CALCULABILITE DANS LES STRUCTURES ALGEBRIQUES DENOMBRABLES

Abstract

Computability in Countable algebraic structures

We study the computability in discrete enumerable algebraic structures from the viewpoint of a given class of constructions $\mathcal{C}$. Our walk is to relativize for the class $\mathcal{C}$ the methods of constructive mathematics. The most important class we study is $\mathcal{P}$: the class of polynomial time computable functions.

We introduce the notion of *completely* $\mathcal{C}$*-computable algebraic structure* (the $\mathcal{C}$-computability of evaluation of formulas). We prove that the most elementary algebraic structures are *completely* $\mathcal{P}$*-computable in a natural sense.* For example the natural completely $\mathcal{P}$-computable presentation of the ring of polynomials with integer coefficients is the usual one (dense presentation with integers in binary).

We study the $\mathcal{P}$-computability of linear algebra. For commutative rings, we give strong links between the three notions:

- $\mathcal{P}$-computability of determinants
- $\mathcal{P}$-computability of the product of a list of matrices
- $\mathcal{P}$-computability of addition, multiplication, exact division, and $\mathcal{P}$-majoration of determinants (in the case of an integral domain).

(these links are often given for the arithmetic complexity only).

Résumé

Cette étude est consacrée aux ensembles discrets énumérables lorsqu'on adopte le point de vue des constructions d'une classe donnée $\mathcal{C}$. La classe que nous avons essentiellement en vue est celle des constructions en temps polynomial. La démarche générale que nous suivons est de relativiser à une classe de construction donnée les méthodes de mathématiques constructives.

Dans le A , nous donnons les définitions de base, et quelques résultats élémentaires.

Dans le B , nous nous intéressons aux structures algébriques dénombrables effectives.

Les notions de "calcul algébrique", "calcul algébrique formel" et "calcul de classe $\mathcal{C}$" interfèrent alors entre elles. Cela nous amène à la notion de "structure algébrique complètement $\mathcal{C}$-calculable", qui s'avère être une bonne notion. Par définition, une présentation d'une structure algébrique est complètement $\mathcal{C}$-calculable lorsque l'évaluation des formules est $\mathcal{C}$-calculable. Nous établissons donc un lien entre la notion introduite et les présentations "par formule" ou "en magma" (§ e).

Nous montrons que les structures algébriques les plus élémentaires sont complètement $\mathcal{P}$-calculables, et en général "de manière naturelle". Cela implique qu'il y a une $\mathcal{P}$-présentation naturellement attachée à une structure algébrique élémentaire. Par exemple la $\mathcal{P}$-présentation naturelle de $(\mathbb{N}, 0, 1, +)$ est la présentation en unaire, tandis que la présentation naturelle de $(\mathbb{N}, 0, 1, +, \times)$ est la présentation en binaire.

De nombreuses structures algébriques "libres de type fini" sont complètement $\mathcal{P}$-calculables et ont une structure de $\mathcal{P}$-calculabilité naturelle. Par exemple les algèbres de polynômes (à un nombre fini d'indéterminées) sur $\mathbb{Z}$, $\mathbb{Q}$ ou sur un anneau fini. Un quotient d'une de ces algèbres sera également complètement $\mathcal{P}$-calculable lorsque l'idéal noyau est une partie $\mathcal{P}$-détachable de l'algèbre des polynômes.

Il semble très improbable que la clôture algébrique de $\mathbb{Q}$ puisse être présentée de manière complètement $\mathcal{P}$-calculable; nous donnons néanmoins un exemple (en B.g) d'extension algébrique infinie de $\mathbb{Q}$ présentée de manière que l'addition et le produit y soient complètement $\mathcal{P}$-calculables.

Dans le C , qui peut être lu à peu près indépendamment du B , l'objectif est de montrer que l'algèbre linéaire "classique" est une algèbre en temps polynomial.

Nous construisons un bon stock d'anneaux commutatifs sur lesquels "le calcul des déterminants est en temps polynomial", à peu de chose près les mêmes que ceux qui ont été montrés complètement $\mathbf{P}$-calculables dans la partie B . Nous mettons en évidence le lien étroit entre la calculabilité des déterminants en temps polynomial d'une part et la calculabilité du produit d'une liste de matrices en temps polynomial d'autre part.

Enfin, nous étudions en détail la méthode du pivot améliorée à la Bareiss et sa calculabilité en temps polynomial.

I N T R O D U C T I O N

Les mathématiques "ordinaires" ont un contenu constructif. Telle est du moins la thèse des mathématiques constructives (cf. [**CA**] et [**CAL**] pour une mise en pratique de cette thèse). Cette affirmation peut être interprétée de la manière suivante: tout théorème de mathématiques "ordinaires" , affirmant l'existence de certains objets "concrets" vérifiant certaines propriétés sous certaines hypothèses, doit pouvoir être *réalisé* sous forme d'un algorithme construisant l'objet en question à partir des données fournies dans les hypothèses. En général une preuve constructive d'un théorème fournit de manière immédiate un algorithme primitif récursif qui réalise le théorème en question.

Cette étude (et d'autres dans la même série) se situe dans le contexte général suivant: expliciter, dans les mathématiques ordinaires, les théorèmes qui peuvent être réalisés par des algorithmes de complexité "faible" (en temps polynomial par exemple). Il nous a semblé naturel de prendre une base de mathématiques constructives pour développer ce travail.

Dans cette étude, consacrée aux structures algébriques dénombrables, nous poursuivons les deux objectifs suivants:

- expliciter les interférences entre calcul algébrique et calculabilité au sens de la complexité
- expliciter dans quelle mesure l'algèbre linéaire ordinaire est en temps polynomial.

La démarche générale que nous suivons est de relativiser à une classe de construction donnée les méthodes de mathématiques constructives.

Nous utiliserons les mathématiques constructives de manière informelle[1] (c.-à-d. comme un mathématicien classique utilise la théorie des ensembles).

Disons en très bref que les mathématiques constructives dans le style Bishop n'énoncent que des théorèmes ayant une signification algorithmique. Elles fournissent donc, selon nous, une base naturelle pour tout travail mathématique centré sur la discussion d'algorithmes.

Nous indiquons maintenant deux ou trois définitions sensibles de mathématiques constructives, parce qu'elles nous guideront lorsque nous restreindrons les constructions à une classe préétablie.

