux. Le nombre de feuilles de ces arbres est le *nombre de places de l'expression arithmétique*.

Exemple 4.10 *Par exemple* $((\circ+\circ+\circ)*\circ)/(\circ-\circ)$ *est une expression arithmétique à 6 places.*

Exercice 4.11 *1) Donner la grammaire des expressions arithmétique et les premières d'entre elles.*
2) Comment définir le domaine de définition d'une expression arithmétique ?

4.4.6 Monômes noncommutatifs

Cette structure est familière aux étudiants de nos formations, c'est celle des *mots* sur un alphabet donné A. La grammaire de ces mots est

$$M = \epsilon + \sum_{a \in A} aM \tag{25}$$

l'ensemble engendré est le *monoïde libre* $M = A^*$.

Exercice 4.12 *Donner la grammaire pour les mots de* $\{a,b\}^*$ *sans* a^2. *Sans* a^2 *ni* b^2.

4.4.7 Monômes commutatifs

Ce sont les monômes du calcul algébrique. Par exemple pour deux lettres $\{a,b\}$, les monômes sont les expressions $a^i b^j$. Ces monômes sont munis d'une structure de monoïde par

$$(a^{i_1} b^{j_1})(a^{i_2} b^{j_2}) = a^{i_1+i_2} b^{j_1+j_2} \tag{26}$$

Plus généralement, soit un alphabet fini $A = \{a_1, a_2, \cdots, a_n\}$, le monoïde commutatif libre est défini par

$$A^{\oplus} = \{a_1^{i_1} a_2^{i_2} \cdots a_n^{i_n}\}_{i_k \in \mathbb{N}} \tag{27}$$

la loi étant donnée par

$$(a_1^{i_1} a_2^{i_2} \cdots a_n^{i_n})(a_1^{j_1} a_2^{j_2} \cdots a_n^{j_n}) = a_1^{i_1+j_1} a_2^{i_2+j_2} \cdots a_n^{i_n+j_n} \tag{28}$$

ce qui permet les calculs comme $(x^3 y^5 z^2)(x^2 y^8 z^4) = x^5 y^{13} z^6$.

Exercice 4.13 *Payement par pièces. (Donné en cours.)*

5 Les constructeurs set, multiset & list

5.1 Définitions générales

5.2 Set

5.3 List

5.4 Multiset

5.4.1 OGF

5.4.2 EGF

5.5 Séries rationnelles (repésentations linéaires et aspect automatique)

Exercices préliminaires. — Fontaine de pièces de Wilf, polyomino tas.
Avant de généraliser la théorie des séries rationnelles à plusieurs variables (non-commutatives), il est utile de voir comment elles peuvent se représenter par un automate (unaire et à mltiplicités). On a la proposition suivante (énoncée dans le cas général où l'ensemble des scalaires K est un corps commutatif quelconque)

Proposition 5.1 *Soit $S = \sum_{n\in\ N} a_n z^n \in K\langle\langle z\rangle\rangle$ une série. Les conditions suivantes sont équivalentes*
i) S est rationnelle, c'est à dire $S = P(Q)^{-1}$ où P,$Q \in K\langle z\rangle$ et $Q(0) \neq 0$
ii) Les coefficients de S vérifient une récurrence linéaire

$$(\exists(\alpha_j)_{0\leq j<k} \in K^k)(\forall n \in \mathbb{N})(a_{n+k} = \sum_{j=0}^{k-1} \alpha_j a_{n+j}) \tag{29}$$

iii) Il existe $\lambda \in K^{1\times n}$, $T \in K^{n\times n}$,$\gamma \in K^{n\times 1}$ tels que

$$(\forall n \in \mathbb{N})(a_n = \lambda T^n \gamma) \tag{30}$$

Preuve — ii) $\Longrightarrow$ iii). —
La relation de récurrence linéaire implique

$$(a_{n+1},a_{n+2}\cdots,a_{n+k}) = (a_n,a_{n+1}\cdots,a_{n+k-1}) \begin{pmatrix} 0 & 0 & \cdots & \cdots & 0 & \alpha_0 \\ 1 & 0 & \ddots & & \vdots & \vdots \\ 0 & 1 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 & \vdots \\ \vdots & \vdots & & \ddots & 0 & \alpha_{k-2} \\ 0 & 0 & \cdots & \cdots & 1 & \alpha_{k-1} \end{pmatrix} \tag{31}$$

soit, en posant T, la matrice et $v_n = (a_n,a_{n+1}\cdots,a_{n+k-1})$, $v_{n+1} = v_n T$, d'où $v_n = v_0 T^n$. On a finalement

$$a_n = v_n \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = (a_0,a_1\cdots,a_{k-1})T^n \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \tag{32}$$

iii) $\Longrightarrow$ i). —
En effet, $S = \sum_n a_n z^n = \sum_n \lambda T^n \gamma z^n = \lambda(\sum_n T^n z^n)\gamma = \lambda(I - zT)^{-1}\gamma$. Mais

$$(I - zT)^{-1} = \frac{1}{det(I - zT)} \text{comatrice}(I - zT) \tag{33}$$

et les $Q(z) = det(I - zT)$ est un polynôme en z tel que $Q(0) = 1$ et comatrice(I-zT) est une matrice de polynômes en z (exercice !!). D'où le résultat.
i) $\Longrightarrow$ ii). —
On peut poser $Q(z) = \sum_{j=0}^{k-1} \beta_j z^j$ avec $\beta_0 = 1$. Comme $P = SQ$, pour tout $n \in \mathbb{N}$, on a $\langle P|z^n\rangle = \sum_{p+q=n} \beta_p a_q$, soit, si $n > N = max(\deg(P),k)$, $\sum_{p+q=n} \beta_p a_q = 0$ ce qui peut encore s'écrire $a_n = -\sum_{j=1}^{k} \beta_j a_{n-j}$, ce qui donne, pour tout $n \in \mathbb{N}$,

$$a_{n+N} = -\sum_{j=1}^{k} \beta_j a_{n+N-j} \tag{34}$$

ce qui entraine (ii). ♣

Définition 5.2 *Un triplet $\mathcal{T} = (\lambda,T,\gamma)$ tel que $\langle S|z^n\rangle = \lambda T^n \gamma$ est appellé* repésentation linéaire *de dimension n de S. De même S est appelée* comportement *de $\mathcal{T}$.*

Note 5.3 *Une série rationnelle admet en général plusieurs représentations linéaires. La dimension minimale de ces représentations est appellée* rang *de S. C'est aussi la dimension de l'espace vectoriel engendré par les décalées de S.*

5.5.1 Produit de Hadamard

C'est juste le produit des fonctions (fonctions "coefficient"), il sera noté $\odot$. Par exemple pour les séries d'une variable on a

$$\sum_{n=0}^{\infty} a_n z^n \odot \sum_{n=0}^{\infty} b_n z^n = \sum_{n=0}^{\infty} a_n b_n z^n \tag{35}$$

Exercice 5.4 *Effectuer les produits de Hadamard suivants*

a) $\frac{1}{1-z^2} \odot \frac{1}{1-2z}$ *b)* $\frac{1}{1+z+z^2} \odot \frac{1}{1-2z}$ *c)* $\frac{1}{1+z+z^2} \odot f(z)$

d) $\frac{1}{1-z^2} \odot e^z$ *e)* $\frac{z}{1-z^2} \odot e^z$ *f)* $\frac{1}{1-z} \odot f(z)$

Montrer que le résultat de (c) est rationnel si $f(z)$ est rationnelle i.e. si $f(z) = \frac{P(z)}{Q(z)}$; $Q(0) \neq 0$
indication. *— Pour le (b), décomposer en éléments simples. Pour le (c) on pourra remarquer que $\frac{1}{1+z+z^2} = \frac{1-z}{1-z^3}$.*

Théorème 5.5 PRODUIT DE HADAMARD DE SÉRIES RATIONNELLES. —
Soient $S,T \in \mathbb{C}[[z]]$ rationnelles. Alors $S \odot T$ est rationnelle.

Preuve — On peut remarquer qu'une série $R \in \mathbb{C}[[z]]$ est rationnelle ssi l'ensemble de ses décalées $(\gamma_z^*)^k R$ est de rang fini. Comme $\gamma_z^*(U \odot V) = \gamma_z^*(U) \odot \gamma_z^*(V)$, on a le résultat.

6 Génération aléatoire

6.1 Engendrer le hasard

Dès les premiers temps des ordinateurs, on les a appliqués à la simulation de phénomènes trop complexes pour être décrits exactement (on dit “bien modelisés”). Ils ont alors l’air d’être régis par le hasard (foudre, finance, météo).
La question est alors :
“Comment concevoir des générateurs de tirages automatiques qui soient équirépartis ?”
Notons qu’à partir de l’équirépartition on peut simuler les autres lois.

Exercice 6.1 *Soit une loi discrète donnée par un tableau*

k	$\cdots$	k_i	$\cdots$	k_n
$p(X=k)$	$\cdots$	p_i	$\cdots$	p_n

a) On suppose d’abord que $p_i = \frac{n_i}{d_i}$ et $d = ppcm(d_i)$, montrer comment simuler X avec un générateur équiréparti sur $[1..d]_N$.
b) Les p_i sont réels quelconques, expliquer sur un exemple (cf. la cible) pourquoi il vaut mieux utiliser les fractions continues pour approximer les p_i.

Le premier générateur de nombres aléatoires a été conçu selon la méthode du milieu du carré (middle square method), dont la recette est la suivante :
a) Prendre un nombre à 10 chiffres.
b) L’élever au carré.
c) Prendre les 10 chiffres du milieu.
Par exemple, avec le mini-programme suivant, on peut avoir la middle-square method.

```
>MSM:=proc(n)
local i,LL,S;
      LL:=convert(n^2,base,10);
      S:=0;
      for i from 6 to 15 do S:=S+LL[i]*10^(i-6) od;
      S
end;

>MSM(1234567890);
                    1578750190
>MSM(");
                    4521624250
>MSM(");
                    868581880
```

Question. — Comment évaluer les performances d’un tel générateur ?
La première idée est de faire une statistique sur un grand nombre de tirages.
La seconde est d’examiner les orbites.
ReponseSi le générateur est bon :
a) On met un certain temps avant de revoir une valeur (cf théorème de la période max).
b) Les tirages sont (semblent ??) indépendants (cf les générateurs à deux pas).

Exerc. Machine 6.2 *1) a) Faire 10^6 tirages par la* `MSM` *avec longueurs 3, 4, 8. Sont-ils équirépartis ?*
b) Faire calculer les orbites. Que constate-t-on dans ce cas ?

c) La situation s'améliore-t-elle quand on augmente la longueur ?
2) Quelles sont les plus petites périodes, les plus grandes, combien y a-t-il de cycles ?

6.2 Générateurs à un pas

Nous pouvons formaliser cette classe de générateurs comme suit.

Définition 6.3 *Soit F un ensemble fini, $x_0 \in F$ et $f : F \to F$ une application, On appelle générateur (à un pas) le triplet (F,f,x_0).*

Exemple 6.4 *A) Soit $E_{n+1} = [0,10^n - 1[$, l'ensemble des entiers à $n+1$ chiffres (écrits en base 10). On considère l'application f définie par les règles suivantes:*
1) Si $N = (a_n a_{n-1} \cdots a_0)_1 0$ est pair (i.e. si $a_0 = 0,2,4,6,8$) $f(N) = N/2$.
2 Sinon $f(N) = ((a_0 - 1)a_n a_{n-1} \cdots a_1)_1 0$.
On a par exemple, avec $n = 2;\ x_0 = 91$,

$$91 \to 09 \to 80 \to 40 \to 20 \to \mathbf{10} \to 05 \to 40 \to 20 \to \mathbf{10} \to \cdots$$

B) Soit m, un module. Considérer les générateurs à un pas avec $F = \mathbb{Z}/m\mathbb{Z}$ et f une fonction polynôme. Par exemple $x^2 + 1$.

Exerc. Machine 6.5 (EVELYN NELSON). — *On considère la fonction de transition suivante dans E_4 :*
i) Pour un nombre $N \in E_4$, $c(N)$ (resp. $d(N)$) désigne le réarrangement croissant (resp. décroissant) des chiffres de N.
ii) $f(N) = c(N) - d(N)$.
Soit C_4, l'ensemble des chiffres de la forme $k(1111)$ avec $0 \leq k \leq 9$ (ce sont les nombres qui ont leurs quatre chiffres égaux).
1) Montrer que $f(C_4) \subset C_4$ et que si $N \in E_4 - C_4$, on a $f(N) \in E_4 - C_4$.
On posera $D_4 = E_4 - C_4$.
2) Implémenter le générateur (x_0,f).
3) Faire la liste des cycles, que remarque-t-on ?

Exercice 6.6 *Faire dessiner les graphes de différentes fonctions.*

6.2.1 Paramètres

Les caractéristiques d'un générateur sont données par la proposition suivante :

Proposition 6.7 *Soit (F,f,x_0) un générateur à un pas. Alors :*
i) La suite $(x_n)_{n\geq 0}$ définie par

$$x_0;\ x_{n+1} = f(x_n)$$

est ultimement périodique, plus précisément,
ii) Il existe un plus petit indice μ dont la valeur est prise deux fois (indice d'entrée dans la période) et un plus petit entier λ (période) tel que, pour $n \geq \mu;\ k \geq 0$

$$x_n = x_{n+k\lambda}$$

L'ensemble des valeurs de la suite est $\{x_j\}_{0\leq j\leq \mu+\lambda-1}$

Voici l'exemple d'un petit programme qui calcule l'orbite d'un élément dans les entiers modulo N.

```
>orb1:=proc(x0,f,B)
local i,LL,x;
      x:=x0:LL:=NULL:
      for i to N while not member(x,LL) do LL:=LL,x: x:=f(x) od
      [LL,x]
end;
```

```
> f := x-> x^2+x+1 mopt41;
                        f := x-> x^2+x+1;
> orb1(0,f,41);
                        [0,1,3,13,19,12,34,2,7,16,27,19]
> orb1(5,f,41);
                        [5,31,3,9,9]
> orb1(8,f,41);
                        [8,32,32]
> orb1(11,f,41);
                        [11,10,29,10]
> orb1(14,f,41);
                        [14,6,2,7,16,27,19,12,34,2]
```

Les paramètres sont

x_0	0	5	8	11	14
μ	4	3	1	1	2
λ	7	1	1	2	7

L'orbite de 0 a une période de 7 son cycle est 19,12,34,2,7,16,27, à ce cycle se "raccrochent" d'autres branches, comme celle de l'orbite de 14 (14,6,$\mathbf{2}$,$\cdots$). L'orbite de 5 a une période de 1 (orbite apériodique).

Applications 6.8 *Pour la loi uniforme sur $[1,n]_{\mathbb{N}}$ une urne équitable a n boules peut bien faire l'affaire. Informatiquement, l'urne est remplacée par une fonction aléatoire du type* `rand()`. *Nous verrons le type de générateur comme en utilise Maple (c'est un générateur congruentiel linéaire, cf paragraphe suivant). Par exemple, on a :*

```
>rand(1000);
proc()
local t
global seed;
       seed:=irem(427419669081 *_seed,999999999989; t:=_seed;irem(t,1000)
end;
>_seed;
                        1
>rand(1000)();
```

```
                    81
>_seed;
                    427419669081
```

Noter que l'on obtient ainsi un "hasard faible" qui est, en général bon (voir toutefois les triplets [8]) pour la simulation parce qu'il est équiréparti (mais il n'est pas aléatoire)

Remarque 6.9 *La compréhension de ces paramètres est fondamentale et est à l'origine de nombreuses applications (notamment en factorisation : attaques de systèmes sécurisés du type RSA).*

Plus généralement, on a la notion de suite ultimement périodique.

Définition 6.10 *On dit qu'une suite x_n est ultimement périodique ssi il existe un certain rang N à partir duquel elle est périodique. Soit*

$$(\exists N)(\exists t > 0)(\forall n \geq N)(x_{n+t} = x_n)$$

Note 6.11 *Une telle suite peut donc se mettre sous la forme*

$$(\cdots (x_N, x_{N+1} \cdots x_{N+t-1})^\infty)$$

(comme $a(ba)^\infty$ par exemple), mais on constate qu'il y a une façon plus compacte que les autres de l'écrire sous cette forme (dans l'exemple précédent, c'est $(ab)^\infty$). Ceci détermine l'indice d'entrée dans le cycle et la période.

- paramètres
- opérations (produit cartésien,image)
- celles qui proviennent d'un G1P (rappel) et autres
- fonctions réversibles et orbites

Exercice 6.12 *La suite ultimement périodique $10(100)^\infty$ provient-elle d'un générateur à un pas ?*

Exerc. Machine 6.13 *1) a) Tester l'amplitude du générateur de hasard standard de Maple. Est-ce $[0..10^{12} - 11]_{\mathbb{N}}$, comme semble l'indiquer l'aide ?*
b) Avec cette connaissance, former un tirage aléatoire de Bernouilli à deux dimensions.
c) Expérimenter et comparer avec le tirage précédent.
2) Faire une statistique sur la `MSM` *pour $N = 2{,}3$ $(\lambda, n(\lambda))$ où $n(\lambda)$ est la nombre de points de départ qui aboutissent sur un cycle de longueur λ). (On aménagera la statistique de la façon la plus parlante possible en prenant par ex. λ dans des intervalles d'amplitude 100, et on raffinera certains intervalles.)*

Remarque 6.14 *L'image d'un générateur à un pas n'est pas toujours un générateur à un pas comme le montrent les exemples ci-dessous.*
i) Projection d'un générateur à deux pas :

$$\begin{pmatrix} x_{n+1} \\ x_{n+2} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x_n \\ x_{n+1} \end{pmatrix} \tag{36}$$

dans $(\mathbb{Z}/5\mathbb{Z})^2$ et la première projection.
On obtient la suite $[0,1,1,2,3,0,3,3,1,4,0,4,4,3,2,0,2,2,4,1]^\infty$, on observe que le retour d'une valeur n'entraine pas nécessairement le retour de la suivante.
ii) Cascade de congruences (technique utilisée par Maple) : On considère un générateur GCL1 $x_{n+1} = ax_n + b \text{ mopt } m$ de période maximale (cf le théorème (6.17)). On le réduit modulo une autre congruence ($m_1 < m$) par exemple on peut montrer (et l'observer à la machine) que, pour que le résultat $y_k \equiv x_k[m_1]$ est aussi ultimement périodique et de période λ_y qui divise $m = \lambda_x$. Mais pour que y_k soit équiréparti, il faut et il suffit que m_1 divise m. Pourquoi ? Expliquer alors pourquoi y_k provient d'un générateur à un pas.