---

[1] Les logiciens ont pour leur part beaucoup travaillé sur des systèmes formels qui peuvent rendre compte des mathématiques pratiquées dans un livre tel que [**CA**] (le premier livre de Bishop date de 1967, et la logique intuitionniste de Heyting date de 1930). On pourra par exemple consulter [**FCM**] à ce sujet.

Les notions de construction ou opération sont considérées comme des *notions premières, non définies,* au même titre que la notion d'entier naturel .

Constructivement, un ensemble $(X, \neq_X)$ est donné lorsque:

- on décrit ce qu'il faut faire pour construire un objet de l'ensemble X .
- on décrit, concernant les objets de X , une **relation de séparation** , notée $\neq_X$, et vérifiant les propriétés suivantes (axiomes pour une relation de séparation):

  pour tous x , y , z dans X

  i. $x \neq_X x$ est absurde

  ii. $x \neq_X y$ équivaut à $y \neq_X x$

  iii. $x \neq_X y$ implique $x \neq_X z$ ou $y \neq_X z$

NB: le "ou" , dans iii. , est un "ou" constructif, c.-à-d. doit pouvoir être constaté comme résultat d'une construction.

On définit alors une **relation d'égalité**, notée $x =_X y$, par : " $x \neq_X y$ est absurde ". Cette égalité de X est une relation d'équivalence[2].

Un ensemble $(X, \neq_X)$ est appelé **discret** , lorsque, pour tous x et x' dans X , on a : $x \neq_X x'$ ou $x =_X x'$. L'ensemble des nombres réels "n'est pas" discret dans la mesure où on ne sait pas décider "en général" si 2 réels donnés sont égaux ou séparés.

On appelle **fonction** de l'ensemble $(X, \neq_X)$ vers l'ensemble $(Y, \neq_Y)$ une opération de X vers Y qui vérifie la propriété d'extensionnalité suivante :

$$F(x) \neq_Y F(x') \Rightarrow x \neq_X x'.$$

Une fonction $f : X \longrightarrow Y$ est dite **surjective** si on connait une opération r de Y vers X vérifiant : pour tout $y \in Y$, $f(r(y)) =_Y y$. Notez que r n'est pas nécessairement une fonction.

Une **énumération** d'un ensemble X est à très peu de choses près une application surjective de $\mathbb{N}$, ensemble des entiers naturels, sur X : elle est donnée précisément comme suit :

- une fonction $f : \mathbb{N} \longrightarrow X \cup \{u\}$ et une opération $r : X \longrightarrow \mathbb{N}$ qui vérifient : pour tout x de X , on a $f(r(x)) =_X x$.

L'objet u est extérieur à X, il a été rajouté pour le cas où on ne sait pas a priori si X est vide ou non . Si X est "habité", c.-à-d. si on connait un élément de X , il revient au même de dire qu'il existe une application surjective de $\mathbb{N}$ sur X . L'opération r n'est pas nécessairement une fonction. Un ensemble qui possède une énumération est dit **énumérable**.

Si maintenant nous considérons une classe de constructions $\mathcal{C}$, et que nous estimons que seules les constructions de cette classe sont acceptées, nous obtenons la notion correspondante de $\mathcal{C}$-ensemble, ou ensemble $\mathcal{C}$-présenté.

Par exemple, si nous considérons les constructions faisables par une machine de Turing, nous aurons une notion d'ensemble "récursivement présenté".

Pour ce qui concerne une version relativisée à $\mathcal{C}$ de la notion d'ensemble discret, nous demanderons que l'alternative $x \neq_X x'$ ou $x =_X x'$ puisse être tranchée au moyen d'une $\mathcal{C}$-construction à partir des entrées x et x' . Si nous voulions relativiser à $\mathcal{C}$ la notion de

---

2 Cette étude est consacrée aux ensembles discrets énumérables ; dans ce cas (et dans celui des espaces métriques), il y a une relation de séparation au sens constructif. Dans [**CA**] , Bishop donne une définition de la notion d'ensemble basée sur une relation d'égalité plutôt que de séparation.

relation de séparation, sans hypothèse de discrétion, le problème serait plus délicat, et la réponse à apporter n'est peut-être pas unique[3].

[3] Signalons néanmoins que la notion d'espace métrique séparable complet se laisse relativiser à une classe $\mathbf{C}$ de manière simple et directe, ce qui permet de traiter dans ce cadre une grande partie de l'analyse. Par exemple on a des définitions naturelles de $\mathbf{C}$-nombre réel ou de $\mathbf{C}$-fonction continue de $[0,1]$ vers $\mathbb{R}$.

A) GENERALITES SUR LES $\mathcal{C}$-ENSEMBLES-DISCRETS

Nous supposerons que la classe de constructions $\mathcal{C}$ concerne des objets du type "mots sur un alphabet fini". Plus précisément, pour tous alphabets finis A et B, si A* désigne le langage engendré par A, nous supposons définies les constructions de classe $\mathcal{C}$ de A^{*k} vers B*.

a) Quelques classes de constructions intéressantes

Stabilité par composition

Comme nous avons en vue des classes de constructions qui fournissent des opérations de A^{*k} vers B*, la question de la stabilité de ces opérations par composition se pose naturellement. Ce n'est pas le cas lorsqu'on étudie les algorithmes comme "sélecteurs de langage".

Or, des classes de complexité comme **DTIME**(n^2) ne sont pas stables par composition. Nous introduisons donc pour remédier à cet inconvénient des classes de complexité où la taille de la sortie est mieux majorée que le temps de calcul, ou l'espace de calcul.

Nous notons **SPACERES**(f) la classe des algorithmes où la taille de la sortie (space résultat) est majorée par f(n), où n est la taille de l'entrée.

Précisons ici quelques abréviations, certaines très classiques, que nous utiliserons:

DTIME(O(f)) pour $\cup_{c,a}$ **DTIME**(c+a.f)

LINTIME	= **DT1** = **DTIME**(O(n))	**DT0**	= $\cup_c$ **DTIME**(n+c)
$\mathcal{P}$	= $\cup_b$ **DTIME**($O(n^b)$)	**DTNLG**	= $\cup_b$ **DTIME**($O(n.\mathbf{lg}^b(n))$)
DSP1	= **DSPACE**(O(n))	**PSPACE**	= $\cup_b$ **DSPACE**($O(n^b)$)
RES0	= $\cup_c$ **SPACERES**(n+c)	**RES1**	= **SPACERES**(O(n))
RESP	= $\cup_b$ **SPACERES**($O(n^b)$)		
$\mathcal{P}_0$	= **RES0** $\cap$ $\mathcal{P}$	$\mathbf{DTNLG_0}$	= **DTNLG** $\cap$ **RES0**
$\mathbf{DTIME_0}(O(n^k))$	= **RES0** $\cap$ **DTIME**($O(n^k)$) etc...		
$\mathcal{P}_1$	= **RES1** $\cap$ $\mathcal{P}$	$\mathbf{DTNLG_1}$	= **DTNLG** $\cap$ **RES1**
$\mathbf{DTIME_1}(O(n^k))$	= **RES1** $\cap$ **DTIME**($O(n^k)$) etc...		