Exercice 6.1 *A) Suites ultimement périodiques, méthodes de* BRENT, *de* FLOYD *[9] pp 308, 337, 346.*
B) Implémenter les différentes méthodes et comparer leurs performances sur les générateurs suivants:

$$\begin{aligned} x_{n+1} &= 3141692621x_n + 2718281829 \text{ mopt } 10^{10} \\ x_{n+1} &= x_n^2 + 5x_n + 1 \text{ mopt } 10^{32} \end{aligned}$$

6.2.2 Algorithmes de Brent et Floyd

Il est facile de déterminer les paramètres de la suite définie par un générateur à un pas lorsque celle-ci

- n'est pas trop longue
- est composée de nombres pas trop grands

mais, dans la pratique, on peut être amené à tester des suites de nombres de plus de 100 chiffres dont on ne sait pas la longueur de la période, il est alors hors de question de tout stocker, il faut se contenter de méthodes "locales" qui ne demandent de stocker, à chaque instant que deux valeurs. C'est le cas des algorithmes de Brent et Floyd.

Brent. —
On procède aux comparaisons suivantes:

x_0	x_1	$\cdots$	x_{2^k-1}	$\cdots$
x_1	x_2,x_3	$\cdots$	$x_{2^k}, \cdots x_{2^{k+1}-1}$	$\cdots$

jusqu'à ce que l'on trouve une coïncidence $x_{2^l-1} = x_m;\ m \in [2^l \cdots 2^{l+1} - 1]$. Ceci se produit forcément dès que $2^l - 1 \geq e$ (indice d'entrée dans le cycle, inconnu rappellons-le) et que $2^l \geq \lambda$. Soit donc $x_{2^l-1} = x_m;\ m \in [2^l, \cdots 2^{l+1} - 1]$, la coïncidence trouvée, on a $\lambda = m - (2^l - 1)$. Maintenant que l'on connait λ, on procède aux comparaisons

x_0	x_1	$\cdots$	x_k	$\cdots$
x_λ	$x_{\lambda+1}$	$\cdots$	$x_{\lambda+k}$	$\cdots$

la première a lieu pour $k = e$. L'étude de complexité de cet algorithme dépasse le cadre de ce cours, mais peut être trouvée dans [8, 9].

Floyd. —

On procède aux comparaisons suivantes

x_0	x_1	$\cdots$	x_d	$\cdots$
x_1	x_2	$\cdots$	x_{2k}	$\cdots$

la première coïncidence se produit pour le premier k multiple de λ qui dépasse e. L'indice k trouvé est un multiple de λ (mais pas nécéssairement λ), on procède alors aux comparaisons suivantes

x_0	x_1	$\cdots$	x_l	$\cdots$
x_d	x_{d+1}	$\cdots$	x_{d+l}	$\cdots$

la première conïncidence se produit pour $l = \mu$. On finit en déterminant λ par

x_μ	x_μ	$\cdots$	x_μ	$\cdots$
$x_{\mu+1}$	$x_{\mu+2}$	$\cdots$	$x_{\mu+k}$	$\cdots$

le premier k qui produit une égalité est $k = \lambda$.

6.2.3 Générateurs congruentiels linéaires

On appelle ainsi (en abr. GCL) les générateurs à un pas définis par $x_0;\ x_{n+1} = ax_n + b \operatorname{mopt} m$ où m est un module. Quand ils sont utilisés comme générateurs de hasard (benin) on cherche que leur période soit maximum (soit m). Voici quelques exemples donnés dans [9].

Exemple 6.15 *1)* $x_0 = 0;\ x_{n+1} = 4x_n + 1 \operatorname{mopt} 9$.
$(0 \to 1 \to 5 \to 3 \to 4 \to 8 \to 6 \to 7 \to 2 \to)^\infty$
2) $x_0 = 0;\ x_{n+1} = 2x_n + 1 \operatorname{mopt} 48$.
$0 \to 1 \to 3 \to 7 \to (15 \to 31 \to)^\infty$
3) $x_0 = 0;\ x_{n+1} = 3x_n + 1 \operatorname{mopt} 20$.
$(0 \to 1 \to 4 \to 12 \to)^\infty$
4) $x_0 = 0;\ x_{n+1} = 2x_n + 1 \operatorname{mopt} 5$.
$(0 \to 1 \to 3 \to 2)^\infty$ *et, si* $x_0 = 4$, $(4 \to)^\infty$
C'est ce type de générateur qu'utilisent les langages de programmation. Par exemple en Maple, on a:

```
>rand(1000);
proc()
local t
global seed;
       seed:=irem(427419669081 *_seed,999999999989; t:=_seed;irem(t,1000)
end;
>_seed;
                    1
>rand(1000)();
                    81
>_seed;
                    427419669081
```

Noter que l'on obtient ainsi un "hasard faible" qui est, en général bon (voir toutefois les triplets [8]) pour la simulation parce qu'il est équiréparti (mais il n'est pas aléatoire).

Exercice 6.16 *Vérifier la période du générateur précédent par* BRENT *et* FLOYD. *Comparer les performances de ces méthodes.*

On le théorème suivant qui indique comment fabriquer des générateurs de période maximale.

Théorème 6.17 *Pour qu'un GCL $x_{n+1} = ax_n + b \bmod m$ soit de période maximale il faut et il suffit que les conditions suivantes soient vérifées:*
a) b est inversible mopt m.
b) $a \equiv 1\ [p]$ pour tout p premier divisant m.
c) Si $4|m$ alors $a \equiv 1[4]$

Preuve —
Période maximale → Critère. —

- On a $x_n = a^n.x_0 + [n]_a.b$
- S'il y a une période maximale, elle passe par zéro. En posant $y_0 = x_{n_0} = 0$ on a $y_n = [n]_a.b$ et la période est max pour y_n, il existe n_1 tel que $[n_1]_a.b = 1$ d'où (a).
- Soit $p|m$, on a une projection $\mathbb{Z}_m \to \mathbb{Z}_p$, si la période est maximale dans $\mathbb{Z}_m$, c'est aussi la cas dans $\mathbb{Z}_p$ (on note $\mathbb{Z}_N$ une classe de restes modulo N, classique ou centrée par exemple).
- Si $a \not\equiv 1\ [p]$, on a, dans $\mathbb{Z}_p$, le point fixe $\frac{b}{1-a}$, ce qui est incompatible avec la période maximale, d'où (b).
- Si $4|m$, comme $a \equiv 1\ [2]$, on a $a \equiv 1{,}3\ [4]$. Si $a \equiv 3 \equiv -1\ [4]$, on a $x_{n+2} = -(-x_n + b) + b = x_n$, il n'y a donc pas de période maximale d'où (c).

Critère → Période maximale. —

- (Réduction du problème)
  1. Si $m = \prod p^{\alpha(p)}$, il suffit de démontrer que la période est maximale dans tous les $\mathbb{Z}_{p^\alpha}$
  2. Regardons le cycle de 0, qui est engendré par le générateur

     $$y_0 = 0; y_{n+1} \equiv a.y_n + b$$

     on a, comme précédement, $y_n \equiv [n]_a.b\ [m]$, et puisque b est inversible modulo m, il suffit de montrer que le critère entraine $[n]_a$ est de période m dans $\mathbb{Z}_m$.
- On montre que la période de $[n]_a$ est maximale à l'aide de l'identité

  $$[sq]_a = [s]_a.[q]_{a^s}$$

♣

Exerc. Machine 6.18 *Soit (F,f,x_0), un générateur. Au lieu d'une orbite, on peut vouloir tracer tout le graphe (la pieuvre) de f. Pour cela, il faut savoir "raccrocher" les éléments aux arbres qui se raccrochent aux cycles. La première méthode à laquelle on pense est de "scanner" les éléments non visités un par un. Mais, il est des cas (nous allons en voir deux) ou l'on peut créer un fonction antécédent qui prend un élément y et retourne l'ensemble des solutions de l'équation $y = f(x)$.*
1er Cas *: Les GCL à un pas $x_0;\ x_{n+1} = ax_n + b \bmod m$.*
1.1) $pgcd(a,m) = 1$ alors on calcule un inverse de a modulo m par la méthode de l'algorithme d'Euclide étendu qui donne les coefficients de Bezout $au+mv = 1$ `gcdex` *en Maple et MuPAD. On a donc $au \equiv 1$. Ainsi $y \equiv ax + b[m]$ est équivalent à $y - b \equiv ax$ et par multiplication par u, on a $u(y - b) \equiv x\ [m]$ solution unique.*
1.2) a et m ont des diviseurs communs. On calcule $d = pgcd(a,m)$ et par `gcdex` *on calcule des coefficients u,v tels que $au + mv = d$. Soit maintenant à résoudre $y \equiv ax + b[m]$. Il y a deux cas :*
1.2.1) $y - b \not\equiv 0[d]$ pas de solution en x et on se trouve à une feuille de l'arborescence.

1.2.2) $y - b = kd$ *alors, en posant* $a_1 = a/d$, $m_1 = m/d$ *on a, de manière équivalente,* $k \equiv a_1 x[m_1]$. *Comme* $pgcd(a_1,m_1) = 1$, *on est ramené au cas précédent.*

2ème Cas *: Les générateurs quadratiques du type* $x_{n+1} \equiv ax_n^2 + bx_n + c[p]$ *(*p *premier). Il faut résoudre* $y \equiv ax^2 + bx + c[p]$ *soit* $ax^2 + bx + (c-y) \equiv 0[p]$. *La discussion se fait classiquement par* $\Delta := b^2 - 4a.(c-y)$ *(voir le détail, utilisé dans les générateurs à deux pas (6.4.4)).*

6.3 Générateurs à deux pas

Q1 Si on voit sortir une suite ultimement pérodique d'une boîte noire, comment reconnaitre qu'elle provient d'un générateur à un pas ?
Q2 On constate que les "tirages" ne sont pas indépendants, peut-on améliorer cette situation ?
Q3 Comment appliquer BRENT et FLOYD au nouveau type de générateurs ?
Repartons de la suite $x_0,x_1;\ x_{n+2} = x_n + x_{n+1} \text{ mopt } 5$, c'est une suite périodique de période 20, telle qu'une valeur soit "fonction" des deux précédentes, ceci peut se formaliser de la façon suivante.

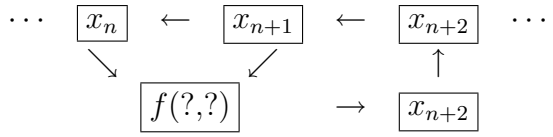
Définition 6.19 *Soit* F *un ensemble fini,* $x_0,x_1 \in F$ *et* $f : F^2 \to F$ *une application, On appelle générateur (à deux pas) le triplet* $(F,f,(x_0,x_1))$. *La suite associée au générateur est donnée par* $x_0,x_1;\ x_{n+2} = f(x_n,x_{n+1})$.

Exercice 6.20 *Montrer que la suite des "Fibonacci impairs"* $a_n = F_{2k-1}$ *vérifie la récurrence*

$$a_{n+2} = 3a_{n+1} - a_n$$

Exemple 6.21 *i) Soit* $F = \mathbb{Z}/7\mathbb{Z}$ $f(x,y) = x^2 + y$ *et* $(x_0,x_1) = (1,2)$ *On a la suite* $1 \to 2 \to 3 \to 0 \to 2 \to 2 \to -1 \to 3 \to 4 \to -1 \to 1 \to 2$
ii) $x_0 = 1$, $x_1 = 2$, $x_{n+2} \equiv 3x_n + x_{n+1} \text{mopt} 9$

Note 6.22 *En utilisant la notation d'un "linear shift register" (utilisés abondamment en codage), on a*



Exercice 6.23 *i) Faire tourner* BRENT *et* FLOYD *sur des générateurs quadratiques du type de (6.18).*
ii) Faire tourner BRENT *et* FLOYD *sur les générateurs suivants (a,b=main; c,d=machine).*
a) $(x_0,x_1) = (0,1)$ $x_{n+2} \equiv 2(x_n + x_{n+1})$ [16] *b)* $(x_0,x_1) = (1,1)$ $x_{n+2} \equiv x_n^2 + x_{n+1})$ [13]
c) $(x_0,x_1) = (1,1)$ $x_{n+2} \equiv x_n^2 + x_{n+1}^2)$ [103] *d)* $(x_0,x_1) = (1,1)$ $x_{n+2} \equiv x_n^{(x_{n+1})}$ [1001]

La vectorisation (qui consiste à considérer la suite (x_n,x_{n+1})) permet de ramener l'étude d'un générateur à deux pas à celle d'un générateur à un pas.

6.3.1 Vectorisation et paramètres

Proposition 6.24 *i) La suite engendrée par un générateur à deux pas* $(F,f,(x_0,x_1))$ *est la première projection de la suite engendrée par le générateur à un pas* $(F^2,g,(x_0,x_1))$ *où* g *est donnée par* $g(x,y) = (y,f(x,y))$. *En particulier :*
ii) Cette suite est ultimement périodique, ses paramètres sont ceux de la suite "vectorisée" $((x_n,x_{n+1}))_{n\geq 0}$.

Remarque 6.25 *i) Le résultat précédent permet d'appliquer les algorithmes de* BRENT *et* FLOYD *aux générateurs à deux pas.*
ii) Avec les notations de Mupad, en notant $c := (x,y)$*, on aurait*

```
g(c)=(op(c,2),f(op(c,1),op(c,2)))
```

Exemple 6.26 *La suite de Fibonacci dans* $\mathbb{Z}/5\mathbb{Z}$ *se vectorise en*

$$\begin{pmatrix} x_0 \\ x_1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}; \begin{pmatrix} x_{n+2} \\ x_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_{n+1} \\ x_n \end{pmatrix} \tag{37}$$

(voir remarque (6.14)).
En utilisant le produit par blocs on a que

$$\begin{pmatrix} x_{n+1} & x_n \\ x_{n+2} & x_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$$

ce qui prouve que la période est celle de $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ *(modulo 5) et que l'indice est* 0.

Un exemple dont on maîtrise les paramètres est celui des générateurs linéaires à deux pas (GL2P), dont la fonction de transition est $f(x,y) = ax + by$. Par exemple, la suite de Fibonacci modulo p $F_0 = 0, F_1 = 1;\ F_{n+2} = F_n + F_{n+1} \bmod p$ (en faire l'étude).

6.4 Générateurs du type GL2P

6.4.1 Généralités

La suite fournie par un GL2P est donnée par

$$\begin{cases} x_0, x_1 \\ x_{n+2} = ax_n + bx_{n+1} \quad (\mathrm{RL2}) \end{cases}$$

la relation (RL2) s'appelle récurrence linéaire d'ordre deux.
À cette récurrence est attachée une l'équation $r^2 = a + br$ appellée équation caractéristique et qui provient de la considération suivante

Proposition 6.27 *Pour qu'une suite de puissances* $(r^n)_{n\geq 0}$ *(suite géométrique de premier terme* 1*) vérifie RL2, il faut et il suffit qu'elle la vérifie pour* $n = 0$*, soit*

$$r^2 = a + br \tag{38}$$

Pour concevoir des générateurs efficaces, il faut pouvoir les paramétrer de façon qu'ils aient une grande période. Pour cela il est nécéssaire de les décomposer en "petits" générateurs dont on maîtrise la période. Ce seront les suites $(r^n)_{n\geq 0}$ et $(nr^n)_{n\geq 0}$.

6.4.2 Combinaison de deux générateurs

La suite $(r^n)_{n\geq 0}$ mopt$p$ est produite par un GL1P et $(nr^n)_{n\geq 0}$ mopt$p$ est produite par un GL2P.

Proposition 6.28 *i) Soit $m > 0$ un entier et α,β,r_1,$r_2 \in \mathbb{N}$ alors la suite de nombres $(\alpha r_1^n + \beta r_2^n)_{n\geq 0}$ est produite par le générateur*

$$\begin{cases} \alpha+\beta, \alpha r_1+\beta r_2 \\ x_{n+2} = (r_1+r_2)x_{n+1} - (r_1 r_2)x_n \quad \text{(RL2)} \end{cases}$$

ii) Dans les mêmes conditions que précedemment, la suite de nombres $(\alpha r^n + \beta n r^n)_{n\geq 0}$ est produite par le générateur

$$\begin{cases} \alpha+\beta, \alpha r_1+\beta r_2 \\ x_{n+2} = 2r x_{n+1} - (r^2)x_n \quad \text{(RL2)} \end{cases}$$

Remarque 6.29 *En fait, il suffit de remarquer que, dans les deux cas, l'équation caractéristique doit avoir r_1,r_2 comme racines ($r = r_1 = r_2$) dans le deuxième cas. Celle-ci est alors $(r - r_1)(r - r_2) = 0$.*

6.4.3 Décomposition et calcul de la période d'un GL2P ($m = p$ premier).

Voici comment on procède:

1. On résout si possible l'équation caractéristique
2. On combine les résultats de façon à trouver les mêmes conditions initiales.

Par exemple pour Fibonnacci, on trouve $r = 3$ comme solution unique pour $m = p = 5$. L'équation caractéristique est $r^2 = 1 + r$ et ses racines dans différents "moduli" sont ($\{\} = \emptyset$ signifie qu'il n'y a pas de racine). On peut montrer d'ailleurs que les seuls p premiers tels que l'équation ait des racines sont de la forme $10k \pm 1$.

p	3	5	7	11	13	17	19	23	29	31	37	41
r	$\{\}$	$\{3\}$	$\{\}$	$\{4,8\}$	$\{\}$	$\{\}$	$\{5,15\}$	$\{\}$	$\{6,24\}$	$\{9,13\}$	$\{\}$	$\{7,35\}$

Dans le cas où il y a deux racines distinctes r_1,r_2 il existe toujours des coefficients u,v tels que l'on ait les deux premiers termes de le suite analysée soit $x_k = ur_1^k + vr_2^k;\ k = 0,1$ en ce cas la relation précédente reste vraie pour tout k.
Dans le cas où il n'y a qu'une racine r, il existe toujours des coefficients u,v tels que l'on ait les deux premiers termes de le suite analysée soit $x_k = (uk + v)r^k;\ k = 0,1$ en ce cas la relation précédente reste vraie pour tout k.
On peut énoncer :

Proposition 6.30 *i) Dans le cas où l'équation caractéristique admet deux racines distinctes r_1,r_2 il existe toujours des coefficients u,v tels que l'on ait les deux premiers termes de le suite analysée soit*

$$x_k = ur_1^k + vr_2^k;\ k = 0,1$$

en ce cas la relation précédente reste vraie pour tout k.
ii) Dans le cas où l'équation caractéristique n'admet qu'une racine r il existe toujours des coefficients u,v tels que l'on ait les deux premiers termes de le suite analysée soit $x_k = (uk + v)r^k;\ k = 0,1$ en ce cas la relation précédente reste vraie pour tout k.
iii) Les couples (u,v) déterminés précédemment sont uniques.

Nous ne traitons pas cette année le cas où il n'y a pas de racine. Voyons maintenant, avec plus de détails, la technique utilisée pour résoudre les équations du second degré modulo p (premier impair).

6.4.4 Carrés et équations du second degré dans $\mathbb{F}_p$

L'équation du second degré dans $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p;\ p \neq 2$ se discute comme dans le cas classique (i.e. réel) en tenant compte des carrés. *Dans tout ce paragraphe, p désigne un nombre premier $\neq 2$.*

Proposition 6.31 *L'équation du second degré $ax^2 + bx + c = 0;\ a \neq 0$ se discute et résout selon le discriminant $\Delta = b^2 - 4ac$.*
i) Si $\Delta = \delta^2$ est un carré dans $\mathbb{F}_p$ alors l'équation admet les racines

$$\frac{-b-\delta}{2a};\ \frac{-b+\delta}{2a}$$

ii) Si Δ n'est pas un carré, l'équation n'a pas de solution.

Remarque 6.32 *Si $\Delta = 0$, les deux racines du cas (i) se confondent en une racine dite double $\frac{-b}{2a}$.*

Les carrés se calculent sur la "première moitié" de $\mathbb{F}_p$.

Proposition 6.33 *L'application donnée par $x- > x^2$ définit une bijection entre $[0..\frac{p-1}{2}]$ et l'ensemble des carrés de $\mathbb{F}_p$.*

$p=$	3			5				7					11						
			2			4	3			6	5	4			10	9	8	7	6
	x	0	1	x	0	1	2	x	0	1	2	3	x	0	1	2	3	4	5
	x^2	0	1	x^2	0	1	4	x^2	0	1	4	2	x^2	0	1	4	2	5	3

Exercice 6.34 *Résoudre et discuter dans $\mathbb{Z}/p\mathbb{Z}$:*
a) $x^2 + x + 1 = 0;\ p = 11,23,31$ *b)* $x^2 + 4x + 2 = 0;\ p = 17,29$
c) $x^2 + mx + 1 = 0;\ p = 7,11,13$ *d)* $x^3 + 1 = 0;\ p = 19,23$
e) $x^4 = m;\ p = 29,31$ *f)* $x^4 + x^2 + 1 = 0;\ p = 11,23,31$

6.4.5 Calcul de la période d'un GCL2

Rappelons ici la discussion.
La suite fournie par un GL2P est donnée par

$$\begin{cases} x_0,x_1 \\ x_{n+2} = \alpha x_{n+1} + \beta x_n \quad \text{(RL2)} \end{cases}$$

la relation (RL2) s'appelle récurrence linéaire d'ordre deux.
Voici comment on procède :

1. On résout si possible l'équation caractéristique
2. On combine les résultats de façon à trouver les mêmes conditions initiales.

Exercice 6.35 *i) ($p = 5$) Résoudre et discuter les 25 équations*

$$r^2 = \alpha r + \beta$$

pour $(\alpha,\beta) \in \mathbb{F}_5$ (essayer de regrouper des cas, voir des symétries etc..)
ii) Constater que si on tire les paramètres $(\alpha,\beta) \in \mathbb{F}_5^2$ "au hasard" (équidistribué), la probabilité que l'équation(38) ait $0,1,2$ racines est :

Nb. rac.	*0*	*1*	*2*
Proba.	$\frac{2}{5}$	$\frac{1}{5}$	$\frac{2}{5}$

iii) (Cas général) On considère maintenant $p \neq 2$ quelconque et on tire les paramètres $(\alpha,\beta) \in \mathbb{F}_p^2$ au hasard (équidistribué). Montrer que la probabilité que l'équation(38) ait $0,1,2$ racines est :

Nb. rac.	*0*	*1*	*2*
Proba.	$\frac{p-1}{2p}$	$\frac{1}{p}$	$\frac{p-1}{2p}$

iv) Faire des expériences machine sur différentes valeurs de p.
a) Exhaustives : examiner **tous** *les couples (α,β).*
b) Aléatoires (grandes valeurs de p) : utiliser un générateur de hasard.

On rappelle que, pour p premier, un élément non nul $g \in \mathbb{Z}/p\mathbb{Z}$ vérifie toujours $g^{p-1} = 1$ (Fermat). Mais il peut y avoir des puissances plus petites. Le plus petit $k > 0$ telle que $g^k = 1$ est appellé l'ordre de g. Voici à titre d'exemple les ordres des $g \neq 0$ dans $\mathbb{Z}/19\mathbb{Z}$.

g	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
ord(g)	1	18	18	9	9	9	3	6	9	18	3	6	18	18	18	9	9	2

Les périodes sont données par la tableau suivant:

racines		$x_n =$	période
0 est rac. ou $0 \in \{u,v\}$		$(x_n)_{n\geq 1}$ vient d'un GCL1.	
$r_1,r_2 \neq 0$	$r_1 \neq r_2$	$x_n = ur_1^n + vr_2^n$	$ppcm(ord(r_1),ord(r_2))$
$u,v \neq 0$	$r_1 = r_2 = r$	$x_n = (un+v)r^n$	$p \times ord(r)$

Par exemple, pour Fibonacci mod 5, on a

$$x_n \equiv 3^n + n.3^n \text{mopt} 5$$

ce qui explique la période de $20 = 5.4$. Pour Fibonacci modulo 11, on a

$$x_n \equiv 10 * 4^n + 2 * 8^n \equiv -4^n + 2 * 8^n \text{mopt} 11$$

ce qui explique la période de 10 car $ord(4) = 5;\ ord(8) = 10$

Exercice 6.36 *a) Concevoir un programme qui donne les ordres des éléments modulo p.*
b) Faire, pour différentes valeurs de p, la statistique $p \to$ `(maxord(p),numaxord(p))` *où* `maxord` *est l'ordre maximal et* `nummaxord` *est le nombre des éléments d'ordre maximal. Que remarque-t-on ?*

La notion de générateur a déjà été utilisée pour RSA, nous la rappellons ici.

Proposition/Definition 6.37 *i) Pour tout p premier, il existe des éléments $g \in \mathbb{Z}_p$ tels que*

$$\mathbb{Z}_p - \{0\} = \{g^k\}_{0 \leq k \leq p-2} = \{1, g, g^2, g^3, \cdots g^{p-2}\}$$

c'est à dire que les puissances de g décrivent tous les éléments non-nuls.
ii) De tels éléments (exactement ceux qui sont d'ordre maximal soit $p-1$) sont appellés génŕateurs.
iii) (Calcul de l'ordre d'un élément quelconque) Si g est un générateur, on a

$$ord(g^k) = \frac{p-1}{pgcd(k, p-1)}$$

la conclusion de cette étude est que la période d'un générateur à deux pas avec solutions de l'EC est : soit un diviseur de $p-1$ (cas où il y a deux racines), soit $p \times ord(r)$ (cas où il n'y a qu'une seule racine r) et donc la plus longue période réalisable avec un générateur "à racine(s)" est $p(p-1)$. On verra aussi que la plus longue période d'un générateur "sans racine" est $p^2 - 1$. Soit pour les premiers nombres premiers $\neq 2$

p	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$p(p-1)$	6	20	42	110	156	272	342	506	812	930	1332	1640	1806	2162
p^2-1	8	24	48	120	168	288	360	528	840	960	1368	1680	1848	2208

6.5 Autres générateurs

Knuth donne dans [8] (p26), un générateur de D.J. Mitchell et D.P Moore

$$X_n = (X_{n-24} + X_{n-55}) \text{ mopt } m$$

où les termes initiaux $X_0 \cdots X_{54}$ sont des entiers arbitraires non tous pairs. Il a pour période $2^f(2^{55}-1)$ pour $m = 2^e$ et $0 \leq f < e$ (cf [8] p34 Ex. 11) et se programme à l'aide d'une liste cyclique à 55 pas.

6.6 Généateurs à k pas

6.7 Énumérer, classer, indexer

6.8 Répartitions équitables et moins équitables

7 Systèmes et Calcul

7.1 Introduction

Exemples d'automates booléens, stochastiques, de comptage, de plus courts chemins. Les semi-anneaux associés sont : $\mathbb{B}$, $\mathbb{R}_+$,$\mathbb{N}$,$([0, +\infty], min, +)$.

7.2 Description de la structure d'automate

7.2.1 Graphe pondéré

L'élément de base de ces graphes est la flêche $A = q_1 \xrightarrow{a|\alpha} q_2$ avec $q_i \in Q$, $a \in \Sigma$, $\alpha \in k$ où Q est un ensemble d'états, Σ un alphabet et k, un semi-anneau[5]. Pour un tel objet, on définit, selon les conventions générales de la théorie des graphes,

- $t(A) := q_1$ ("tail": queue, source, origine)
- $h(A) := q_2$ ("head" tête, but, extrémité)
- $l(A) := a$ ("label" étiquette)
- $w(A) := \alpha$ ("weight" poids).

Un *chemin* est une suite d'arêtes $c = A_1 A_2 \cdots A_n$ (c'est un mot en les arêtes et sa longueur est n) telle que $h(A_k) = t(A_{k+1})$ pour $1 \leq k \leq n-1$ pour un tel chemin $t(c) = t(A_1)$, $h(c) = h(A_n)$, $l(c) = l(A_1)l(A_2)\cdots l(A_n)$ (concaténation), $w(c) = w(A_1)w(A_2)\cdots w(A_n)$ (produit dans le semi-anneau).
Par exemple pour le chemin de longueur 3 suivant ($k = \mathbb{N}$),

$$u = p \xrightarrow{a|2} q \xrightarrow{b|3} r \xrightarrow{c|5} s \tag{39}$$

on a $t(u) = p$, $h(u) = s$, $l(u) = abc$, $h(u) = 30$.
Le poids d'un ensemble de chemins de même source, but et étiquette est la somme des poids des chemins de cet ensemble. Ainsi, si

$$\mathbf{q}1 \quad \overset{\xrightarrow{u|\alpha}}{\underset{\xrightarrow{u|\beta}}{}} \quad \mathbf{q}2 \tag{40}$$

le poids de cet ensemble de chemins est $\alpha + \beta$. On a donc que les poids se multiplient en série et s'aditionnent en parallèle. Les diagrammes suivants montrent la nécessité des axiomes de semi-anneau.

Diagramme	Identité	Nom
$p \overset{\xrightarrow{a\|\alpha}}{\underset{\xrightarrow{a\|\gamma}}{\xrightarrow{a\|\beta}}} q$	$\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$	Associativité de $+$
$p \overset{\xrightarrow{a\|\alpha}}{\underset{\xrightarrow{a\|\beta}}{}} q$	$\alpha + \beta = \beta + \alpha$	Commutativité de $+$
$p \overset{\xrightarrow{a\|\alpha}}{\underset{\xrightarrow{a\|0}}{}} q$	$\alpha + 0 = \alpha$	Élément neutre (droite) de $+$
$p \xrightarrow{a\|0} q \xrightarrow{b\|\beta} r$	$0 + \beta = \alpha$	Élément neutre (gauche) de $+$
$p \xrightarrow{a\|\alpha} q \xrightarrow{b\|\beta} r \xrightarrow{c\|\gamma} s$	$\alpha(\beta\gamma) = (\alpha\beta)\gamma$	Associativité de $\times$
$p \overset{\xrightarrow{a\|\alpha}}{\underset{\xrightarrow{a\|\beta}}{}} q \xrightarrow{b\|\gamma} r$	$(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma$	Distributivité (droite) de $\times$ sur $+$
$p \xrightarrow{a\|\alpha} q \overset{\xrightarrow{b\|\beta}}{\underset{\xrightarrow{b\|\gamma}}{}} r$	$\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$	Distributivité (gauche) de $\times$ sur $+$
$p \xrightarrow{a\|\alpha} q \xrightarrow{b\|1_k} r$	$\alpha \times 1_k = \alpha$	Élément neutre (droite) de $\times$
$p \xrightarrow{a\|1_k} q \xrightarrow{b\|\beta} r$	$1_k \times \beta = \beta$	Élément neutre (gauche) de $\times$

5. Nous verrons plus bas que les axiomes de la structure de semi-anneau sont contraints par la définition même du système de transitions ainsi obtenu.

7.2.2 Structure et comportement des automates

Un automate à poids ou pondéré (“automaton with weights”) est la donnée de trois éléments vectoriels (I,M,T):

$$\begin{cases} \bullet \text{ Un vecteur d'entrée } I \in k^{1\times Q} \\ \bullet \text{ Une famille (indexée à A) de matrices de transition } M : A \to k^{Q\times Q} \\ \bullet \text{ Un vecteur de sortie } T \in k^{Q\times 1} \end{cases}$$

La donnée des transitions (M) est équivalente à celle d’un graphe pondéré dont les sommets sont Q, l’alphabet A et les poids sont pris dans k. De plus celle de I (resp. T) correspond à la donnée de flêches rentrantes (resp. sortantes) marquées avec des poids. Dans tout ce processus, on peut ne pas indiquer les flêches de poids nul.
Ce type d’automates généralise les automates (booléens) de la théorie des langages (que l’on obtient alors pour $k = \mathbb{B}$) est une machine qui prend un mot en entrée et retourne un coefficient (dans k) en sortie. Son comportement est donc une fonction $\mathcal{A} : \ A^* \to k$ (que l’on peut noter, de manière équivalente, comme une série $\mathcal{A} = \sum_{w\in A^*} \mathcal{A}(w)w$).

Calcul du poids $\mathcal{A}(w)$. —
On étend d'abord la fonction de transition M à A^* par

$$M(\epsilon) = I_{Q\times Q},\ M(w) = M(a_1a_2\cdots a_n) = M(a_1)M(a_2\cdots M(a_n) \tag{41}$$

où $I_{Q\times Q}$ est la matrice identité de format $Q \times Q$. Le calcul du poids d'un mot est alors, par définition,

$$\mathcal{A}(w) := IM(w)T \tag{42}$$

d'après la règle de multiplication des matrices, on a bien que $IM(w)T$ est une matrice de format 1×1 et donc un élément de k. Le lien avec le graphe de l'automate est donné par la proposition suivante :

Proposition 7.1 *Soit, pour deux états r,s et un mot $w \in A^*$*

$$\mathcal{A}^{r,s}(w) := I_r \left(\sum_{\substack{c,\ \text{chemin}\ l(c)=w \\ t(c)=r,\ h(c)=s}} weight(c) \right) T_s \tag{43}$$

alors

$$\mathcal{A}(w) = \sum_{r,s\in Q} \mathcal{A}^{r,s}(w) \tag{44}$$

Cette proposition a le sens intuitif suivant :

1. l'équation (43) donne le poids calculé comme au paragraphe précédent
   - on fait le bilan parallèle (c'est à dire une somme) des poids des chemins qui joignent r à s
2. on multiplie (à gauche si c'est non commutatif) par le poids d'entrée en r
3. on multiplie (à droite si c'est non commutatif) par le poids de sortie en s

7.2.3 Premiers automates

1. Longueur totale $\sum_{w\in A^*} |w|w$
2. Comptage des a, $\sum_{w\in A^*} |w|_a w$ et des b, $\sum_{w\in A^*} |w|_b w$
3. Produit des degrés partiels $\sum_{w\in A^*} |w|_a|w|_b w$
4. Autres produits $\sum_{w\in A^*} F_{|w|}|w|w$, $\sum_{w\in A^*} F_{|w|_a}|w|_b w$

Fin du tronc commun

7.2.4 Composition des automates

Somme et multiplication par un coefficient constant

Produit de Hadamard

Produit (de concaténation)

Nous avons vu que nous pouvions coder de "l'infini dans du fini" en considérant les suites ultimement périodiques que sont les développements illimités des rationnels. Nous allons voir

qu'il en est de même pour la production des automates finis, en effet, un automate fini, dès qu'il possède un chemin réussi qui comporte un boucle, reconnaît un langage infini.

Exercice 7.2 *Montrer que cette condition est suffisante, autrement dit, si aucun chemin réussi ne comporte de boucle, alors le langage reconnu par l'automate est fini.*

Commençons par un exemple : On considère un automate (booléen), d'ensemble d'états Q et dont les transitions sont étiquetées par un alphabet A. Cet automate, via la correspondance (graphes $\leftrightarrow$ matrices) peut être vu comme un triplet (I,T,M) avec :

$$\begin{cases} \bullet \text{ Un vecteur d'entrée } I \in k^{1\times Q} \\ \bullet \text{ Une famille de matrices de transition } M : A \to k^{Q\times Q} \\ \bullet \text{ Un vecteur de sortie } T \in k^{Q\times 1} \end{cases}$$

Dans les automates usuels, les scalaires sont pris dans $\{0,1\}$. Si on considère ces nombres comme des entiers naturels, l'opération $w \to IM(w)T$ donne le nombre de chemins réussis. Une expression rationnelle du comportement de l'auromate (tenant compte des multiplicités) résulte du calcul suivant

$$\sum_{w\in\Sigma^*} (IM(w)T)w = I(\sum_{w\in\Sigma^*} M(w)w)T = I(Id_n - \sum_{a\in\Sigma} M(a)a)^{-1}T$$

si on note $M_\Sigma = \sum_{a\in\Sigma} M(a)a$, on a $M_\Sigma^* = (Id_n - \sum_{a\in\Sigma} M(a)a)^{-1}$. C'est la matrice dont l'entrée d'adresse (i,j) est la somme

$$\sum_{\substack{w \text{ étiquette} \\ \text{un chemin de } i \text{ vers } j}} (\text{nb de chemins } i \to j \text{ d'étiquette } w)w$$

par exemple la matrice

$$M_\Sigma = \begin{pmatrix} a & a \\ b & 0 \end{pmatrix}$$

a pour étoile

$$M_\Sigma^* = \begin{pmatrix} (a+ab)^* & (a+ab)^*a \\ b(a+ab)^* & (ba^*a)^* \end{pmatrix}$$

il est facile de voir que les séries associées sont sans multiplicité (i.e. pour (i,j) et w donnés il existe au plus un chemin d'étiquette w), mais ce n'est pas le cas pour

$$Q_\Sigma = \begin{pmatrix} a & a \\ b & a \end{pmatrix}$$

qui a pour étoile

$$Q_\Sigma^* = \begin{pmatrix} (a+aa^*b)^* & (a+aa^*b)a^*a \\ a^*b(a+aa^*b)^* & (a+ba^*a)^* \end{pmatrix}$$

Exercice 7.3 *1) Dessiner les automates (sans vecteurs d'entrée et sortie) associés aux matrices M_Σ,Q_Σ.*
2) a) Montrer, en utilisant un raisonnement sur les chemins dans un graphe étiqueté convenable, que pour deux lettres, on a $(a+b)^* = (a^*b)a^*$ (élimination de Lazard monoïdale).
b) Appliquer cette identité pour trouver une autre forme de $(a+aa^*b)^*$.
c) Montrer que $a^*aa^* = a\frac{1}{(1-a)^2} = \sum_{n\geq 1} na^n$.

d) Si un mot ne se termine pas par b, sa multiplicité dans $(a^*aa^*b)^*$ est nulle, mais s'il s'écrit $w = a^{n_1}ba^{n_2}b\cdots a^{n_k}b$, on a $(w,(a^*aa^*b)^*) = n_1 + n_2 + \cdots n_k$. En déduire le développement (i.e. les multiplicités des mots) de $(a^*aa^*b)^*a^*$, puis des 4 coefficients de la matrice Q_Σ^*.
3) a) Soit l'alphabet à quatre lettres $\Sigma = \{a_{11},a_{12},a_{21},a_{22}\}$, montrer directement en raisonnant sur les chemins, que si $G = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ on a

$$G^* = \begin{pmatrix} A_{11} & A_{11}a_{12}a_{22}^* \\ a_{22}^*a_{21}A_{11} & A_{22} \end{pmatrix};\ A_{11} = (a_{11} + a_{12}a_{22}^*a_{21})^*,\ A_{22} = (a_{22} + a_{21}a_{11}^*a_{12})^*$$

b) Expliquer en quoi ces formules fournissent un algorithme permettant de calculer l'étoile de toute matrice de séries propres.