Nous ferons souvent référence également à la classe $\mathcal{P}\mathbf{r}$ des fonctions primitives récursives, et à la classe **Rec** des fonctions récursives.

Ce sont toutes des classes stables par composition. Et on a l'inclusion évidente:

PSPACE $\subset$ **RESP**.

Lorsque $\mathbb{N}$ est présenté en binaire, une opération f de $\mathbb{N}$ vers $\mathbb{N}$ est **RES0** ssi f(n) = O(n), et elle est **RES1** ssi il existe un k tel que f(n) = $O(n^k)$

Mesures de la grandeur des entrées et sorties

Par ailleurs, on a parfois intérêt à considérer une mesure de l'entrée qui ne soit pas directement la taille de l'objet (pour un type de description choisi), tout en étant polynomialement relié à la taille.

Expliquons-nous sur un exemple : considérons les algèbres $\mathbf{M_n}(\mathbb{Z})$. Pour une matrice $A = (a_{ij})$, la taille $s(A)$ dans une présentation "naturelle" , sera : $s(A) = n^2 + \Sigma s(a_{ij})$

Cependant, si nous considérons $t(A) := n + s(\Sigma |a_{ij}|)$, on peut vérifier facilement que, pour 2 matrices A et B , on obtient l'inégalité : $t(AB) \leq t(A) + t(B)$. Par ailleurs les "mesures" t et s sont polynomialement reliées. Mais avec la mesure t le produit des matrices est **RES0**, ce qui n'est pas le cas avec la mesure "naturelle" s .

Ainsi, un ensemble sera toujours présenté avec une mesure de la grandeur des objets qui le composent.

Si la mesure n'est pas précisée, c'est qu'il s'agit de la taille "naturelle" au sens de la longueur du mot utilisé pour représenter l'objet .

Notons que 2 objets de X , distincts en tant que mots de A* , mais égaux dans X , ont en général 2 mesures distinctes: par exemple un même nombre rationnel peut être représenté par 2 fractions distinctes, de tailles distinctes .

Lorsque la classe de construction $\mathfrak{C}$ considérée est une classe de complexité, il faudra la comprendre au sens de la mesure considérée lorsqu'est définie la présentation de l'ensemble étudié (comme nous venons de le faire en affirmant que le produit des matrices est **RES0** lorsqu'on utilise la mesure t) .

Hypothèses concernant la classe de constructions $\mathfrak{C}$

Nous devons expliciter quelques hypothèses générales concernant la classe $\mathfrak{C}$ des constructions considérées.

Ces hypothèses seront en quelque sorte nos "axiomes de la théorie des $\mathfrak{C}$-ensembles-discrets". Elles seront immédiatement vérifiées pour les classes que nous avons en vue. Elles permettent de faire fonctionner les constructions élémentaires concernant les $\mathfrak{C}$-ensembles-discrets. Comme nous envisageons dans nos applications essentiellement les classes $\mathfrak{P}_0$, $\mathfrak{P}_1$, $\mathfrak{P}$, **DTNLG**, **PSPACE**, $\mathbb{P}\mathbf{r}$, **Rec** , on pourrait très bien se passer de ce paragraphe, qui manifeste un souci de généralité peut-être abusif.

Nous allons formuler nos hypothèses de manière assez lâche, renvoyant un exposé plus détaillé en note (n.1).

Nous abrègerons " construction de classe $\mathfrak{C}$ " en **$\mathfrak{C}$-construction** .

Nous désignerons par A et B des alphabets finis, A* et B* les langages qu'ils engendrent.

L'ensemble **Lst** (A*), des listes d'éléments de A* (ou encore : suites finies d'éléments de A*), peut être réalisé comme une partie d'un langage A°* (où A° est obtenu en rajoutant à A des symboles représentant [,] et ;) . Si X_1 , X_2 ,..., X_n sont des parties de A*, l'ensemble $X_1 \times X_2 \times ... \times X_n$ peut être réalisé comme une partie de **Lst**(A*) (listes convenables de n éléments).

Les $\mathfrak{C}$-constructions doivent permettre d'accomplir 2 tâches :

- définir les $\mathfrak{C}$-parties des ensembles A* , et
- définir les $\mathfrak{C}$-opérations entre $\mathfrak{C}$-parties X et Y d'ensembles A* et B*, lorsqu'on a défini pour X et Y une mesure de la grandeur de leurs objets.

La mesure de la grandeur d'un objet de X ($\mathfrak{C}$-partie de A*) est toujours supposée vérifier les propriétés suivantes:

- c'est un entier naturel > 0 , et
- elle est polynomialement reliée à la taille naturelle (qui est la longueur du mot, sauf pour le mot vide v de taille 1)
- l'identité $I : x \to x$ de $(X, \| \|_{A^*})$ vers $(X, \| \|_X)$ est une $\mathbb{C}$-opération

Voici maintenant la formulation de nos hypothèses:

- **constructions élémentaires appartenant à $\mathbb{C}$**:
  toutes les constructions de la classe $\mathbf{DTNLG_0}$ sont dans $\mathbb{C}$.
- **rapport entre $\mathbb{C}$-parties et $\mathbb{C}$-opérations:**
  une partie X de A* est une $\mathbb{C}$-partie si et seulement si sa fonction caractéristique (opération de A* vers {**oui**,**non**}) est une $\mathbb{C}$-opération (ici A* est muni de la mesure naturelle).
- **propriétés de stabilité pour les $\mathbb{C}$-opérations:**
  * stabilité pour la composition.
  * stabilité pour la définition par cas :
    f et g sont 2 $\mathbb{C}$-opérations de X vers Y , sl est une $\mathbb{C}$-opération de X vers {**oui**,**non**} , on définit l'opération $h : X \to Y$, par :
    $h(x) := f(x)$ si $sl(x) =$ **oui** , et $h(x) := g(x)$ sinon
  * stabilité pour **Lst** :
    si $f : X \to Y$ est une $\mathbb{C}$-opération, il en est de même pour l'opération
    g: **Lst** $(X) \to$ **Lst** (Y) , définie par
    $g([x_1,x_2,...,x_n]) := [f(x_1),f(x_2), ... ,f(x_n)]$.

b) $\mathbb{C}$-ensembles-discrets , $\mathbb{C}$-fonctions , $\mathbb{C}$-structures algébriques

Présentation d'un ensemble énumérable

D'un point de vue constructif, les objets d'un ensemble X sont en général représentés par des mots écrits sur un alphabet fini déterminé A . Seuls certains mots de A* représentent des objets de X .