Exemple 7.4 *Soit L_n le langage fini formé des mots w tels que $|w|_a + 2|w|_b = n$.*
a) Écrire les premiers termes $L_0,L_1,L_2\cdots$.
b) Calculer $|L_n|$ à l'aide d'une récurrence simple.
c) Montrer que $SG = \sum_n |L_n|t^n = (t + t^2)^* = \frac{1}{1-t-t^2}$.
*d) Faire le lien avec le nombre de pavages d'un rectangle $2 \times n$ par des dominos 2×1 ([**?**] pp 321) comment coder les pavages, les énumérer, les générer.*
e) À l'aide des décalages, former l'automate qui reconnait la série S.

On a un analogue parfait de ce qui se passe pour les rationnels positifs. Plus précisément :

Exercice 7.5 *A) On considère les arbres $1-2$ qui sont les arbres à 1 ou deux fils.*
À chaque arbre $1-2$, dont les noeuds internes sont signés par "$+$" s'ils ont deux fils et "$()^{-1}$" s'ils en ont un on fait correspondre une fraction (i.e. son évaluation avec les feuilles en 1) donnée par la règle récursive

$$ev(\bullet) = 1;\ ev((\mathcal{A}_1,\mathcal{A}_2)) = ev((\mathcal{A}_1) + ev(\mathcal{A}_2);\ ev((\mathcal{A})) = \frac{1}{ev(\mathcal{A})}$$

montrer que l'ensemble des valeurs obtenues est $\mathbb{Q}_+^*$. Est-ce que la représentation est unique ? Est-ce qu'elle englobe les fractions continues ? Comment caractériser les arbres qui les donnent ?
B) On considère les séries sur un alphabet A (i.e. fonctions $A^* \to k$ où k est un semi-anneau (i.e. suffisant pour faire la calcul matriciel).
a) Montrer que les conditions suivantes sont équivalentes :
i) La série S est l'évaluation d'une expression rationnelle.
ii) La série S est combinaison linéaire d'un ensemble de séries $S_1,S_2,\cdots S_n$ qui est (linéairement) stable par décalages soit

$$(\forall x \in A)(\forall i \in [1..n])(x^{-1}S_i = \sum_{0\le j\le n} \mu_{i,j}(x)S_j$$

iii) Il existe $\lambda \in K^{1\times n}$, $\mu : A \to K^{n\times n}$,$\gamma \in K^{1\times n}$ tels que pour tout $w \in A^*$, $(S,w) = \lambda\mu(w)\gamma$ (où $\mu()$ dénote encore l'extention de μ à A^*).

Lorsque l'on a une partie $X \in A^*$, on peut se demander :
Quel est le langage $L(X)$ engendré par X ?
c'est à dire les suites finies d'instructions (i.e. le sous-monoïde engendré). On a $L(X) = \sum_{n\ge 0} X^n$ à coefficients dans $\mathbb{B}$. La même somme à coefficients dans $\mathbb{N}$ contient plus d'informations (soit le nombre de façons d'obtenir w comme produit de facteurs dans X).

Automates. Automates à multiplicité (notion de coût). Comportement d'un automate. Séries (exemples), rationnelles.
Passage SGO $\leftrightarrow$ Aut $\leftrightarrow$ Exp. rat.
Exemples de $\mathbb{N}$ et $\mathbb{Z}$ automates.
Séries génératrices (rationnelles -arbres de Fibonacci- et non rationnelles -arbres binaires, chemins de Dyck-). Résolution des premières récurrences, décalage et Δ. Complexité du comptage des boucles. Arbres $1-2$.

7.3 Séries

7.3.1 Exemple : Comportement d'un automate

7.3.2 Opérations sur les séries

7.3.3 Lien avec les grammaires et les structures de données

7.3.4 Énumération

7.3.5 Rudiments de Calcul Modulaire

8 Fonctions génératrices (approfondissement)

8.1 Une variable

8.2 Application au calcul de complexité

8.3 Plusieurs variables

9 TD et TP (E. Laugerotte & J-P. Dubernard)

MI-MIM TD1 Calcul Formel 2002/2003

Exercice 1 On considère les expressions arithmétiques suivantes :

- $x * (y + z) * (-2)$
- $2 * x/y * z^4$
- $x \wedge (y \wedge z)$

1) Construire les arbres associés. CF

2) À l'aide des fonctions **whattype**, **nops**, **op** de Maple, confirmer et en déduire les types.

3) À l'aide de la fonction **subs** de Maple, remplacer x par $2 * x1 + x2$ dans les expressions précédentes.

Exercice 2 À l'aide des fonctions **whattype**, **nops**, **op** de Maple, donner l'arbre et le type associé à $22/7$ et à 32.6789.

Exercice 3 (Suite de Fibonacci) Soit (F_n) la suite définie par

$$\begin{cases} F_0 = 0, \\ F_1 = 1, \\ F_{n+2} = F_{n+1} + F_n \quad \forall n \in \mathbb{N}. \end{cases}$$

1) Écrire une procédure récursive Maple efficace calculant F_n.

2) Calculer F_n en fonction de n. Pouvez-vous en déduire une nouvelle procédure ? Est-elle plus performante ?

3) Montrer que, pour tout entier n,

$$F_{n+1}^2 - F_n F_{n+2} = (-1)^n.$$

4) Montrer que, pour tout entier n,

$$F_{n+m} = F_m F_{n+1} + F_{m-1} F_n,$$

puis en déduire que

$$\text{pgcd}(F_n, F_m) = F_{\text{pgcd}(n,m)}.$$

Exercice 3 (Algorithme d'Euclide)

1) Écrire une procédure Maple rendant le PGCD de deux nombres entiers naturels a et b.

2) En supposant connu le théorème de Dirichlet qui dit que la probabilité pour que deux entiers positifs u et v soient premiers est de $\frac{6}{\pi^2}$, écrire une procédure qui calcule efficacement le PGCD de plusieurs entiers.

Exercice 4 (Théorème de Lamé) On suppose que a et b sont deux entiers naturels tels que $a > b > 0$.

1) Si l'algorithme d'Euclide demande n itérations pour le calcul du PGCD de a et b, montrer que $a \geq F_{n+2}$ et $b \geq F_{n+1}$. Combien y a-t-il d'itérations si $a = F_{n+2}$ et $b = F_{n+1}$?

2) Avec les mêmes hypothèses qu'en **1)**, montrer que

$$n + 2 < \frac{\log_{10} \sqrt{5}(a+1)}{\log_{10} \phi}$$

et

$$n + 1 < \frac{\log_{10} \sqrt{5}(b+1)}{\log_{10} \phi}$$

où ϕ est le nombre d'or i.e la racine positive de l'équation $X^2 - X - 1 = 0$.

3) Si n est le nombre de chiffres décimaux d'un entier b positif, montrer que

$$\left\lfloor \frac{\log_{10} \sqrt{5}(b+1)}{\log_{10} \phi} \right\rfloor \leq 5p + 1.$$

4) Si n est le nombre d'itérations de l'algorithme d'Euclide pour $a > b > 0$, montrer que

$$n \leq 5 \left(\lfloor \log_{10} b \rfloor + 1 \right).$$

En déduire la complexité de l'algorithme d'Euclide.

Travaux Pratiques 1 - Opérations sur les entiers

Manipulations 1 Taper, noter les résultats affichés et comprendre...

```
>22/7;
>evalf(%);
>a:=23/7;
>evalf(a,500);
>18/12;
>?igcd
>igcd(456,752);
```

Manipulations 2 Idem.

```
>sum(i,i=1..n);
>factor(%);
>sum(i^2,i=1..n);
>factor(%);
```

Exercice 1

1) Calculer la forme factorisée de la somme $\sum_{i=1}^{n} i^3$.

2) Chercher le mode d'emploi de l'instruction `length`.

3) Donner le nombre de chiffres de $\sum_{i=1}^{100} i^7$.

Exercice 2

1) Calculer 100!.

2) Donner le nombre de chiffres de 100!.

3) Donner les 50 premières décimales de π.

Exercice 3

1) Calculer (ou programmer) la somme $S_n = \sum_{k=1}^{n} \frac{1}{k}$.

2) Exprimer de façon exacte puis de façon approchée S_7, S_{20}, S_{40}, S_{1000} et $S_{1000000}$.

Exercice 4

1) Trouver la décomposition en facteurs premiers de $98765432101234567 89$.

2) Calculer le nombre de diviseurs.

Travaux Pratiques 2 - L'algorithme d'Euclide

Manipulations d'ensembles Tapez les ordres suivants et observez les réponses.

```
>A:={1,3,5,7,9};
>B:={0,2,4,6,8};
>C:={seq(2*i,i=0..9)};
>DD:=A union B;
>X:=A intersect C;
>Y:=C minus B;
```

Exercice 1 Soit S l'ensemble des entiers strictement inférieurs à 100. Soient A, B et C les sous-ensembles de S respectivement multiples de 2, de 3 et de 5. On note $\overline{X}$ le complémentaire de la partie X de S et on définit l'opération Δ par $X\Delta Y = (X \cap \overline{Y}) \cup (Y \cap \overline{X})$

1) Déterminer $(A\Delta B) \cap (A\Delta C)$.

2) Déterminer $A\Delta(B \cap C)$.

3) A-t-on $(A\Delta B) \cap (A\Delta C) \subset A\Delta(B \cap C)$?

Exercice 2

1) Écrire une procédure Maple rendant le premier (resp. dernier) élément d'une liste.

2) Écrire une procédure Maple rendant la liste privée de son premier (resp. dernier) élément.

3) Écrire une procedure Maple réalisant la fusion de deux listes.

4) Écrire une procédure Maple rendant une liste "miroir" de L.

Exercice 3 Les nombres de Mersenne sont de la forme $M_p = 2^p - 1$ avec p premier.

1) Écrire les nombres de Mersenne pour $p \leq 31$.

2) Parmi eux, quels sont ceux qui sont premiers ?

3) Décomposer les autres en facteurs premiers et trouver leurs diviseurs.

Exercice 4 Soit p un nombre premier $(p \geq 5)$. On définit la somme

$$S_p = \sum_{k=1}^{p-1} \frac{1}{k}.$$

1) Calculer S_5, S_7, S_{29} sous forme de fraction irréductible.

2) Donner le reste de la division du numérateur de S_p par p^2 pour les trois valeurs de p précédentes.

3) Calculer le reste de la division du numérateur de S_p par p^2 pour tout p premier dans l'ensemble $\{2, \ldots, 100\}$.

Exercice 5

1) Écrire une procédure qui calcule le PGCD de deux entiers.

2) Écrire une procédure qui calcule le PGCD de plusieurs entiers sachant que la probabilité pour que deux entiers positifs u et v soient premiers est de $\frac{6}{\pi^2}$.

3) Écrire une procédure qui calcule le PPMC de plusieurs entiers.

Travaux Pratiques 3 - Représentation graphique

Il y a trois types d'objets Maple que l'on peut représenter graphiquement :

- **une expression**

```
>P:=x^3-3*x^2+x+1;
>plot(P,x=-5..5,-3..3);
```

- **une fonction**

```
>f:=x->if x=0 then 1 else sin(x)/x fi;
>plot(f,-3*Pi..3*Pi);
```

- **une ligne polygonale**

```
>L:=[[1,1],[3,4],[1,3],[-1,5]];
>plot(L);
```

On peut représenter également une famille (g_n) de fonctions (respectivement d'expressions) :

```
>g:=n->n*exp(x)+x;
>famille:={seq(g(n),n=0..10)};
>plot(famille,x=-5..5,y=-5..5);
```

Exercice 1 Représenter la fonction f définie par $f(x) = x \sin x$ dans les fenêtres suivantes [-10,10,-10,10] et [-500,500,-500,500].

Exercice 2 Représenter la suite de fonctions (f_n) définie par $f_n(x) = nx/(1 + n^2x^4)$ pour n variant de 0 à 10 dans la fenêtre [0,2,0,10].

Exercice 3 Représenter sur un même graphique la fonction $f(x) = e^x$ et la suite de fonctions (f_n) pour $n \in \{0, \ldots, 10\}$ définie par $f_n(x) = \sum_{k=0}^{n} x^k/k!$. Reprendre le même travail avec la fonction $f(x) = -\ln(1 - x)$ et la suite de fonctions (f_n) définie par $f_n(x) = \sum_{k=1}^{n} x^k/k$.

Exercice 4 Étant donnée une fonction numérique f, un réel a et un entier n, on veut obtenir la liste

$$L_n = [[u_0,0],[u_0,u_1],[u_1,u_1],[u_1,u_2], \ldots ,[u_{n-1},u_n],[u_n,u_n]]$$

avec

$$\begin{cases} u_0 = a, \\ u_{n+1} = f(u_n), \quad \forall n \in \mathbb{N}. \end{cases}$$

1) Déterminer cette liste quand $f(x) = 1/2(x^2 + 1)$, $a = 1/2$ et $n = 4$. Représenter, si possible sur un même graphique, la courbe de f, la droite $y = x$ et la liste L_4.

2) Écrire une procédure Maple qui admet une fonction f, un réel a et un indice n, et qui construit la liste L_n. Représenter sur un même graphique, la courbe de f, la droite $y = x$ et la liste L_n avec $a = 1.2$ et $n = 15$.

3) Écrire une procédure Maple qui "automatise" cette étude graphique.

4) Étudier graphiquement les suites définies par les récurrences

$$\begin{cases} u_0 = 1 \\ u_{n+1} = 2u_n/(1+u_n) - \ln(1+u_n) \quad \forall n \in \mathbb{N} \end{cases}$$

$$\begin{cases} u_0 = 1 \\ u_{n+1} = 2(1 - e^{-u_n}) \quad \forall n \in \mathbb{N} \end{cases}$$

$$\begin{cases} u_0 = 3.9 \\ u_{n+1} = 2\sqrt{4 - u_n} \quad \forall n \in \mathbb{N} \end{cases}$$

Travaux Pratiques 4 - Nombres aléatoires

Exercice 1 Écrire une procédure qui calcule les n premiers termes de la suite obtenue par la méthode MSM connaissant la graine et le nombre maximum de chiffres dans l'écriture décimale. Quel nombre suit 1010101010 et 3792 dans la méthode MSM ? Donner les premiers termes si la graine est 2345678 et le nombre maximum de chiffres est 16.

Exercice 2 On considère un générateur donné par :

$$\begin{aligned} u_0 &= g \\ u_i &= f(u_{i-1}) \ [m] \ (i > 0) \end{aligned}$$

1) Écrire une procédure calculant le nième terme de la suite connaissant g, f et m.

2) Montrer que la suite est ultimement périodique.

3) Soit $\ell(n)$ la plus grande puissance de 2 qui est plus petite ou égale à n. Montrer qu'il existe un entier $n > 0$ tel que $u_n = u_{\ell(n)-1}$. Écrire un algorithme (l'algorithme de Brent) qui calcule les différents paramètres de la suite ultimement périodique. Évaluer l'efficacité du générateur de nombres aléatoires de Maple puis celui du langage C qui est donné par :

$$u_n = 1103515245 \times u_{n-1} + 12345 \ [2^{31}] \ (n > 0).$$

4) Soit le générateur à deux pas défini par :

$$\begin{aligned} u_0 &= g_0 \\ u_1 &= g_1 \\ u_i &= f(u_{i-1},u_{i-2}) \ [m] \ (i > 1) \end{aligned}$$

Quelle transformation faut-il faire pour appliquer l'algorithme de Brent ? Généraliser aux générateurs à n pas.

10 TD

Calcul Formel 2002/2003

Exercice 1 Donner des formes closes de fonction génératrice ordinaire et exponentielle de la suite $2,5,13,35,\ldots,2^n+3^n,\ldots$.

Exercice 2 Pavage d'un rectangle $2 \times n$
1. Quel est le nombre T_n de façons de recouvrir entièrement un rectangle $2 \times n$ avec des dominos 2×1? Nous supposerons que les dominos sont tous identiques et que seule compte leur orientation (verticale ou horizontale).
2. Un collectionneur excentrique achète des pavages $2 \times n$ par des dominos au prix de 4 euros le domino vertical et 1 euro le domino horizontal¿ Combien de pavages valent exactement m euros?

Exercice 3 Résoudre les relations de récurrence suivantes par la méthode des fonctions génératrices :
1. $\begin{cases} F_0 = 0, F_1 = 1, \\ F_n = F_{n-1} + F_{n-2} \text{ sinon.} \end{cases}$
2. $\begin{cases} U_0 = U_1 = 1, \\ U_n = 4U_{n-1} - 4U_{n-2} + n - 1 \text{ sinon.} \end{cases}$
3. $\forall n \geq 2, 2U_n = 3U_{n-1} - U_{n-2}$
4. $\forall n \geq 2, U_n = 4U_{n-1} - 4U_{n-2}$
5. $\begin{cases} U_0 = 1, U_1 = 0, \\ U_n = 3U_{n-1} - 2U_{n-2} + n/2^n \text{ sinon.} \end{cases}$

Exercice 4 Résouder les relations de récurrence simultanées

$$\begin{cases} U_0 = 1, U_1 = 0 \text{ et } \forall n \geq 2, U_n = U_n = 2V_{n-1} + U_{n-2} \\ V_0 = 0, V_1 = D10 \text{ et } \forall n \geq 2, V_n = U_n = U_{n-1} + U_{n-2} \end{cases}$$

Exercice 5 On suppose que la durée d'un point dans le code morse est de 2 unités de temps et celle d'un trait de 3 unités. Déterminer la fonction génératrice des mots du code morse selon leur durée
Exercice 6 Nombres de Stirling de deuxième espèce
Soit $\left\{ \begin{array}{c} n \\ k \end{array} \right\}$ lr nombre de façons de partitionner $[n] = \{1,2,\ldots,n\}$ en k classes (ou sous ensembles). Par exemple, $\left\{ \begin{array}{c} 4 \\ 2 \end{array} \right\} = 7$.
1. Déterminer une récurrence sur les $\left\{ \begin{array}{c} n \\ k \end{array} \right\}$.
2. En déduire une expression de $B_k(x) = \sum_n \left\{ \begin{array}{c} n \\ k \end{array} \right\}$, puis de $\left\{ \begin{array}{c} n \\ k \end{array} \right\}$.

Exercice 7 Dans le "problème du collectionneur de coupons", imaginons que nous voudrions avoir la collection complete des d photos des stars de cinéma. A chaque achat d'une boîte de céréales, on obtient une de ces photos qui peut bien sûr être une que l'on a déja.
Soit p_n la probalité d'obtenir en n achats exactement la collection complète.

1. Montrer que

$$p_n = \frac{d! \left\{ \begin{array}{c} n \\ k \end{array} \right\}}{d^n}.$$

2. Soit $p(x) = \sum_n d_n x^n$. Montrer que

$$p(x) = \frac{(d-1)!x^d}{(d-x)(d-2x)\cdots(d-(d-1)x)}.$$

Exercice 8 Soit T un arbre binaire complet à $2n+1$ sommets. On considère

$$E = \sum_{x \text{ feuille}} prof(x),$$

$$I = \sum_{x \text{ sommet interne}} prof(x)$$

Trouver une relation entre E, I et n et la démontrer.

Exercice 9 Soient C_n le nombre d'arbres binaires complets ayant $2n+1$ sommets et $C(x)$ la fonction génératrice de ces arbres selon le nombre de sommets.

$$C(x) = \sum_{n \geq 0} C_n x^n.$$

1. Déterminer une récurrence sur les C_n.
2. En utilisant le résultat précédent, trouver une équation fonctionnelle pour $C(x)$ et la résoudre.
3. En déduire la valeur de C_n.

Exercice 10 Le but de cet exercice est d'énumérer les objets étudiés en construisant une bijection avec des mots d'un langage.
1. Construire tous les arbres binaires complets ayant au plus 5 sommets.
2. Déterminer un codage de ces arbres par des mots construits sur l'alphabet $\{x,\overline{x}\}$.
3. Calculer le codage des arbres construits en 1.
4. Caractériser le langage engendré par ces mots et déterminer la grammaire algébrique correspondante.
5. En déduire une équation fonctionnelle et la résoudre.
6. En utilisant l'équation fonctionnelle déterminée en 4., écrire un programme Maple calculant les p premiers termes de $C(x)$.

Exercice 11 Après avoir fait une dictée aux élèves de sa classe, un instituteur redistribue les copies. On note b_n le nombre de façons de distribuer les copies de façon à ce qu'aucun élève ne reçoive sa propre copie.
1. Calculer b_1,b_2 et b_3.
2. Montrer que l'on a la relation $b_n = (n-1)(b_{n-1} + b_{n-2})$, pour $n > 2$.
3. Etablir la relation $b_n - b_{n-1} = (-1)^n$, pour $n \geq 2$.
4. On pose $b_0 = 1$ et on définit la série génératrice exponentielle par

$$b)z) = \sum_{n \geq 0} \frac{b_n z^n}{n!}.$$

Montrer que $b(z) = \dfrac{e^{-z}}{1-z}$.

11 Séries

11.1 Introduction

Les séries jouent le rôle d'un outil très important en MATHÉMATIQUES (algèbre : réalisation explicites de complétés, analyse : développement de fonctions analytiques, développements asympotiques, géométrie : classes de singularités, probabilités : séries génératrices de probabilités), en INFORMATIQUE (combinatoire - algébrique, énumérative, analytique -, analyse d'algorithmes, grammaires d'objets, théorie des langages), en PHYSIQUE (probléme des moments, développements perturbatifs, solutions d'ED) et dans l'art de l'ingénieur (électronique : transformée en "z", séries de Fourier, développement de caractéristiques non linéaires, Linear Shift Register) pour ne citer que quelques unes de leurs applications.

11.2 Les séries sont des fonctions

Les séries se présentent sous forme d'une somme (finie ou infinie)

$$\sum_{m \in M} \text{coefficient}(m) m \tag{45}$$

l'ensemble M pouvant être un ensemble de monômes ou un ensemble de fonction bien choisies (séries d'exponentielles, séries de Fourier, de Dirichlet). Dans ce cours, nous nous limiterons au cas des monômes. Dans ce cadre rentrent

1. les séries et polynômes d'une ou plusieurs variables (commutatives, non commutatives ou partiellement commutatives)
2. les fonctions symétriques
3. les séries et polynômes de Laurent, de Malcev
4. les séries d'exponentielles, de Bertrand et de Dirichlet

le caractère commun de ces séries est que l'ensemble des monoômes M est fermé (stable en français) pour la multiplication.

11.3 Séries liées à des statistiques

11.3.1 La formule exponentielle

Soit G une classe de graphes étiquetés qui est

1. Stable par renommage. C'est à dire, si on réétiquette les sommets (bijectivement, c'est à dire sans répéter des étiquettes), on reste dans la classe.
2. Stable par composantes connexes c'est à dire, un graphe est dans G ssi toutes ses composantes connexes y sont.

on peut appliquer la formule exponentielle.

Théorème 11.1 *Soit $M(n,k)$ le nombre de graphes :*
i) Dont les étiquettes sont $[1..n]$
ii) Qui ont k composantes connexes.
On forme la série

$$SGE(G) = \sum_{n,k\geq 0} M(n,k)\frac{z^n}{n!}y^k \tag{46}$$

alors

$$SGE(G) = e^{y\sum_{n\geq 1} M(n,1)\frac{z^n}{n!}} \tag{47}$$

`TODO exemples: classes de Burnside, Nombres Idempotents`

11.3.2 Multisection de séries

Problème général. —

Soit $F(z) = \sum_n a_n z^n$ une série. On cherche des expressions pour les séries "restreintes" $F_C(z) = \sum_n$ vérifie $_C\, a_n z^n$.

Problème particulier : multisection de séries. —

Soit $b \in \mathbb{N}^*$, les conditions $c(b,r)[n]$ seront "le reste de n dans la division par b est r".
Pour une série $F(z)$, on pose

$$\text{section}(F,b,r) = \sum_{n\equiv r\ [b]} a_n z^n = \sum_{k=0}^{\infty} a_{bk+r} z^{bk+r} \tag{48}$$

11.4 Types courants (de séries)

Pour pouvoir faire des opérations sur les séries, il faut supposer que l'on sait opérer sur les coefficients. Pour simplifier notre approche, nous supposerons que les coefficients sont réels ou complexes (i.e. $k = \mathbb{R}$ ou $\mathbb{C}$)[6].
D'autre part, on se limitera aux séries pour lesquelles l'ensemble des monômes est stable poour une certaine opération associative $(M,*)$. On dit que $(M,*)$ est un *semigroupe*.

Définition 11.2 *Soit k en corps et $(M,*)$ un semigroupe. On appelle série sur M à coefficients dans k, toute fonction $M \overset{coeff}{\mapsto} k$.*

6. En fait une telle restriction est inutile en pratique et l'espace des coefficients peut être restreint aux anneaux et même - avec encore plus de succès en Informatique - aux semi-anneaux qui sont des structures qui vérifient les axiomes des anneaux sauf l'existence d'un opposé pour tout élément

11.5 Exemples

Les séries de toutes sortes sont des fonctions (avec ou sans restrictions) sur les monoïdes constitués par les monômes. Voyons quelques exemples.

Séries	Monômes	Restrictions	Remarques
Univariées en z	$z^{\mathbb{N}} = \{z^n\}_{n\in\mathbb{N}}$	Aucune	Espace noté $k[[z]]$
Polynômes en z	$z^{\mathbb{N}} = \{z^n\}_{n\in\mathbb{N}}$	Support fini	Espace noté $k[z]$
Plusieurs variables commutatives ($\mathbb{X}$)	$\mathbb{N}^{(\mathbb{X})}$, fonctions $X \mapsto \mathbb{N}$ à support fini	Aucune	Espace noté $k[[\mathbb{X}]]$
Polynômes à plusieurs variables commutatives ($\mathbb{X}$)	$\mathbb{N}^{(\mathbb{X})}$, fonctions $X \mapsto \mathbb{N}$ à support fini	Support fini	Espace noté $k[\mathbb{X}]$
Plusieurs variables noncommutatives ($\mathbb{X}$)	$\mathbb{X}^*$, monoïde libre sur l'alphabet $\mathbb{X}$	Aucune	Espace noté $k\langle\langle\mathbb{X}\rangle\rangle$
Polynômes à plusieurs variables noncommutatives	$\mathbb{X}^*$, monoïde libre sur l'alphabet $\mathbb{X}$	Support fini	Espace noté $k\langle\mathbb{X}\rangle$
Séries de Laurent	$z^{\mathbb{Z}} = \{z^n\}_{n\in\mathbb{Z}}$	$n \geq N;\ N \in \mathbb{Z}$	Espace noté $k((z))$
Polynômes de Laurent	$z^{\mathbb{Z}} = \{z^n\}_{n\in\mathbb{Z}}$	Support fini	Espace noté $k(z,z^{-1})$
Séries de Puiseux	$z^{\mathbb{Q}_+} = \{z^\alpha\}_{\substack{\alpha\in\mathbb{Q}\\ \alpha>0}}$	Aucune	
Séries de Malcev	$(\Gamma, \prec)$ groupe totalement ordonné	Support bien ordonné	Espace noté $k((\Gamma))$
Séries de Taylor	$z^{\mathbb{N}} = \{z^n\}_{n\in\mathbb{N}}$	Rayon de convergence	Espace noté $k[[\{z\}]]$ $k = \mathbb{R}$ ou $\mathbb{C}$
Exponentielles	$\{e^{nz}\}_{n\in\mathbb{N}}$		
Dirichlet	$\{n^{-z}\}_{n>0}$ entier		
Bertrand	$e^{\alpha z} ln(z)^\beta n^\gamma$		

11.6 Produit scalaire $\langle$série$|$polynôme$\rangle$ et premières opérations

Pour suivre l'usage en ce qui concerne les séries citées et quelques autres (polynômes d'exponentielles) nous appelerons *polynôme* une série $M \mapsto k$ à support fini. L'espace des séries sera noté k^M et celui des polynômes $k^{(M)}$.

Définition 11.3 *La dualité entre k^M et $k^{(M)}$ est définie, pour $S \in k^M$ et $P \in k^{(M)}$ par*

$$\langle S|P\rangle = \sum_{m\in M} S(m)P(m) \tag{49}$$

on vérifie facilement que cette somme est à support fini (donc bien définie).

Exercice 11.4 *1) a) Rappeler la structure d'EV de $k^X = \mathcal{F}(X,k)$. Montrer que $k^{(X)} = \{f \in k^X \mid supp(f)$ est fini$\}$ est un SEV de k^X.*
*b) Pour toute partie $Z \subset X$, χ_Z est la fonction caractéristique de Z (avec les notations de l'informatique $\chi_Z(x) = [x \in Z]$ où $[\,]$ est le symbole d'Iverson [**?**]). Montrer que, si Z_1 et Z_2 sont disjointes, on a $\chi_{Z_1} + \chi_{Z_2} = \chi_{Z_1\cup Z_2}$.*
c) Que se passe-t-il si les parties ne sont pas disjointes ?, si $k = \mathbb{Z}_2$?
d) Montrer que pour $S \in k^M;\ m \in M$, on a $\langle S|\chi_{\{m\}}\rangle = S(m)$
2) a) Montrer que pour tout $P \in k^{(M)}$, on a

$$P = \sum_{m\in M} \langle P|\chi_{\{m\}}\rangle \chi_{\{m\}} \tag{50}$$

b) Montrer que l'application $M \mapsto k^M$ définie par $m \mapsto \chi_{\{m\}}$ a son image dans $k^{(M)}$ et qu'elle est injective. On identifiera alors m à χ_m.
c) Comment se réécrit l'équation (81) avec l'identification du (b) ?
3) On veut prolonger aux séries l'écriture (81) ou plutôt sa version simplifiée avec l'identification du 2) b). On dira qu'une famille $(S_i)_{i\in I}$ de séries est sommable *si, pour tout $m \in M$, la fonction $I \mapsto k$ define par $i \mapsto S_i(m)$ est à support fini. Dans ce cas, on dira que la famille $(S_i)_{i\in I}$ est de somme S définie par $S(m) = \sum_{i\in I} S_i(m)$. On notera $S = \sum_{i\in I} S_i$*
Soit $S \in k^M$ une série. Montrer que la famille $(\langle S|m\rangle m)_{m\in M}$ est sommable et que $S = \sum_{m\in M}\langle S|m\rangle m$.

12 Séries d'une variable ($\mathbb{C}[[z]]$)

Faute de temps, nous n'aborderons pas les opérations sur les séries en général, mais nous concentrerons sur celles à une variable de façon que l'étudiant sache calculer dans $\mathbb{C}[[z]]$.

12.1 Opérations sur les séries

Tableau des opérations usuelles (décalage, intégration, dérivation).

Nom	Opérateur	Effet sur $S = \sum_{n=0}^{\infty} a_n z^n$
Décalage	γ_z^*	$\sum_{n=0}^{\infty} a_{n+1} z^n$
Dérivation	$\frac{d}{dz}$	$\sum_{n=1}^{\infty} a_n n z^{n-1}$
Intégration	$\int_0$	$\sum_{n=0}^{\infty} a_n \frac{z^{n+1}}{n+1}$
Sommes cumulées	$\gamma_{\frac{1}{1-z}}$	$\sum_{n=0}^{\infty} \left(\sum_{j=0}^{n} a_j\right) z^n$
Étoile ($a_0 = 0$)		$\frac{1}{1-S} = \sum_{n=0}^{\infty} S^n$

Exercice 12.1 *Prendre ces opérateurs deux par deux et donner des formules pour la composition et l'échange (si elles existent). Par exemple prouver la formule $\gamma_z^* \frac{d}{dz} - \frac{d}{dz}\gamma_z^* = (\gamma_z^*)^2$.*

12.2 Les deux produits : Convolution (produit de Cauchy) et produit de Hadamard

12.2.1 Produit de Cauchy

Ce produit s'obtient facilement à partir de la notation sommatoire. On multiplie formellement les sommes. Avec $S = \sum_{n=0}^{\infty}\langle S|z^n\rangle z^n$; $T = \sum_{m=0}^{\infty}\langle T|z^m\rangle z^m$ on a

$$ST = \sum_{n,m=0}^{\infty} \langle S|z^n\rangle\langle T|z^m\rangle z^{n+m} \tag{51}$$

puis, en regroupant par degrés,

$$ST = \sum_{r=0}^{\infty} \Big(\sum_{n+m=r} \langle S|z^n\rangle\langle T|z^m\rangle \Big) z^r \tag{52}$$

Définition 12.2 *Soient S,$T \in \mathbb{C}[[z]]$. On définit le produit (de Cauchy) ou convolution de ces deux séries par la formule (83).*

$$ST = \sum_{r=0}^{\infty} \Big(\sum_{n+m=r} \langle S|z^n\rangle\langle T|z^m\rangle \Big) z^r \tag{53}$$

Exercice 12.3 SUPPORT D'UN PRODUIT. —
On rappelle que le support d'une série $R = \sum_{n\in\mathbb{N}} \langle R|z^n\rangle z^n$ est l'ensemble des $n \in \mathbb{N}$ pour lesquels $\langle R|z^n\rangle \neq 0$.
Donner les supports des séries suivantes

a) $\frac{1}{1-z^2}$ *b)* $\frac{z^k}{1+\beta z}$ *c)* $\frac{1}{1+z+z^2}$

d) $\frac{1}{1-z^3}$ *e)* $\frac{1-z}{1-z^2}$ *f)* $\frac{1}{1-z} + \frac{1}{1+z}$

Exercice 12.4 ÉTOILE D'UNE SÉRIE. —
La notion de sommabilité définie dans l'exercice (14.4) est reprise ici dans le cadre plus simple des séries complexes à une variable.
On dira qu'une famille $(S_i)_{i\in I}$ de séries est sommable *si, pour tout $n \in \mathbb{N}$, la fonction $I \mapsto \mathbb{C}$ define par $i \mapsto \langle S_i|z^n\rangle$ est à support fini. Dans ce cas, on dira que la famille $(S_i)_{i\in I}$ est de somme S définie par $\langle S|z^n\rangle = \sum_{i\in I}\langle S_i|z^n\rangle$. On notera $S = \sum_{i\in I} S_i$*

1) Soit $T \in \mathbb{C}[[z]]$ et S_i sommable. Montrer que TS_i est sommable et que $\sum_{i\in I} TS_i = T\sum_{i\in I} S_i$.
2) a) Soit $S \in \mathbb{C}[[z]]$ une série sans terme constant (formellement $\langle S|z^0\rangle = 0$), montrer que la famille $(S^k)_{k\in\mathbb{N}}$ est sommable.
b) Montrer que $\sum_{k\in\mathbb{N}} S^k = (1-S)^{-1}$ dans $\mathbb{C}[[z]]$.
3) En posant $S = a_0 + S^+$ où $a_0 = \langle S|z^0\rangle$ et $S^+ = S - a_0 = \sum_{n>0}\langle S|z^n\rangle z^n$, montrer la proposition (15.5).

Proposition 12.5 SÉRIES INVERSIBLES. — *Soit $S \in \mathbb{C}[[z]]$, S est inversible dans $\mathbb{C}[[z]]$ ssi son terme constant $\langle S|z^0\rangle$ l'est.*

Exercice 12.6 *1) Fontaine de pièces de Wilf (donné en cours).*
2) Polyominos tas stricts (donné dans la présentation du cours).