S'il existe un test (une opération) P de A* vers {**oui**,**non**} indiquant si le mot m représente ou non un objet de X , l'ensemble est alors énumérable . Lorsqu'on a ainsi décrit les objets d'un ensemble énumérable X , on dit qu'on a défini une **présentation** de X.

Tout ensemble énumérable peut naturellement être "présenté".

La catégorie des $\mathfrak{C}$-ensembles-discrets

Définition A.b1 :

Un **$\mathfrak{C}$-ensemble-discret** (ou ensemble-discret-$\mathfrak{C}$-présenté) est donné lorsque:

- on considère un alphabet fini A
- on considère une opération P_X de classe $\mathfrak{C}$ de A* vers {**oui**,**non**} acceptant un langage $X \subset A^*$: les mots de X seront les objets de l'ensemble.
- on a défini une opération V_X de classe $\mathfrak{C}$, de $X \times X$ vers {**oui**,**non**}, qui vérifie, pour tous x, y, z de X :

  $V_X(x,x) =$ **oui** , $V_X(x,y) = V_X(y,x)$,

  $V_X(x,y) = V_X(y,z) =$ **oui** $\Rightarrow$ $V_X(x,z) =$ **oui**

  (l'égalité de x et y comme éléments de X est définie par $V_X(x,y) =$ **oui**) .
- on a défini une mesure de la grandeur des mots de X , polynomialement reliée à la taille. (la mesure doit toujours être un entier > 0)

Notations : La mesure de la grandeur de l'objet x du $\mathfrak{C}$-ensemble-discret X sera en général notée $\|x\|_X$, ou plus simplement $\|x\|$.
En toute rigueur, le $\mathfrak{C}$-ensemble-discret X devrait être noté $(A, P_X, V_X, \| \ \|_X)$.

Remarque : l'identité entre mots de A* peut être $\mathfrak{C}$-testée; c'est donc une relation d'égalité possible.

Rappelons qu'une fonction de X vers Y est par définition une opération extensionnelle (c.-à-d.: qui se comporte bien par rapport aux relations de séparation définies sur X et Y). Ceci nous amène à définir la catégorie des $\mathfrak{C}$-ensembles discrets comme suit.

Définition A.b2 : Etant donnés deux $\mathfrak{C}$-ensembles-discrets X et Y , on appellera **$\mathfrak{C}$-fonction** de X vers Y une opération de classe $\mathfrak{C}$ de X vers Y qui est une fonction de X vers Y .

On a donc défini la catégorie des $\mathfrak{C}$-ensembles-discrets.

On appellera **$\mathfrak{C}$-équivalence** un isomorphisme dans cette catégorie. Lorsque on a deux classes de constructions $\mathfrak{C}_1$ et $\mathfrak{C}_2$ avec $\mathfrak{C}_1 \subset \mathfrak{C}_2$, il y a un foncteur d'oubli de la catégorie des $\mathfrak{C}_1$-ensembles-discrets vers celle des $\mathfrak{C}_2$-ensembles-discrets.

Quelques $\mathfrak{C}$-équivalences (plus de détails en note n.2)

Pour un entier n (abstrait) nous noterons **lg**(n) sa longueur lorsqu'il est écrit en binaire. L'ensemble $\mathbb{N}$ des entiers naturels présentés en binaire est une **DT0**-partie de {0,1}* , qui est **DT0**-équivalente à {0,1}* , donc $\mathfrak{C}$-équivalente à {0,1}* ($\mathfrak{C}$ contient $\mathbf{DTNLG_0}$). De même, l'ensemble $\mathbb{N}$ présenté en base b est une **DT0**-partie de A* , qui est **DT0**-équivalente à A*, où A est un alphabet à b lettres : {0,1,...,b-1} . Le changement de base de numérotation est une fonction de classe $\mathbf{DTNLG_1}$. En prenant **lg**(n) pour mesure de l'entier n écrit en base b , les présentations de $\mathbb{N}$ en binaire et en base b sont donc $\mathfrak{C}$-équivalentes. De même, en modifiant convenablement la mesure des mots dans A* , les ensembles A* sont 2 à 2 $\mathfrak{C}$-équivalents .

Soit par ailleurs $X = (A, P_X, V_X, \| \ \|_X)$ un $\mathfrak{C}$-ensemble-discret. Notons X' le $\mathfrak{C}$-ensemble-discret $X' := (A, P_X, V_X, \| \ \|_{X'})$, où seule la mesure de la grandeur des objets a été modifiée. Soit la fonction $I : x \to x$, définie de X vers X': I est une $\mathfrak{C}$-équivalence si la classe $\mathfrak{C}$ contient $\mathfrak{P}$, puisque les mesures sont polynomialement reliées entre elles. Il

est donc bien clair que l'introduction d'une mesure de la taille des objets n'a d'intérêt pratique que pour les classes de constructions strictement plus petites que $\mathbb{P}$. Dans le cas contraire, la catégorie obtenue sans introduire de mesure de la taille des objets, équivalente à la catégorie des $\mathbb{C}$-ensembles-discrets, est bien suffisante.

Sous-$\mathbb{C}$-ensembles-discrets, applications $\mathbb{C}$-surjectives, $\mathbb{C}$-quotients

Si X est le $\mathbb{C}$-ensemble-discret $(A, P_X, V_X, \| \ \|_X)$, un **sous-$\mathbb{C}$-e-d** Y de X est défini lorsqu'on a donné une $\mathbb{C}$-fonction f de X vers {**oui**,**non**}. Cela définit la $\mathbb{C}$-partie $Y := \{ x \in X ; f(x) = \textbf{oui} \}$ de A*.

On définit l'égalité et la mesure sur Y comme induites par celles de X. L'injection canonique $Y \to X$ est alors une $\mathbb{C}$-fonction. Les sous-$\mathbb{C}$-e-d de X sont stables par intersection, réunion et différence. Un sous-$\mathbb{C}$-e-d de X est encore appelé une **partie $\mathbb{C}$-détachable** de X, ou une **$\mathbb{C}$-partie** de X.