12.2.2 Séries rationnelles

Définition 12.7 *Une série $S \in \mathbb{C}[[z]]$ est dite rationnelle si elle peut s'exprimer sous la forme $S = \frac{P}{Q};\ P,Q \in C[z];\ Q(0) \neq 0$.*

Nous allons voir trois caractérisations (très importantes) des séries rationnelles :

- **Rat**. — Fraction rationnelle $S = \frac{P}{Q};\ Q(0) \neq 0$
- **Coeff**. — Coefficients $\langle S|z^n\rangle = \sum_{(s,\lambda)\in F} \alpha(s,\lambda) n^s \lambda^n$, avec F fini.
- **Rec**. — Récurence linéaire

$$(\exists(\alpha_0,\alpha_1,\cdots\alpha_k) \in \mathbb{C}^{k+1})(\forall n \in \mathbb{N})(\langle S|z^{n+k}\rangle = \sum_{j=0}^{k-1} \alpha_j \langle S|z^{n+j}\rangle)$$

les étudiants devront être maîtres du passage de l'une des ces formes à l'autre. Nous allons les détailler maintenant.
Rat→**Rec**. — Comme $Q(0) \neq 0$, on met la fraction $\frac{P}{Q}$ sous la forme

$$\frac{N(z)}{1 - \sum_{j=1}^{m} \beta_j z^j} \tag{54}$$

(en divisant haut et bas par $Q(0)$). Une fois ceci fait, on a

$$S(1-\sum_{j=1}^{m}\beta_j z^j) = S - S(\sum_{j=1}^{m}\beta_j z^j) = N(z) \tag{55}$$

soit

$$S = S(\sum_{j=1}^{m}\beta_j z^j) + N(z) \tag{56}$$

Maintenant, pour $k \geq sup(\deg(N(z)),m)$, on a $\langle N|z^{n+k}\rangle = 0$ d'où

$$\langle S|z^{n+k}\rangle = \sum_{j=1}^{n}\beta_j\langle z^j S|z^{n+k}\rangle = \sum_{j=1}^{n}\beta_j\langle S|z^{n+k-j}\rangle \tag{57}$$

qui est la récurrence linéaire cherchée.

Exercice 12.8 *Les nombres de Fibonacci sont donnés par la récurrence*

$$F_0 = 0,\, F_1 = 1;\; F_{n+2} = F_n + F_{n+1} \tag{58}$$

a) Redémontrer que la série génératrice des nombres de Fibonacci est $S(z) = \frac{z}{1-z-z^2}$.
b) En déduire que celle des nombres de Fibonacci impairs $T(z) = \sum_{n\geq 0} F_{2n+1}z^n$ *est* $\frac{1}{1-3z+z^2}$
c) En déduire la relation de récurrence satisfaite par ces nombres (les $a_n = F_{2n+1}$*).*

Rec→Rat. — Soit S qui vérifie la relation de récurrence linéaire, donnée par des coefficients $(\alpha_0,\alpha_1,\cdots\alpha_k) \in \mathbb{C}^k$,

$$(\forall n \in \mathbb{N})(\langle S|z^{n+k}\rangle = \sum_{j=0}^{k-1}\alpha_j\langle S|z^{n+j}\rangle) \tag{59}$$

on a , pour tout n,

$$\langle(\gamma_z^*)^k S|z^n\rangle = \sum_{j=0}^{k-1}\alpha_j(\gamma_z^*)^j\langle S|z^n\rangle \tag{60}$$

soit

$$(\gamma_z^*)^k S - \sum_{j=0}^{k-1}\alpha_j(\gamma_z^*)^j S = 0 \tag{61}$$

si on fait $z^m(\gamma_z^*)^m S$ on obtient la série privée de ses m premiers termes, soit le reste d'ordre m $S - \mathrm{trunc}(S,m-1)$ (où $\mathrm{trunc}(S,l) = \sum_{n=0}^{l}\langle S|z^n\rangle z^n$ est l'opérateur de troncature). En multipliant l'équation précédente par z^k on obtient

$$0 = z^k(\gamma_z^*)^k S - \sum_{j=0}^{k-1}\alpha_j z^{k-j}z^j(\gamma_z^*)^j S = S - \mathrm{trunc}(S,k-1) - \sum_{j=0}^{k-1}\alpha_j z^{k-j}(S - \mathrm{trunc}(S,j-1)) \tag{62}$$

soit

$$S\Big(1-\sum_{j=0}^{k-1}\alpha_j z^{k-j}\Big)=\mathrm{trunc}(S,k-1)-\sum_{j=0}^{k-1}\alpha_j z^{k-j}\mathrm{trunc}(S,j-1) \tag{63}$$

dont le second membre est un polynôme. Ce qui est la forme cherchée

$$S=\frac{\mathrm{trunc}(S,k-1)-\sum_{j=0}^{k-1}\alpha_j z^{k-j}\mathrm{trunc}(S,j-1)}{1-\sum_{j=0}^{k-1}\alpha_j z^{k-j}} \tag{64}$$

Exercice 12.9 *En calculant $F_{n+3}^2-F_{n+2}^2$ trouver une relation de récurrence entre les $a_n=F_n^2$. Calculer la fraction rationnelle $\sum_n F_n^2 z^n$*

Rat→Coeff. — On utilise la décomposition en éléments simples

$$\frac{P}{Q}=E(x)+\sum_{\lambda\in\mathcal{O}_Q}\sum_{j=1}^{n_\lambda}\frac{\alpha(\lambda,j)}{(z-\lambda)^j} \tag{65}$$

il suffit donc de savoir calculer les coefficients du développement de chaque $\frac{1}{(z-\lambda)^j}$ avec $\lambda\neq 0$.

Exercice 12.10 *1) a) Montrer que $\frac{d^k}{dz^k}(1-\beta z)^{-1}=k!\beta^k(1-\beta z)^{-(k+1)}$.*
b) Montrer que $\frac{d^k}{dz^k}(1-\beta z)^{-1}=\sum_{n=k}^{\infty}n(n-1)\cdots(n-k+1)\beta^n z^{n-k}$.
On adopte les notations commodes suivantes
`http://mathworld.wolfram.com/FallingFactorial.html`
Factorielle descendante $(x)_k=x(x-1)\cdots(x-k+1)$
Factorielle ascendante $x^{(k)}=x(x+1)\cdots(x+k-1)$
Binomial généralisé $\left(\begin{array}{c}x\\k\end{array}\right)=\frac{1}{k!}(x)_k=\frac{x(x-1)\cdots(x-k+1)}{k!}$

2) Déduire du (1.b) que

$$\frac{1}{(1-\beta z)^{k+1}}=\sum_{n=k}^{\infty}\left(\begin{array}{c}n\\k\end{array}\right)\beta^{n-k}z^{n-k}=\sum_{m=0}^{\infty}\frac{m^{(k)}}{k!}\beta^m z^m \tag{66}$$

Exercice Machine 12.11 *On veut convertir les factorielles montantes sur la base des puissances. La clef est le triangle des nombres de Stirling de 1ère espèce.*
1) a) Lire et interpréter les résultats du programme suivant

```
> with(combinat);
```

$$[\mathrm{Chi}, bell, \mathrm{binomial}, cartprod, character, choose, composition, conjpart, decodepart, encodepart, fibonacci, firstpart, graycode, inttovec, lastpart, multinomial, nextpart, numbcomb, numbcomp, numbpart, numbperm, partition, permute, powerset, prevpart, randcomb, randpart, randperm, setpartition, stirling1, stirling2, subsets, vectoint]$$

```
> rf:=proc(x,k) product(x+j,j=0..k-1) end;
```

$$rf := \textbf{proc}(x,k)\,\mathrm{product}(x+j, j=0..k-1)\ \textbf{end proc}$$

```
> rf(x,5);
```

$$x\,(x+1)\,(x+2)\,(x+3)\,(x+4)$$

```
> seq(print(expand(rf(x,k))),k=0..7);
```

$$1$$
$$x$$
$$x^2+x$$
$$x^3+3\,x^2+2\,x$$
$$x^4+6\,x^3+11\,x^2+6\,x$$
$$x^5+10\,x^4+35\,x^3+50\,x^2+24\,x$$
$$x^6+15\,x^5+85\,x^4+225\,x^3+274\,x^2+120\,x$$
$$x^7+21\,x^6+175\,x^5+735\,x^4+1624\,x^3+1764\,x^2+720\,x$$

```
> seq(print(seq(stirling1(n,k),k=0..n)),n=0..7);
```

$$1$$
$$0,1$$
$$0,\ -1,1$$
$$0,2,\ -3,1$$
$$0,\ -6,11,\ -6,1$$
$$0,24,\ -50,35,\ -10,1$$
$$0,\ -120,274,\ -225,85,\ -15,1$$
$$0,720,\ -1764,1624,\ -735,175,\ -21,1$$

b) Se renseigner sur les nombres de Stirling de première espèce (par exemple dans les livres ou dans `http://mathworld.wolfram.com/StirlingNumberoftheFirstKind.html`*) et donner l'expression de $x^{(k)}$ en fonction des puissances de x.*
2) On appelle Série Quasi-Polynôme (SQP), une série $P(l,\alpha,z)=\sum_{n=0}^{\infty} n^l\alpha^n z^n$ avec $\alpha\neq 0$.
a) Calculer le produit $P(l_1,\alpha_1,z)P(l_2,\alpha_2,z)$.
b) Exprimer la SGO des nombres de Fibonacci en fonction de deux SQP.
c) Déduire de la question (1) une expression des éléments simples $\frac{1}{(1-\alpha z)^{k+1}}$ en fonction des SQP ($P(l,\alpha,z)=\sum_{n=0}^{\infty} n^l\alpha^n z^n$).

Note 12.12 *On peut montrer que les fonctions $P(l,\alpha,z)$ sont linéairement indépendantes et forment une base des fractions rationnelles sans pôle nul ni partie entière. Ce qui précède montre qu'elles forment une* base multiplicative *de cet espace.*

Coeff→Rat. —

Exercice 12.13 *On suppose qu'à partir d'un certain rang les coefficients de la série S sont une combinaison linéaire d'expressions du type $n^l\alpha^n$.*
1) Montrer que S se décompose de façon unique comme

$$S=P(z)+\sum_{(l,\alpha)\in F}\beta(l,\alpha)P(l,\alpha,z) \tag{67}$$

où P est un polynôme.

Exercice Machine 12.14 *1) a) Lire et interpréter le programme suivant.*

```
> S1:=matrix(10,10,(i,j)->stirling1(i-1,j-1));
```

$$S1 := \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & -3 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -6 & 11 & -6 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 24 & -50 & 35 & -10 & 1 & 0 & 0 & 0 & 0 \\ 0 & -120 & 274 & -225 & 85 & -15 & 1 & 0 & 0 & 0 \\ 0 & 720 & -1764 & 1624 & -735 & 175 & -21 & 1 & 0 & 0 \\ 0 & -5040 & 13068 & -13132 & 6769 & -1960 & 322 & -28 & 1 & 0 \\ 0 & 40320 & -109584 & 118124 & -67284 & 22449 & -4536 & 546 & -36 & 1 \end{bmatrix}$$

```
> S2:=matrix(10,10,(i,j)->stirling2(i-1,j-1));
```

$$S2 := \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 3 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 7 & 6 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 15 & 25 & 10 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 31 & 90 & 65 & 15 & 1 & 0 & 0 & 0 \\ 0 & 1 & 63 & 301 & 350 & 140 & 21 & 1 & 0 & 0 \\ 0 & 1 & 127 & 966 & 1701 & 1050 & 266 & 28 & 1 & 0 \\ 0 & 1 & 255 & 3025 & 7770 & 6951 & 2646 & 462 & 36 & 1 \end{bmatrix}$$

```
> multiply(S1,S2);
```

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

b) Les nombres de Stirling de deuxième espèce $stirling2(n,k)$ *avec* $n,k \in \mathbb{N}$ *forment la matrice inverse de celle des nombres de première espèce. On peut voir cela come une relation entre patrice infinies ou bien comme une infinité de relations au sens suivant.*
Soient les matrices de $\mathbb{Z}^{(N+1)\times(N+1)}$*,*

$$S1(N) = (stirling1(n,k))_{0\le n,k\le N} \text{ et } S2(N) = (stirling2(n,k))_{0\le n,k\le N} \tag{68}$$

alors $S1S2 = I_{(N+1)\times(N+1)}$.
2) Soit $\underline{P}(l,\alpha,z) = \sum_{n=l}^{\infty}(n)_l\,\alpha^n z^n$.
a) Exprimer les $\underline{P}(l,\alpha,z)$ *en fonction des* $P(l',\alpha',z)$*. Écrire soigneusement la matrice de passage.*

b) À l'aide des nombres de Stirling de deuxième espèce, exprimer les $P(l,\alpha,z)$ en fonction des $\underline{P}(l',\alpha',z)$.
3) Déduire de tout ce qui précède une méthode pour exprimer S comme une fraction rationnelle.

Remarque 12.15 *Les passages* **Rec**→**Coeff** *et* **Coeff**→**Rec** *se font par composition des méthodes précédentes. Si l'on tient à des méthodes directes (mais pas nécessairement plus courtes ni plus élégantes), on peut aussi, pour le premier, utiliser une réduction de Jordan de la matrice compagnon associée à la récurrence et utiliser des produits de Hadamard (cf paragraphe (15.2.4)) pour le second.*

12.2.3 Séries rationnelles (repésentations linéaires et aspect automatique)

Avant de généraliser la théorie des séries rationnelles à plusieurs variables (non-commutatives), il est utile de voir comment elles peuvent se représenter par un automate (unaire et à mltiplicités). On a la proposition suivante (énoncée dans le cas général où l'ensemble des scalaires K est un corps commutatif quelconque)

Proposition 12.16 *Soit $S\sum_{n\in N} a_n z^n \in K\langle\langle z\rangle\rangle$ une série. Les conditions suivantes sont équivalentes*
i) S est rationnelle, c'est à dire $S = P(Q)^{-1}$ où P,$Q \in K\langle z\rangle$ et $Q(0) \neq 0$
ii) Les coefficients de S vérifient une récurrence linéaire

$$(\exists(\alpha_j)_{0\leq j<k} \in K^k)(\forall n \in \mathbb{N})(a_{n+k} = \sum_{j=0}^{k-1} \alpha_j a_{n+j}) \tag{69}$$

iii) Il existe $\lambda \in K^{1\times n}$, $T \in K^{n\times n}$,$\gamma \in K^{n\times 1}$ tels que

$$(\forall n \in \mathbb{N})(a_n = \lambda T^n \gamma) \tag{70}$$

Preuve — ii) $\Longrightarrow$ iii). —
La relation de récurrence linéaire implique

$$(a_{n+1},a_{n+2}\cdots,a_{n+k}) = (a_n,a_{n+1}\cdots,a_{n+k-1}) \begin{pmatrix} 0 & 0 & \cdots & \cdots & 0 & \alpha_0 \\ 1 & 0 & \ddots & & \vdots & \vdots \\ 0 & 1 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 & \vdots \\ \vdots & \vdots & & \ddots & 0 & \alpha_{k-2} \\ 0 & 0 & \cdots & \cdots & 1 & \alpha_{k-1} \end{pmatrix} \tag{71}$$

soit, en posant T, la matrice et $v_n = (a_n,a_{n+1}\cdots,a_{n+k-1})$, $v_{n+1} = v_n T$, d'où $v_n = v_0 T^n$. On a finalement

$$a_n = v_n \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = (a_0,a_1\cdots,a_{k-1})T^n \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \tag{72}$$

iii) $\Longrightarrow$ i). —
En effet, $S = \sum_n a_n z^n = \sum_n \lambda T^n \gamma z^n = \lambda(\sum_n T^n z^n)\gamma = \lambda(I - zT)^{-1}\gamma$. Mais

$$(I - zT)^{-1} = \frac{1}{det(I - zT)}\text{comatrice}(I - zT) \tag{73}$$

et les $Q(z) = det(I - zT)$ est un polynôme en z tel que $Q(0) = 1$ et comatrice(I-zT) est une matrice de polynômes en z (exercice !!). D'où le résultat.
i) $\Longrightarrow$ ii). —
On peut poser $Q(z) = \sum_{j=0}^{k-1} \beta_j z^j$ avec $\beta_0 = 1$. Comme $P = SQ$, pour tout $n \in \mathbb{N}$, on a $\langle P|z^n\rangle = \sum_{p+q=n} \beta_p a_q$, soit, si $n > N = max(\deg(P),k)$, $\sum_{p+q=n} \beta_p a_q = 0$ ce qui peut encore s'écrire $a_n = -\sum_{j=1}^{k} \beta_j a_{n-j}$, ce qui donne, pour tout $n \in \mathbb{N}$,

$$a_{n+N} = -\sum_{j=1}^{k} \beta_j a_{n+N-j} \tag{74}$$

ce qui entraine (ii). ♣

Définition 12.17 *Un triplet $\mathcal{T} = (\lambda,T,\gamma)$ tel que $\langle S|z^n\rangle = \lambda T^n \gamma$ est appellé* repésentation linéaire *de dimension n de S. De même S est appelée* comportement *de $\mathcal{T}$.*

Note 12.18 *Une série rationnelle admet en général plusieurs représentations linéaires. La dimension minimale de ces représentations est appellée* rang *de S. C'est aussi la dimension de l'espace vectoriel engendré par les décalées de S.*

12.2.4 Produit de Hadamard

C'est juste le produit des fonctions (fonctions "coefficient"), il sera noté $\odot$. Par exemple pour les séries d'une variable on a

$$\sum_{n=0}^{\infty} a_n z^n \odot \sum_{n=0}^{\infty} b_n z^n = \sum_{n=0}^{\infty} a_n b_n z^n \tag{75}$$

Exercice 12.19 *Effectuer les produits de Hadamard suivants*

a) $\frac{1}{1-z^2} \odot \frac{1}{1-2z}$ *b)* $\frac{1}{1+z+z^2} \odot \frac{1}{1-2z}$ *c)* $\frac{1}{1+z+z^2} \odot f(z)$

d) $\frac{1}{1-z^2} \odot e^z$ *e)* $\frac{z}{1-z^2} \odot e^z$ *f)* $\frac{1}{1-z} \odot f(z)$

Montrer que le résultat de (c) est rationnel si $f(z)$ est rationnelle i.e. si $f(z) = \frac{P(z)}{Q(z)}$; $Q(0) \neq 0$
indication. *— Pour le (b), décomposer en éléments simples. Pour le (c) on pourra remarquer que $\frac{1}{1+z+z^2} = \frac{1-z}{1-z^3}$.*

Théorème 12.20 PRODUIT DE HADAMARD DE SÉRIES RATIONNELLES. —
Soient $S,T \in \mathbb{C}[[z]]$ rationnelles. Alors $S \odot T$ est rationnelle.

Preuve — On peut remarquer qu'une série $R \in \mathbb{C}[[z]]$ est rationnelle ssi l'ensemble de ses décalées $(\gamma_z^*)^k R$ est de rang fini. Comme $\gamma_z^*(U \odot V) = \gamma_z^*(U) \odot \gamma_z^*(V)$, on a le résultat.

13 Systèmes de Calcul Formel et structures de données

13.1 Révision numération

Il est bon, avant d'attaquer, de maîtriser la numération en base quelconque. Voici quelques exercices.

13.1.1 Quelques exercices

Objectifs : Il faut que les étudiants soient maîtres (papier crayon et programmation) des conversions entre bases (avec virgule) et du passage (fraction $\leftrightarrow$ développement périodique). La commande maple pour vérifier les conversions est à chercher dans `convert`, celle pour les développement illimités dans `evalf` (attention à la variable d'environnement `Digits`).

1) Mettre les nombres binaires suivants sous forme décimale
a) $(101101)_2$ b)$(101101101)_2$ c) $(\underbrace{101\cdots101}_{3n \text{ chiffres}})_2$ (pour le (c), on montrera que la réponse dépend de la conversion d'un nombre plus simple)
2) Mettre les fractions suivantes sous forme décimale
a) $(0{,}615)_8$ b) $(12{,}321)_5$ c) $(0,\underbrace{7777777777}_{10 \text{ chiffres}})_8$
3) Calculer
a) $a_n = (0,\underbrace{5\cdots5}_{n \text{ chiffres}})_8$ b) $b_n = (12,\underbrace{1212\cdots12}_{2n \text{ chiffres}})_8$ c) $c_n = (12,\underbrace{2112\cdots2112\cdots}_{n \text{ chiffres}})_8$
d) $f_1 = (0{,}(54321)^\infty)_8$
e) le développement décimal illimité de
i) $23/7$ ii) $7/22$ iii) $1/99999$

4) Conversions Fraction $\leftrightarrow$ Développements illimités en base b (les résultats seront toujours donnés en base dix sauf pour les points c,e).
a) $12{,}(345)^\infty;\ b=10$ b) $12{,}(345)^\infty;\ b=8$
c) $BA/CA;\ b=16$ d) $22/132;\ b=10$ e) $BA{,}(CA)^\infty;\ b=16$

14 Séries

14.1 Introduction

Les séries jouent le rôle d'un outil très important en MATHÉMATIQUES (algèbre : réalisation explicites de complétés, analyse : développement de fonctions analytiques, développements asympotiques, géométrie : classes de singularités, probabilités : séries génératrices de probabilités), en INFORMATIQUE (combinatoire - algébrique, énumérative, analytique -, analyse d'algorithmes, grammaires d'objets, théorie des langages), en PHYSIQUE (probléme des moments, développements perturbatifs, solutions d'ED) et dans l'art de l'ingénieur (électronique : transformée en "z", séries de Fourier, développement de caractéristiques non linéaires, Linear Shift Register) pour ne citer que quelques unes de leurs applications.

14.2 Les séries sont des fonctions

Les séries se présentent sous forme d'une somme (finie ou infinie)

$$\sum_{m \in M} \text{coefficient}(m) m \tag{76}$$

l'ensemble M pouvant être un ensemble de monômes ou un ensemble de fonction bien choisies (séries d'exponentielles, séries de Fourier, de Dirichlet). Dans ce cours, nous nous limiterons au cas des monômes. Dans ce cadre rentrent

1. les séries et polynômes d'une ou plusieurs variables (commutatives, non commutatives ou partiellement commutatives)
2. les fonctions symétriques
3. les séries et polynômes de Laurent, de Malcev
4. les séries d'exponentielles, de Bertrand et de Dirichlet

le caractère commun de ces séries est que l'ensemble des monoômes M est fermé (stable en français) pour la multiplication.

14.3 Séries liées à des statistiques

14.3.1 La formule exponentielle

Soit G une classe de graphes étiquetés qui est

1. Stable par renommage. C'est à dire, si on réétiquette les sommets (bijectivement, c'est à dire sans répéter des étiquettes), on reste dans la classe.
2. Stable par composantes connexes c'est à dire, un graphe est dans G ssi toutes ses composantes connexes y sont.

on peut appliquer la formule exponentielle.

Théorème 14.1 *Soit $M(n,k)$ le nombre de graphes :*
i) Dont les étiquettes sont $[1..n]$
ii) Qui ont k composantes connexes.
On forme la série

$$SGE(G) = \sum_{n,k \geq 0} M(n,k) \frac{z^n}{n!} y^k \tag{77}$$

alors

$$SGE(G) = e^{y \sum_{n \geq 1} M(n,1) \frac{z^n}{n!}} \tag{78}$$

`TODO exemples: classes de Burnside, Nombres Idempotents`

14.3.2 Multisection de séries

Problème général. —

Soit $F(z) = \sum_n a_n z^n$ une série. On cherche des expressions pour les séries "restreintes" $F_C(z) = \sum_n$ vérifie $_C\, a_n z^n$.

Problème particulier : multisection de séries. —

Soit $b \in \mathbb{N}^*$, les conditions $c(b,r)[n]$ seront "le reste de n dans la division par b est r".
Pour une série $F(z)$, on pose

$$\text{section}(F,b,r) = \sum_{n \equiv r \ [b]} a_n z^n = \sum_{k=0}^{\infty} a_{bk+r} z^{bk+r} \tag{79}$$

14.4 Types courants (de séries)

Pour pouvoir faire des opérations sur les séries, il faut supposer que l'on sait opérer sur les coefficients. Pour simplifier notre approche, nous supposerons que les coefficients sont réels ou complexes (i.e. $k = \mathbb{R}$ ou $\mathbb{C}$)[7].
D'autre part, on se limitera aux séries pour lesquelles l'ensemble des monômes est stable poour une certaine opération associative $(M,*)$. On dit que $(M,*)$ est un *semigroupe*.

Définition 14.2 *Soit k en corps et $(M,*)$ un semigroupe. On appelle série sur M à coefficients dans k, toute fonction $M \overset{coeff}{\mapsto} k$.*

7. En fait une telle restriction est inutile en pratique et l'espace des coefficients peut être restreint aux anneaux et même - avec encore plus de succès en Informatique - aux semi-anneaux qui sont des structures qui vérifient les axiomes des anneaux sauf l'existence d'un opposé pour tout élément

14.5 Exemples

Les séries de toutes sortes sont des fonctions (avec ou sans restrictions) sur les monoïdes constitués par les monômes. Voyons quelques exemples.

Séries	Monômes	Restrictions	Remarques
Univariées en z	$z^{\mathbb{N}} = \{z^n\}_{n\in\mathbb{N}}$	Aucune	Espace noté $k[[z]]$
Polynômes en z	$z^{\mathbb{N}} = \{z^n\}_{n\in\mathbb{N}}$	Support fini	Espace noté $k[z]$
Plusieurs variables commutatives ($\mathbb{X}$)	$\mathbb{N}^{(\mathbb{X})}$, fonctions $X \mapsto \mathbb{N}$ à support fini	Aucune	Espace noté $k[[\mathbb{X}]]$
Polynômes à plusieurs variables commutatives ($\mathbb{X}$)	$\mathbb{N}^{(\mathbb{X})}$, fonctions $X \mapsto \mathbb{N}$ à support fini	Support fini	Espace noté $k[\mathbb{X}]$
Plusieurs variables noncommutatives ($\mathbb{X}$)	$\mathbb{X}^*$, monoïde libre sur l'alphabet $\mathbb{X}$	Aucune	Espace noté $k\langle\langle\mathbb{X}\rangle\rangle$
Polynômes à plusieurs variables noncommutatives	$\mathbb{X}^*$, monoïde libre sur l'alphabet $\mathbb{X}$	Support fini	Espace noté $k\langle\mathbb{X}\rangle$
Séries de Laurent	$z^{\mathbb{Z}} = \{z^n\}_{n\in\mathbb{Z}}$	$n \geq N;\ N \in \mathbb{Z}$	Espace noté $k((z))$
Polynômes de Laurent	$z^{\mathbb{Z}} = \{z^n\}_{n\in\mathbb{Z}}$	Support fini	Espace noté $k(z,z^{-1})$
Séries de Puiseux	$z^{\mathbb{Q}_+} = \{z^\alpha\}_{\substack{\alpha\in\mathbb{Q}\\ \alpha>0}}$	Aucune	
Séries de Malcev	$(\Gamma, \prec)$ groupe totalement ordonné	Support bien ordonné	Espace noté $k((\Gamma))$
Séries de Taylor	$z^{\mathbb{N}} = \{z^n\}_{n\in\mathbb{N}}$	Rayon de convergence	Espace noté $k[[\{z\}]]$ $k = \mathbb{R}$ ou $\mathbb{C}$
Exponentielles	$\{e^{nz}\}_{n\in\mathbb{N}}$		
Dirichlet	$\{n^{-z}\}_{n>0}$ entier		
Bertrand	$e^{\alpha z} ln(z)^\beta n^\gamma$		

14.6 Produit scalaire $\langle$série$|$polynôme$\rangle$ et premières opérations

Pour suivre l'usage en ce qui concerne les séries citées et quelques autres (polynômes d'exponentielles) nous appelerons *polynôme* une série $M \mapsto k$ à support fini. L'espace des séries sera noté k^M et celui des polynômes $k^{(M)}$.

Définition 14.3 *La dualité entre k^M et $k^{(M)}$ est définie, pour $S \in k^M$ et $P \in k^{(M)}$ par*

$$\langle S|P\rangle = \sum_{m\in M} S(m)P(m) \tag{80}$$

on vérifie facilement que cette somme est à support fini (donc bien définie).

Exercice 14.4 *1) a) Rappeler la structure d'EV de $k^X = \mathcal{F}(X,k)$. Montrer que $k^{(X)} = \{f \in k^X \mid supp(f)$ est fini$\}$ est un SEV de k^X.*
*b) Pour toute partie $Z \subset X$, χ_Z est la fonction caractéristique de Z (avec les notations de l'informatique $\chi_Z(x) = [x \in Z]$ où $[\,]$ est le symbole d'Iverson [**?**]). Montrer que, si Z_1 et Z_2 sont disjointes, on a $\chi_{Z_1} + \chi_{Z_2} = \chi_{Z_1\cup Z_2}$.*
c) Que se passe-t-il si les parties ne sont pas disjointes ?, si $k = \mathbb{Z}_2$?
d) Montrer que pour $S \in k^M;\ m \in M$, on a $\langle S|\chi_{\{m\}}\rangle = S(m)$
2) a) Montrer que pour tout $P \in k^{(M)}$, on a

$$P = \sum_{m\in M} \langle P|\chi_{\{m\}}\rangle \chi_{\{m\}} \tag{81}$$

b) Montrer que l'application $M \mapsto k^M$ définie par $m \mapsto \chi_{\{m\}}$ a son image dans $k^{(M)}$ et qu'elle est injective. On identifiera alors m à χ_m.
c) Comment se réécrit l'équation (81) avec l'identification du (b) ?
3) On veut prolonger aux séries l'écriture (81) ou plutôt sa version simplifiée avec l'identification du 2) b). On dira qu'une famille $(S_i)_{i\in I}$ de séries est sommable *si, pour tout $m \in M$, la fonction $I \mapsto k$ define par $i \mapsto S_i(m)$ est à support fini. Dans ce cas, on dira que la famille $(S_i)_{i\in I}$ est de somme S définie par $S(m) = \sum_{i\in I} S_i(m)$. On notera $S = \sum_{i\in I} S_i$*
Soit $S \in k^M$ une série. Montrer que la famille $(\langle S|m\rangle m)_{m\in M}$ est sommable et que $S = \sum_{m\in M}\langle S|m\rangle m$.

15 Séries d'une variable ($\mathbb{C}[[z]]$)

Faute de temps, nous n'aborderons pas les opérations sur les séries en général, mais nous concentrerons sur celles à une variable de façon que l'étudiant sache calculer dans $\mathbb{C}[[z]]$.

15.1 Opérations sur les séries

Tableau des opérations usuelles (décalage, intégration, dérivation).

Nom	Opérateur	Effet sur $S = \sum_{n=0}^{\infty} a_n z^n$
Décalage	γ_z^*	$\sum_{n=0}^{\infty} a_{n+1} z^n$
Dérivation	$\frac{d}{dz}$	$\sum_{n=1}^{\infty} a_n n z^{n-1}$
Intégration	$\int_0$	$\sum_{n=0}^{\infty} a_n \frac{z^{n+1}}{n+1}$
Sommes cumulées	$\gamma_{\frac{1}{1-z}}$	$\sum_{n=0}^{\infty} \left(\sum_{j=0}^{n} a_j\right) z^n$
Étoile ($a_0 = 0$)		$\frac{1}{1-S} = \sum_{n=0}^{\infty} S^n$

Exercice 15.1 *Prendre ces opérateurs deux par deux et donner des formules pour la composition et l'échange (si elles existent). Par exemple prouver la formule $\gamma_z^* \frac{d}{dz} - \frac{d}{dz}\gamma_z^* = (\gamma_z^*)^2$.*

15.2 Les deux produits : Convolution (produit de Cauchy) et produit de Hadamard

15.2.1 Produit de Cauchy

Ce produit s'obtient facilement à partir de la notation sommatoire. On multiplie formellement les sommes. Avec $S = \sum_{n=0}^{\infty}\langle S|z^n\rangle z^n$; $T = \sum_{m=0}^{\infty}\langle T|z^m\rangle z^m$ on a

$$ST = \sum_{n,m=0}^{\infty} \langle S|z^n\rangle\langle T|z^m\rangle z^{n+m} \tag{82}$$

puis, en regroupant par degrés,

$$ST = \sum_{r=0}^{\infty} \Big(\sum_{n+m=r} \langle S|z^n\rangle\langle T|z^m\rangle \Big) z^r \tag{83}$$

Définition 15.2 *Soient S,$T \in \mathbb{C}[[z]]$. On définit le produit (de Cauchy) ou convolution de ces deux séries par la formule (83).*

$$ST = \sum_{r=0}^{\infty} \Big(\sum_{n+m=r} \langle S|z^n\rangle\langle T|z^m\rangle \Big) z^r \tag{84}$$

Exercice 15.3 SUPPORT D'UN PRODUIT. —
On rappelle que le support d'une série $R = \sum_{n\in\mathbb{N}} \langle R|z^n\rangle z^n$ est l'ensemble des $n \in \mathbb{N}$ pour lesquels $\langle R|z^n\rangle \neq 0$.
Donner les supports des séries suivantes

a) $\frac{1}{1-z^2}$ *b)* $\frac{z^k}{1+\beta z}$ *c)* $\frac{1}{1+z+z^2}$

d) $\frac{1}{1-z^3}$ *e)* $\frac{1-z}{1-z^2}$ *f)* $\frac{1}{1-z} + \frac{1}{1+z}$

Exercice 15.4 ÉTOILE D'UNE SÉRIE. —
La notion de sommabilité définie dans l'exercice (14.4) est reprise ici dans le cadre plus simple des séries complexes à une variable.
On dira qu'une famille $(S_i)_{i\in I}$ de séries est sommable *si, pour tout $n \in \mathbb{N}$, la fonction $I \mapsto \mathbb{C}$ define par $i \mapsto \langle S_i|z^n\rangle$ est à support fini. Dans ce cas, on dira que la famille $(S_i)_{i\in I}$ est de somme S définie par $\langle S|z^n\rangle = \sum_{i\in I}\langle S_i|z^n\rangle$. On notera $S = \sum_{i\in I} S_i$*

1) Soit $T \in \mathbb{C}[[z]]$ et S_i sommable. Montrer que TS_i est sommable et que $\sum_{i\in I} TS_i = T\sum_{i\in I} S_i$.
2) a) Soit $S \in \mathbb{C}[[z]]$ une série sans terme constant (formellement $\langle S|z^0\rangle = 0$), montrer que la famille $(S^k)_{k\in\mathbb{N}}$ est sommable.
b) Montrer que $\sum_{k\in\mathbb{N}} S^k = (1-S)^{-1}$ dans $\mathbb{C}[[z]]$.
3) En posant $S = a_0 + S^+$ où $a_0 = \langle S|z^0\rangle$ et $S^+ = S - a_0 = \sum_{n>0}\langle S|z^n\rangle z^n$, montrer la proposition (15.5).

Proposition 15.5 SÉRIES INVERSIBLES. — *Soit $S \in \mathbb{C}[[z]]$, S est inversible dans $\mathbb{C}[[z]]$ ssi son terme constant $\langle S|z^0\rangle$ l'est.*

Exercice 15.6 *1) Fontaine de pièces de Wilf (donné en cours).*
2) Polyominos tas stricts (donné dans la présentation du cours).

15.2.2 Séries rationnelles

Définition 15.7 *Une série $S \in \mathbb{C}[[z]]$ est dite rationnelle si elle peut s'exprimer sous la forme $S = \frac{P}{Q};\ P,Q \in C[z];\ Q(0) \neq 0$.*

Nous allons voir trois caractérisations (très importantes) des séries rationnelles :

- **Rat**. — Fraction rationnelle $S = \frac{P}{Q};\ Q(0) \neq 0$
- **Coeff**. — Coefficients $\langle S|z^n\rangle = \sum_{(s,\lambda)\in F} \alpha(s,\lambda) n^s \lambda^n$, avec F fini.
- **Rec**. — Récurence linéaire

$$(\exists(\alpha_0,\alpha_1,\cdots\alpha_k) \in \mathbb{C}^{k+1})(\forall n \in \mathbb{N})(\langle S|z^{n+k}\rangle = \sum_{j=0}^{k-1} \alpha_j \langle S|z^{n+j}\rangle)$$

les étudiants devront être maîtres du passage de l'une des ces formes à l'autre. Nous allons les détailler maintenant.
Rat→**Rec**. — Comme $Q(0) \neq 0$, on met la fraction $\frac{P}{Q}$ sous la forme

$$\frac{N(z)}{1 - \sum_{j=1}^{m} \beta_j z^j} \tag{85}$$

(en divisant haut et bas par $Q(0)$). Une fois ceci fait, on a

$$S(1-\sum_{j=1}^{m}\beta_j z^j) = S - S(\sum_{j=1}^{m}\beta_j z^j) = N(z) \tag{86}$$

soit

$$S = S(\sum_{j=1}^{m}\beta_j z^j) + N(z) \tag{87}$$

Maintenant, pour $k \geq sup(\deg(N(z)),m)$, on a $\langle N|z^{n+k}\rangle = 0$ d'où

$$\langle S|z^{n+k}\rangle = \sum_{j=1}^{n}\beta_j\langle z^j S|z^{n+k}\rangle = \sum_{j=1}^{n}\beta_j\langle S|z^{n+k-j}\rangle \tag{88}$$

qui est la récurrence linéaire cherchée.