Notez que toute $\mathbb{C}$-partie Z de A* contenue dans X ne définit pas nécessairement une partie $\mathbb{C}$-détachable de X, parce que l'égalité dans X peut être plus lâche que celle dans A*, et Z n'est pas forcément saturée pour la relation d'égalité dans X.

Une $\mathbb{C}$-fonction f de X vers Y est dite **$\mathbb{C}$-surjective** lorsqu'on connait une $\mathbb{C}$-opération $r : Y \to X$ qui vérifie, pour tout y de Y : $f(r(y)) =_Y y$.
Notez que r n'est pas nécessairement une fonction.
La composée de deux fonctions $\mathbb{C}$-surjectives est une fonction $\mathbb{C}$-surjective.

Un **$\mathbb{C}$-quotient** de $X = (A, P_X, V_X, \| \ \|_X)$ est par définition un $\mathbb{C}$-ensemble-discret de la forme $X' = (A, P_X, V_{X'}, \| \ \|_X)$, où l'on a, pour tous x, y de X :

$$x =_X y \quad \Rightarrow \quad x =_{X'} y \ .$$

La projection canonique de X sur X' est alors une $\mathbb{C}$-fonction $\mathbb{C}$-surjective. Notez que $V_{X'}$ est une $\mathbb{C}$-fonction de $X \times X$ vers {**oui**,**non**}. (voir le § qui suit pour $X \times X$ comme $\mathbb{C}$-ensemble-discret)

Produit de 2 $\mathbb{C}$-ensemble-discrets , $\mathbb{C}$-structures algébriques

On a une notion naturelle de produit de 2 $\mathbb{C}$-ensembles-discrets : on écrit les mots représentant les éléments x et y de X et Y l'un à la suite de l'autre, séparés par un symbole ne faisant pas partie des alphabets utilisés. Et on pose:

$$\| (x,y) \| = \| x \| + \| y \| \ .$$

Il s'agit d'ailleurs du produit dans la catégorie des $\mathbb{C}$-ensembles-discrets pour des classes $\mathbb{C}$ comme $\mathbb{P}$, $\mathbb{P}_1$, $\mathbf{DTIME_1}(O(n^k))$, $\mathbb{P}\mathbf{r}$, **Rec**. (n.3)

A partir de ces notions de sous-$\mathbb{C}$-e-d et de produit de 2 $\mathbb{C}$-ensembles-discrets, nous pouvons parler de $\mathbb{C}$-lois de composition, de $\mathbb{C}$-relations binaires etc... et donc de $\mathbb{C}$-monoïdes, $\mathbb{C}$-groupes, $\mathbb{C}$-anneaux, $\mathbb{C}$-ensembles-ordonnés et plus généralement de **$\mathbb{C}$-structure algébrique**[4] d'un type donné .

Il faut noter qu'il s'agit de structures algébriques sur des ensembles discrets énumérables.

Chaque fois que c'est possible , nous considèrerons que les axiomes de la structure algébrique sont présentés comme purement universels: par exemple pour les groupes, anneaux

---

[4] Nous ne chercherons pas ici à donner la définition précise la plus générale possible de la notion de $\mathbb{C}$-structure algébrique. Disons que cette structure ne doit impliquer qu'un nombre fini d'ensembles, avec un nombre fini de lois de compositions, de constantes, et de relations (unaire ou binaire ou ternaire ou ...).

et corps . Ainsi, dans un $\mathfrak{C}$-groupe, non seulement la loi produit, mais aussi la loi unaire : $x \to x^{-1}$, doivent être des $\mathfrak{C}$-fonctions. (n.4)

Remarques :

1 - Dans le cas de la classe **Rec**, notre notion de **Rec**-structure est exactement équivalente à la notion de structure algébrique récursivement présentée définie dans [**F-S**].(n.5)

2 - Tout $\mathfrak{C}$-ensemble-discret définit évidemment un ensemble au sens constructif. Lorsqu'un ensemble X est déjà défini constructivement, une **$\mathfrak{C}$-présentation** de cet ensemble est donnée par : - un $\mathfrak{C}$-ensemble-discret X' d'une part, - une bijection entre X et X', d'autre part. Ainsi un $\mathfrak{C}$-ensemble-discret peut-il être considéré comme un ensemble "abstrait" muni d'une structure de $\mathfrak{C}$-calculabilité additionnelle.
De la même manière, lorsqu'un ensemble est muni d'une structure algébrique précise, nous parlerons de **$\mathfrak{C}$-présentation de cette structure algébrique** pour une $\mathfrak{C}$-présentation de l'ensemble X qui fait des lois de composition des $\mathfrak{C}$-fonctions (et des relations unaires, binaires etc ... des $\mathfrak{C}$-relations).

Structures algébriques naturellement primitives récursives

Notons $\mathbb{N}$ pour l'ensemble des entiers naturels présentés en binaire.

Si nous considérons la classe $\mathbb{P}\mathbf{r}$ des fonctions primitives récursives, nous avons immédiatement le résultat suivant (les axiomes de Peano sont là pour ça en quelque sorte...):

Si $\mathbb{N}'$ est une $\mathbb{P}\mathbf{r}$-présentation de la structure algébrique ($\mathbb{N}$, 0 , $n \to n + 1$) , alors la fonction "identité" de $\mathbb{N}$ vers $\mathbb{N}'$ est une $\mathbb{P}\mathbf{r}$-fonction[5].

De manière générale nous dirons qu'une **structure algébrique est naturellement primitive récursive** lorsque il existe une $\mathbb{P}\mathbf{r}$-présentation "naturelle" de cette structure au sens qu'elle est $\mathbb{P}\mathbf{r}$-initiale parmi toutes les $\mathbb{P}\mathbf{r}$-présentations de cette structure. (c.-à-d.: la bijection "identité" qui va de la $\mathbb{P}\mathbf{r}$-structure naturelle vers une autre $\mathbb{P}\mathbf{r}$-présentation est une $\mathbb{P}\mathbf{r}$-fonction). Il est clair que la $\mathbb{P}\mathbf{r}$-présentation "naturelle" est alors unique à $\mathbb{P}\mathbf{r}$-isomorphisme près.