Exercice 15.8 *Les nombres de Fibonacci sont donnés par la récurrence*

$$F_0 = 0,\, F_1 = 1;\; F_{n+2} = F_n + F_{n+1} \tag{89}$$

a) Redémontrer que la série génératrice des nombres de Fibonacci est $S(z) = \frac{z}{1-z-z^2}$.
b) En déduire que celle des nombres de Fibonacci impairs $T(z) = \sum_{n\geq 0} F_{2n+1}z^n$ *est* $\frac{1}{1-3z+z^2}$
c) En déduire la relation de récurrence satisfaite par ces nombres (les $a_n = F_{2n+1}$*).*

Rec→Rat. — Soit S qui vérifie la relation de récurrence linéaire, donnée par des coefficients $(\alpha_0,\alpha_1,\cdots\alpha_k) \in \mathbb{C}^k$,

$$(\forall n \in \mathbb{N})(\langle S|z^{n+k}\rangle = \sum_{j=0}^{k-1}\alpha_j\langle S|z^{n+j}\rangle) \tag{90}$$

on a , pour tout n,

$$\langle(\gamma_z^*)^k S|z^n\rangle = \sum_{j=0}^{k-1}\alpha_j(\gamma_z^*)^j\langle S|z^n\rangle \tag{91}$$

soit

$$(\gamma_z^*)^k S - \sum_{j=0}^{k-1}\alpha_j(\gamma_z^*)^j S = 0 \tag{92}$$

si on fait $z^m(\gamma_z^*)^m S$ on obtient la série privée de ses m premiers termes, soit le reste d'ordre m $S - \mathrm{trunc}(S,m-1)$ (où $\mathrm{trunc}(S,l) = \sum_{n=0}^{l}\langle S|z^n\rangle z^n$ est l'opérateur de troncature). En multipliant l'équation précédente par z^k on obtient

$$0 = z^k(\gamma_z^*)^k S - \sum_{j=0}^{k-1}\alpha_j z^{k-j}z^j(\gamma_z^*)^j S = S - \mathrm{trunc}(S,k-1) - \sum_{j=0}^{k-1}\alpha_j z^{k-j}(S - \mathrm{trunc}(S,j-1)) \tag{93}$$

soit

$$S\Big(1-\sum_{j=0}^{k-1}\alpha_j z^{k-j}\Big)=\mathrm{trunc}(S,k-1)-\sum_{j=0}^{k-1}\alpha_j z^{k-j}\mathrm{trunc}(S,j-1) \tag{94}$$

dont le second membre est un polynôme. Ce qui est la forme cherchée

$$S=\frac{\mathrm{trunc}(S,k-1)-\sum_{j=0}^{k-1}\alpha_j z^{k-j}\mathrm{trunc}(S,j-1)}{1-\sum_{j=0}^{k-1}\alpha_j z^{k-j}} \tag{95}$$

Exercice 15.9 *En calculant $F_{n+3}^2-F_{n+2}^2$ trouver une relation de récurrence entre les $a_n=F_n^2$. Calculer la fraction rationnelle $\sum_n F_n^2 z^n$*

Rat→Coeff. — On utilise la décomposition en éléments simples

$$\frac{P}{Q}=E(x)+\sum_{\lambda\in\mathcal{O}_Q}\sum_{j=1}^{n_\lambda}\frac{\alpha(\lambda,j)}{(z-\lambda)^j} \tag{96}$$

il suffit donc de savoir calculer les coefficients du développement de chaque $\frac{1}{(z-\lambda)^j}$ avec $\lambda\neq 0$.

Exercice 15.10 *1) a) Montrer que $\frac{d^k}{dz^k}(1-\beta z)^{-1}=k!\beta^k(1-\beta z)^{-(k+1)}$.*
b) Montrer que $\frac{d^k}{dz^k}(1-\beta z)^{-1}=\sum_{n=k}^{\infty}n(n-1)\cdots(n-k+1)\beta^n z^{n-k}$.
On adopte les notations commodes suivantes
`http://mathworld.wolfram.com/FallingFactorial.html`
Factorielle descendante $(x)_k=x(x-1)\cdots(x-k+1)$
Factorielle ascendante $x^{(k)}=x(x+1)\cdots(x+k-1)$
Binomial généralisé $\left(\begin{array}{c}x\\k\end{array}\right)=\frac{1}{k!}(x)_k=\frac{x(x-1)\cdots(x-k+1)}{k!}$

2) Déduire du (1.b) que

$$\frac{1}{(1-\beta z)^{k+1}}=\sum_{n=k}^{\infty}\left(\begin{array}{c}n\\k\end{array}\right)\beta^{n-k}z^{n-k}=\sum_{m=0}^{\infty}\frac{m^{(k)}}{k!}\beta^m z^m \tag{97}$$

Exercice Machine 15.11 *On veut convertir les factorielles montantes sur la base des puissances. La clef est le triangle des nombres de Stirling de 1ère espèce.*
1) a) Lire et interpréter les résultats du programme suivant

```
> with(combinat);
```

$$[\mathrm{Chi}, bell, \mathrm{binomial}, cartprod, character, choose, composition, conjpart, decodepart, encodepart, fibonacci, firstpart, graycode, inttovec, lastpart, multinomial, nextpart, numbcomb, numbcomp, numbpart, numbperm, partition, permute, powerset, prevpart, randcomb, randpart, randperm, setpartition, stirling1, stirling2, subsets, vectoint]$$

```
> rf:=proc(x,k) product(x+j,j=0..k-1) end;
```

$$rf := \textbf{\textit{proc}}(x,k)\,\mathrm{product}(x+j,j=0..k-1)\ \textbf{\textit{end proc}}$$

```
> rf(x,5);
```

$$x\,(x+1)\,(x+2)\,(x+3)\,(x+4)$$

```
> seq(print(expand(rf(x,k))),k=0..7);
```

$$1$$
$$x$$
$$x^2+x$$
$$x^3+3\,x^2+2\,x$$
$$x^4+6\,x^3+11\,x^2+6\,x$$
$$x^5+10\,x^4+35\,x^3+50\,x^2+24\,x$$
$$x^6+15\,x^5+85\,x^4+225\,x^3+274\,x^2+120\,x$$
$$x^7+21\,x^6+175\,x^5+735\,x^4+1624\,x^3+1764\,x^2+720\,x$$

```
> seq(print(seq(stirling1(n,k),k=0..n)),n=0..7);
```

$$1$$
$$0,1$$
$$0,\ -1,1$$
$$0,2,\ -3,1$$
$$0,\ -6,11,\ -6,1$$
$$0,24,\ -50,35,\ -10,1$$
$$0,\ -120,274,\ -225,85,\ -15,1$$
$$0,720,\ -1764,1624,\ -735,175,\ -21,1$$

b) Se renseigner sur les nombres de Stirling de première espèce (par exemple dans les livres ou dans `http://mathworld.wolfram.com/StirlingNumberoftheFirstKind.html`*) et donner l'expression de $x^{(k)}$ en fonction des puissances de x.*
2) On appelle Série Quasi-Polynôme (SQP), une série $P(l,\alpha,z)=\sum_{n=0}^{\infty} n^l\alpha^n z^n$ avec $\alpha\neq 0$.
a) Calculer le produit $P(l_1,\alpha_1,z)P(l_2,\alpha_2,z)$.
b) Exprimer la SGO des nombres de Fibonacci en fonction de deux SQP.
c) Déduire de la question (1) une expression des éléments simples $\frac{1}{(1-\alpha z)^{k+1}}$ en fonction des SQP ($P(l,\alpha,z)=\sum_{n=0}^{\infty} n^l\alpha^n z^n$).

Note 15.12 *On peut montrer que les fonctions $P(l,\alpha,z)$ sont linéairement indépendantes et forment une base des fractions rationnelles sans pôle nul ni partie entière. Ce qui précède montre qu'elles forment une* base multiplicative *de cet espace.*

Coeff→Rat. —

Exercice 15.13 *On suppose qu'à partir d'un certain rang les coefficients de la série S sont une combinaison linéaire d'expressions du type $n^l\alpha^n$.*
1) Montrer que S se décompose de façon unique comme

$$S=P(z)+\sum_{(l,\alpha)\in F}\beta(l,\alpha)P(l,\alpha,z) \tag{98}$$

où P est un polynôme.

Exercice Machine 15.14 *1) a) Lire et interpréter le programme suivant.*

```
> S1:=matrix(10,10,(i,j)->stirling1(i-1,j-1));
```

$$S1 := \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & -3 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -6 & 11 & -6 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 24 & -50 & 35 & -10 & 1 & 0 & 0 & 0 & 0 \\ 0 & -120 & 274 & -225 & 85 & -15 & 1 & 0 & 0 & 0 \\ 0 & 720 & -1764 & 1624 & -735 & 175 & -21 & 1 & 0 & 0 \\ 0 & -5040 & 13068 & -13132 & 6769 & -1960 & 322 & -28 & 1 & 0 \\ 0 & 40320 & -109584 & 118124 & -67284 & 22449 & -4536 & 546 & -36 & 1 \end{bmatrix}$$

```
> S2:=matrix(10,10,(i,j)->stirling2(i-1,j-1));
```

$$S2 := \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 3 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 7 & 6 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 15 & 25 & 10 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 31 & 90 & 65 & 15 & 1 & 0 & 0 & 0 \\ 0 & 1 & 63 & 301 & 350 & 140 & 21 & 1 & 0 & 0 \\ 0 & 1 & 127 & 966 & 1701 & 1050 & 266 & 28 & 1 & 0 \\ 0 & 1 & 255 & 3025 & 7770 & 6951 & 2646 & 462 & 36 & 1 \end{bmatrix}$$

```
> multiply(S1,S2);
```

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

b) Les nombres de Stirling de deuxième espèce $stirling2(n,k)$ *avec* $n,k \in \mathbb{N}$ *forment la matrice inverse de celle des nombres de première espèce. On peut voir cela come une relation entre patrice infinies ou bien comme une infinité de relations au sens suivant.*
Soient les matrices de $\mathbb{Z}^{(N+1)\times(N+1)}$*,*

$$S1(N) = (stirling1(n,k))_{0\le n,k\le N} \text{ et } S2(N) = (stirling2(n,k))_{0\le n,k\le N} \qquad (99)$$

alors $S1S2 = I_{(N+1)\times(N+1)}$.
2) Soit $\underline{P}(l,\alpha,z) = \sum_{n=l}^{\infty}(n)_l\,\alpha^n z^n$.
a) Exprimer les $\underline{P}(l,\alpha,z)$ *en fonction des* $P(l',\alpha',z)$*. Écrire soigneusement la matrice de passage.*

b) À l'aide des nombres de Stirling de deuxième espèce, exprimer les $P(l,\alpha,z)$ en fonction des $\underline{P}(l',\alpha',z)$.
3) Déduire de tout ce qui précède une méthode pour exprimer S comme une fraction rationnelle.

Remarque 15.15 *Les passages* **Rec**→**Coeff** *et* **Coeff**→**Rec** *se font par composition des méthodes précédentes. Si l'on tient à des méthodes directes (mais pas nécessairement plus courtes ni plus élégantes), on peut aussi, pour le premier, utiliser une réduction de Jordan de la matrice compagnon associée à la récurrence et utiliser des produits de Hadamard (cf paragraphe (15.2.4)) pour le second.*

15.2.3 Séries rationnelles (repésentations linéaires et aspect automatique)

Avant de généraliser la théorie des séries rationnelles à plusieurs variables (non-commutatives), il est utile de voir comment elles peuvent se représenter par un automate (unaire et à mltiplicités). On a la proposition suivante (énoncée dans le cas général où l'ensemble des scalaires K est un corps commutatif quelconque)

Proposition 15.16 *Soit $S \sum_{n\in\ N} a_n z^n \in K\langle\langle z\rangle\rangle$ une série. Les conditions suivantes sont équivalentes*
i) S est rationnelle, c'est à dire $S = P(Q)^{-1}$ où P,$Q \in K\langle z\rangle$ et $Q(0) \neq 0$
ii) Les coefficients de S vérifient une récurrence linéaire

$$(\exists(\alpha_j)_{0\leq j<k} \in K^k)(\forall n \in \mathbb{N})(a_{n+k} = \sum_{j=0}^{k-1} \alpha_j a_{n+j}) \tag{100}$$

iii) Il existe $\lambda \in K^{1\times n}$, $T \in K^{n\times n}$,$\gamma \in K^{n\times 1}$ tels que

$$(\forall n \in \mathbb{N})(a_n = \lambda T^n \gamma) \tag{101}$$

Preuve — ii) $\Longrightarrow$ iii). —
La relation de récurrence linéaire implique

$$(a_{n+1},a_{n+2}\cdots,a_{n+k}) = (a_n,a_{n+1}\cdots,a_{n+k-1}) \begin{pmatrix} 0 & 0 & \cdots & \cdots & 0 & \alpha_0 \\ 1 & 0 & \ddots & & \vdots & \vdots \\ 0 & 1 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 & \vdots \\ \vdots & \vdots & & \ddots & 0 & \alpha_{k-2} \\ 0 & 0 & \cdots & \cdots & 1 & \alpha_{k-1} \end{pmatrix} \tag{102}$$

soit, en posant T, la matrice et $v_n = (a_n,a_{n+1}\cdots,a_{n+k-1})$, $v_{n+1} = v_n T$, d'où $v_n = v_0 T^n$. On a finalement

$$a_n = v_n \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = (a_0,a_1\cdots,a_{k-1})T^n \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \tag{103}$$

iii) $\Longrightarrow$ i). —
En effet, $S = \sum_n a_n z^n = \sum_n \lambda T^n \gamma z^n = \lambda(\sum_n T^n z^n)\gamma = \lambda(I - zT)^{-1}\gamma$. Mais

$$(I - zT)^{-1} = \frac{1}{det(I - zT)} \text{comatrice}(I - zT) \tag{104}$$

et les $Q(z) = det(I - zT)$ est un polynôme en z tel que $Q(0) = 1$ et comatrice(I-zT) est une matrice de polynômes en z (exercice !!). D'où le résultat.
i) $\Longrightarrow$ ii). —
On peut poser $Q(z) = \sum_{j=0}^{k-1} \beta_j z^j$ avec $\beta_0 = 1$. Comme $P = SQ$, pour tout $n \in \mathbb{N}$, on a $\langle P|z^n\rangle = \sum_{p+q=n} \beta_p a_q$, soit, si $n > N = max(\deg(P),k)$, $\sum_{p+q=n} \beta_p a_q = 0$ ce qui peut encore s'écrire $a_n = -\sum_{j=1}^{k} \beta_j a_{n-j}$, ce qui donne, pour tout $n \in \mathbb{N}$,

$$a_{n+N} = -\sum_{j=1}^{k} \beta_j a_{n+N-j} \tag{105}$$

ce qui entraine (ii). ♣

Définition 15.17 *Un triplet $\mathcal{T} = (\lambda,T,\gamma)$ tel que $\langle S|z^n\rangle = \lambda T^n \gamma$ est appellé* repésentation linéaire *de dimension n de S. De même S est appelée* comportement *de $\mathcal{T}$.*

Note 15.18 *Une série rationnelle admet en général plusieurs représentations linéaires. La dimension minimale de ces représentations est appellée* rang *de S. C'est aussi la dimension de l'espace vectoriel engendré par les décalées de S.*

15.2.4 Produit de Hadamard

C'est juste le produit des fonctions (fonctions "coefficient"), il sera noté $\odot$. Par exemple pour les séries d'une variable on a

$$\sum_{n=0}^{\infty} a_n z^n \odot \sum_{n=0}^{\infty} b_n z^n = \sum_{n=0}^{\infty} a_n b_n z^n \tag{106}$$

Exercice 15.19 *Effectuer les produits de Hadamard suivants*

a) $\frac{1}{1-z^2} \odot \frac{1}{1-2z}$ *b)* $\frac{1}{1+z+z^2} \odot \frac{1}{1-2z}$ *c)* $\frac{1}{1+z+z^2} \odot f(z)$

d) $\frac{1}{1-z^2} \odot e^z$ *e)* $\frac{z}{1-z^2} \odot e^z$ *f)* $\frac{1}{1-z} \odot f(z)$

Montrer que le résultat de (c) est rationnel si $f(z)$ est rationnelle i.e. si $f(z) = \frac{P(z)}{Q(z)}$; $Q(0) \neq 0$
indication. *— Pour le (b), décomposer en éléments simples. Pour le (c) on pourra remarquer que $\frac{1}{1+z+z^2} = \frac{1-z}{1-z^3}$.*

Théorème 15.20 PRODUIT DE HADAMARD DE SÉRIES RATIONNELLES. —
Soient $S,T \in \mathbb{C}[[z]]$ rationnelles. Alors $S \odot T$ est rationnelle.

Preuve — On peut remarquer qu'une série $R \in \mathbb{C}[[z]]$ est rationnelle ssi l'ensemble de ses décalées $(\gamma_z^*)^k R$ est de rang fini. Comme $\gamma_z^*(U \odot V) = \gamma_z^*(U) \odot \gamma_z^*(V)$, on a le résultat.

Références

[1] COHEN H., *A Course in Computational Algebraic Number Theory*. Springer (1993)

[2] CHAR B.W., GEDDES K.O., GONNET G.H., ALI.., *Maple V Library Reference Manual*, Springer (1992).

[3] CHAR B.W., GEDDES K.O., GONNET G.H., ALI.., *Maple V Language Reference Manual*, Springer (1992).

[4] DAVENPORT J., SIRET Y., TOURNIER E., *Calcul formel*, Masson (1986)

[5] DEMAZURE M., Cours d'algèbre : Divisiilité, Primalité, codes. Cassini (1997).

[6] VON ZUR GATHEN J. AND GERAHRD J. Modern Computer Algebra. Cambridge (1999).

[7] KNUTH D., *The art of computer programming* Tome I. Addison-Wesley (1981)

[8] KNUTH D., *The art of computer programming* Tome II. Addison-Wesley (1981)

[9] NAUDIN P., QUITTÉ C., *Algorithmique Algébrique* Masson (1992)