Pour une autre classe de constructions $\mathfrak{C}$, nous pourrions parler de **structure algébrique naturellement de type $\mathfrak{C}$** . En fait, il s'avère que ce n'est pas "la bonne" notion. La bonne notion est celle de structure algébrique "naturellement complètement $\mathfrak{C}$-calculable", que nous étudierons au B .

Si une structure algébrique est naturellement primitive récursive, tous les automorphismes de la $\mathfrak{C}$-structure naturelle sont primitifs récursifs.

Les structures algébriques "de type fini" qui peuvent être $\mathbb{P}\mathbf{r}$-présentées possèdent une $\mathbb{P}\mathbf{r}$-présentation naturelle (la seule qu'on considère en général). (n.6) . Mais il y a des groupes de présentation finie pour lesquels l'égalité n'est pas récursivement décidable (Théorème de Novikoff), donc qui ne peuvent pas être **Rec**-présentés.

Notez que ($\mathbb{N}$, $\times$) n'est pas naturellement primitive récursive puisqu'il existe des automorphismes non primitifs récursifs de cette structure.

---

5 Divertissement mathématique : toute $\mathbb{P}\mathbf{r}$-présentation de la structure algébrique ($\mathbb{N}$, 0 , $n \to n+1$, $n \to n \dot{-} 1$) est-elle $\mathbb{P}\mathbf{r}$-équivalente à la présentation standard ?
Voici par ailleurs un exemple de structure algébrique constructivement définie qui "n'est pas" constructivement isomorphe à ($\mathbb{N}$, $n \to n + 1$): l'ensemble sous-jacent est $\mathbb{N}$, le successeur de a est $a + 1$ sauf éventuellement dans les 2 cas suivants : si a est le 1er contre-exemple à la conjecture de Machin-Bidule, le successeur de a est 0, et le successeur de $a - 1$ est $a + 1$. Dans cet exemple, la fonction successeur est bien définie, mais on ne sait pas déterminer un élément n'ayant pas de prédécesseur tant qu'on n'a pas résolu la conjecture de Machin-Bidule.

Problème ouvert : construire un groupe de présentation finie pour lequel l'égalité est récursive mais pas primitive récursive. (si la réponse est positive cela donne un exemple de groupe discret **Rec**-présenté mais qui ne peut pas être $\mathbb{P}\mathbf{r}$-présenté)
NB: comme la plupart des problèmes ouverts signalés dans ce texte, celui-ci n'est pas "garanti ouvert" par l'auteur.

Sous-structures et structures quotients

Etant donnée une $\mathfrak{C}$-structure algébrique X , si Y est une partie $\mathfrak{C}$-détachable qui est une sous-structure , on obtient de manière évidente une $\mathfrak{C}$-présentation de la structure algébrique Y , on dit que Y est une **$\mathfrak{C}$-sous-structure** de X .

On définit de même une notion de **$\mathfrak{C}$-structure-quotient** lorsqu'un $\mathfrak{C}$-quotient est une structure quotient.

$\mathfrak{C}$-sous-structures et $\mathfrak{C}$-structures-quotients vérifient les propriétés caractéristiques universelles habituelles.

Pour qu'un quotient d'un $\mathfrak{C}$-groupe soit un $\mathfrak{C}$-quotient il faut et suffit que le noyau de la projection soit un $\mathfrak{C}$-sous-groupe, c.-à-d. un sous-groupe $\mathfrak{C}$-détachable.

°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°

Désormais, sauf mention explicite du contraire, nous utiliserons "ensemble" pour "ensemble discret", et "$\mathfrak{C}$-ensemble" pour "$\mathfrak{C}$-ensemble-discret".

°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°

c) Entiers naturels

Présentation en unaire

Nous noterons $\mathbb{N}_1$ l'ensemble des entiers naturels présenté en unaire, par exemple sous forme {1}* ou sous forme **Lst** (c.-à-d. **Lst**(alphabet vide)), ou sous toute autre forme $\mathfrak{C}$-équivalente .

La structure algébrique ($\mathbb{N}_1$, 0 , 1 , + , $\dot{-}$, **div , mod** , >) est une $\mathfrak{P}_0$-structure; le produit est $\mathfrak{P}$ mais pas **RES1**. (a $\dot{-}$ b est égal à a – b si a > b , et à 0 sinon)

Présentation en binaire

Nous noterons $\mathbb{N}$ l'ensemble des entiers naturels présenté en binaire, ou de toute autre manière $\mathfrak{C}$-équivalente. Par exemple présenté en base b , (dès que $\mathfrak{C}$ contient $\mathbf{DTNLG_0}$), mais en prenant pour mesure, au lieu de la longueur t_0 du mot : 1 + Ent(t_0 . (log(2)/log(b))).

Du point de vue de la théorie des langages, le $\mathfrak{C}$-ensemble $\mathbb{N}$ joue un rôle essentiel du fait qu'il est $\mathfrak{C}$-équivalent à {0,1}*, ou encore à B* pour n'importe quel alphabet fini B ayant au moins 2 lettres (dès que $\mathfrak{C}$ contient $\mathbf{DTNLG_0}$).

La structure algébrique ($\mathbb{N}$, 0 , 1 , + , $\dot{-}$, $\times$, **div** , **mod** , >) est une $\mathfrak{P}_0$-structure.

Notation: nous réservons la notation **lg**(n) pour "longueur de l'entier n s'il était écrit en binaire" (même si l'entier n considéré à ce moment-là n'est pas exprimé en binaire).

Le $\mathfrak{C}$-ensemble $\mathbb{N}_1$ est $\mathfrak{C}$-équivalent à la $\mathfrak{C}$-partie $\mathbf{N}_1$ de $\mathbb{N}$ formée des puissances de 2 . Mais il n'existe pas de $\mathfrak{P}$-fonction injective de $\mathbb{N}$ vers $\mathbb{N}_1$. Les $\mathfrak{P}$-ensembles

$\mathbb{N}$ et $\mathbb{N}_1$ ne sont pas $\mathcal{P}$-équivalents. La fonction $n \to n$ de $\mathbb{N}_1$ vers $\mathbb{N}$ est une $\mathcal{P}$-fonction, mais pas une $\mathcal{P}$-équivalence.

Autres présentations

Il existe bien d'autres présentations de l'ensemble des entiers naturels, 2 à 2 non $\mathcal{P}$-équivalentes.

Par exemple on peut noter $\mathbb{N}_b$ le $\mathcal{P}$-ensemble obtenu par une présentation "en bibase b" :
un entier n est présenté sous forme d'une liste de couples (i , a_i), où i est un entier écrit en base b , et a_i est un chiffre de cette base, les i arrivant en ordre croissant, et avec : $n = \Sigma\, a_i b^i$. La structure algébrique $(\mathbb{N}_b , + , \times , >)$ est une $\mathcal{P}_1$-structure, mais rien ne va plus avec la soustraction ou la division. (cf., dans $\mathbb{N}_b$ la soustraction $b^i - 1$) . La fonction $n \to n$ de $\mathbb{N}$ vers $\mathbb{N}_b$ est une $\mathcal{P}$-fonction, mais non pas une $\mathcal{P}$-équivalence.

Nous allons voir maintenant comment la notion classique de dénombrabilité se scinde en plusieurs notions bien distinctes du point de vue constructif et du point de vue des $\mathcal{C}$-ensembles.

Enumérations[6]:

Rappelons qu'une énumération d'un ensemble X est donnée par une fonction $f : \mathbb{N} \to X \cup \{u\}$ et une opération $r : X \to \mathbb{N}$ qui vérifient : pour tout x de X , on a $r(f(x)) =_X x$. (l'objet u est extérieur à X).

Lorsque X est un $\mathcal{C}$-ensemble , f une $\mathcal{C}$-fonction et r une $\mathcal{C}$-opération, nous disons que X est **$\mathcal{C}$-énumérable**, et que **f est une $\mathcal{C}$-énumération** de X .

Toute $\mathcal{C}$-fonction surjective de $\mathbb{N}$ sur un $\mathcal{C}$-ensemble X n'est pas forcément une $\mathcal{C}$-énumération car elle peut n'être pas $\mathcal{C}$-surjective. (cf. par exemple la fonction $n \to \mathbf{lg}(n)$ de $\mathbb{N}$ vers $\mathbb{N}$: c'est une $\mathcal{P}$-fonction surjective qui n'est pas $\mathcal{P}$-surjective)

Par contre on a :

Tout $\mathcal{P}$-ensemble X est $\mathcal{P}$-énumérable.
Plus généralement , si $\mathcal{C}$ est une classe de constructions contenant $\mathcal{P}$, tout $\mathcal{C}$-ensemble X est $\mathcal{C}$-énumérable.

En effet, remarquons tout d'abord que la mesure de la grandeur des objets de X n'intervient pas, puisque nous raisonnons à une $\mathcal{C}$-équivalence près, et que $\mathcal{C}$ contient $\mathcal{P}$. D'autre part, si X est construit sur l'alphabet A , on pourra composer une $\mathcal{P}$-équivalence $\mathbb{N} \to A^*$ avec la $\mathcal{C}$-fonction de A^* dans $X \cup \{u\}$ définie comme suit:
- si $x \in X$, $x \to x$, sinon $x \to u$.
On vérifie que la composée est bien une $\mathcal{C}$-énumération.

Remarque : Un mathématicien classique qui veut se faire une idée de ce que peut bien signifier un ensemble énumérable discret pour un constructiviste peut se tenir le discours suivant : admettons une notion a priori d'effectivité (ce qui est plus facile que d'admettre une notion a priori d'ensemble à la Cantor - Zermelo - Frankel) ; notons **Constr** la classe de toutes les fonctions effectivement calculables portant sur des langages A^* ; alors la catégorie des ensembles énumérés discrets pour un constructiviste est équivalente à celle des

---

6 La terminologie énumération, dénombrement, numérotation choisie ici est "assez" arbitraire, et ne prétend naturellement pas être exhaustive.

Constr-ensembles-discrets , au sens des définitions ci-dessus, qui peuvent être lues avec des lunettes "classiques".

Dénombrements

Un **dénombrement** d'un ensemble X est par définition une énumération (f,r) de X telle que r soit une fonction.

Un ensemble discret qui possède une énumération (f,r) possède un dénombrement (f,r') : r'(x) est le plus petit entier n inférieur ou égal à r(x) tel que : $x =_X f(n)$. Par ailleurs un ensemble dénombrable X est nécessairement discret. Autrement dit, "dénombrable" équivaut à "énumérable et discret".

La notion de dénombrement, relativisée à la classe de constructions $\mathfrak{C}$, donne les notions de **$\mathfrak{C}$-dénombrement**, et de $\mathfrak{C}$-ensemble **$\mathfrak{C}$-dénombrable**.

Par le même argument que ci-dessus, tout **PSPACE**-ensemble-discret est **PSPACE**-dénombrable. Et de même pour toute classe $\mathfrak{C}$ stable par récurrence bornée (une définition par récurrence bornée est une définition par récurrence primitive où on astreint la fonction définie à rester majorée par une fonction donnée préalablement). Par contre l'ensemble énumérable $\mathbb{P}\mathbf{r}(\mathbb{N},\mathbb{N})$ des $\mathbb{P}\mathbf{r}$-fonctions de $\mathbb{N}$ vers $\mathbb{N}$ n'est pas **Rec**-dénombrable. (l'égalité n'y est pas **Rec**-décidable)

Si (f,r) est un $\mathfrak{C}$-dénombrement du $\mathfrak{C}$-ensemble X , la $\mathfrak{C}$-opération $x \to f(r(x))$ "choisit" un élément particulier dans chaque classe d'équivalence de la relation $=_X$. Autrement dit, les différents "représentants" d'un élément de $(X, =_X)$ possèdent une "forme réduite canonique", qui peut être $\mathfrak{C}$-calculée.

Un $\mathfrak{P}$-ensemble-discret n'est pas "a priori" $\mathfrak{P}$-dénombrable: cette question a manifestement à voir avec le fameux problème $\mathfrak{P} = \mathcal{NP}$? . (cf. n.7)

Numérotations:

Par définition, une **numérotation** d'un ensemble X est une énumération (f,r) qui vérifie:

i. si $f(n) = u$, alors pour tout $m > n$, $f(m) = u$

ii. si $f(p) \neq u$ et $f(p) =_X f(q)$, alors $p = q$

Toute numérotation est un dénombrement.

Les ensembles finis sont numérotables. Les ensembles infinis dénombrables sont numérotables. L'ensemble des contre-exemples à la conjecture de Goldbach "n'est pas" numérotable.

La notion de numérotation, relativisée à la classe de constructions $\mathfrak{C}$, donne les notions de **$\mathfrak{C}$-numérotation**, et de $\mathfrak{C}$-ensemble **$\mathfrak{C}$-numérotable**.

L'ensemble $\mathbb{Q}$ des nombres rationnels est de manière naturelle un $\mathfrak{P}$-ensemble, qui est $\mathfrak{P}$-dénombrable, mais qui ne semble pas $\mathfrak{P}$-numérotable. Cela confirmerait l'impression intuitive que l'ensemble $\mathbb{Q}$ est un petit peu plus compliqué que $\mathbb{N}$ ou que l'ensemble des nombres décimaux.

Si $f : \mathbb{N} \to \mathbb{N}$ est une fonction récursive qui croît plus vite que toute fonction $\mathbb{P}\mathbf{r}$, construite par récurrence double, son image peut être une partie $\mathbb{P}\mathbf{r}$-détachable de $\mathbb{N}$, (et donc un $\mathbb{P}\mathbf{r}$-ensemble), mais elle n'est pas $\mathbb{P}\mathbf{r}$-numérotable. (n.8)

De la même manière, et plus simplement, $\mathbb{N}_1$ est un ensemble $\mathfrak{P}$-dénombrable qui n'est pas $\mathfrak{P}$-numérotable.

$\mathcal{P}$-ensembles $\mathcal{P}$-réductibles

Nous introduisons enfin une notion qui est une version affaiblie de la $\mathcal{P}$-dénombrabilité. Elle nous sera utile dans certains théorèmes par la suite.

Un $\mathcal{P}$-ensemble X est dit **$\mathcal{P}$-réductible** si on a un polynôme Q et une $\mathcal{P}$-opération

r : $X \to X$, qui vérifient :

- pour tout x de X , $r(x) =_X x$
- si $y =_X x$, alors $\|r(x)\| < Q(\| y \|)$

On peut dire que l'opération r remplace le représentant x par un autre représentant r(x) , mais de taille raisonnable: c'est une sorte de forme réduite non canonique, mais utilisable pour les calculs de classe $\mathcal{P}$.

La notion de $\mathcal{P}$-réductibilité est une notion qui apparaît naturellement dans certaines preuves de $\mathcal{P}$-calculabilité. Néanmoins, il semble que tous les exemples utiles d'ensembles $\mathcal{P}$-réductibles soient également, de manière immédiate, des ensembles $\mathcal{P}$-dénombrables. La notion de $\mathcal{P}$-réductibilité n'est donc pas nécessaire pour les applications les plus courantes des théorèmes où elle intervient. Elle constitue sans doute un raffinement peu utile de la notion de $\mathcal{P}$-dénombrabilité.

d) Présentations des entiers relatifs et des nombres rationnels

Symétrisation d'un $\mathcal{C}$-monoïde commutatif régulier

La construction du symétrisé du monoïde commutatif régulier M , en munissant $M \times M$ de la relation d'égalité convenable, fonctionne sans problème du point de vue des $\mathcal{C}$-structures algébriques.

En termes savants: le foncteur d'oubli des $\mathcal{C}$-groupes abéliens vers les $\mathcal{C}$-monoïdes commutatifs réguliers possède un adjoint à gauche.

On notera que lorsqu'un $\mathcal{P}$-monoïde commutatif n'est pas régulier, l'égalité dans le groupe obtenu classiquement par symétrisation peut ne pas être décidable[7].

Soit M un $\mathcal{C}$-monoïde commutatif régulier, G un $\mathcal{C}$-groupe, $f : M \to G$ un homomorphisme qui fait de G le symétrisé de M . Pour que f fasse de G le $\mathcal{C}$-symétrisé de M , il faut et suffit que :

- f est une $\mathcal{C}$-fonction, et
- il existe 2 $\mathcal{C}$-opérations g_1 et g_2 de G vers M telles que, pour tout x dans G , on ait : $x =_G f(g_1(x)) - f(g_2(x))$.

---

[7] Soit (u_p) une $\mathcal{P}$-suite d'entiers, d'image non récursive. Considérons le monoïde commutatif librement engendré par une suite (a_n) et codé par la partie de **Lst**($\mathbb{N}$) formée par les listes croissantes d'entiers. Introduisons la relation d'équivalence stable engendrée par les relations $a_{3n+1}.a_{3p+2} = a_{3n}.a_{3p+2}$ si $n = u_p$. On obtient un $\mathcal{P}$-monoïde commutatif. Mais dans le symétrisé, $a_{3n+1} = a_{3n}$ si et seulement si n est une valeur prise par la suite (u_p) .

Les propriétés d'admettre un $\mathfrak{P}$-dénombrement ou une $\mathfrak{P}$-numérotation ne passent pas "a priori" d'un $\mathfrak{P}$-monoïde commutatif régulier à son symétrisé[8].

Nous dirons qu'un $\mathfrak{C}$-monoïde commutatif M noté multiplicativement est **$\mathfrak{C}$-divisible** lorsqu'il existe une $\mathfrak{C}$-opération D de $M \times M$ vers $M \cup \{u\}$ vérifiant :

si $D(a,b) = u$, alors pour tout $x \in M$: $a.x \neq b$, et , si $D(a,b) \in M$,
alors : $a.D(a,b) = b$.

Un $\mathfrak{C}$-monoïde commutatif régulier M est $\mathfrak{C}$-divisible si et seulement si M "est" une partie $\mathfrak{C}$-détachable de son symétrisé: plus précisément: si l'homomorphisme $f : M \to G$ est une $\mathfrak{C}$-équivalence entre M et une $\mathfrak{C}$-partie de G .

La présentation standard $\mathbb{Z}$

La présentation des entiers relatifs sous forme d'un nombre en binaire avec un signe, sera considérée comme la présentation standard, et sera notée $\mathbb{Z}$.

Elle fait de $(\mathbb{Z}, +, -, \times,$ **div** , **mod** , $<)$ une $\mathfrak{P}_0$-structure. De plus ce $\mathfrak{P}_0$-groupe est $\mathfrak{P}_0$-isomorphe au $\mathfrak{P}_0$-symétrisé de $\mathbb{N}$ [(9)].

De manière générale nous noterons $\mathbb{Z}$ toute présentation des entiers relatifs $\mathfrak{P}_1$-isomorphe à la présentation standard et faisant de $(\mathbb{Z}, +, -, \times,$ **div** , **mod** , $<)$ une $\mathfrak{P}_0$-structure.

C'est le cas par exemple pour la présentation en base 3 avec les chiffres 0 , 1 , -1 ou encore en base 2 avec les chiffres 0 , 1 , -1 et la relation d'égalité convenable (cette présentation peut être utile pour l'écriture de valeurs approchées successives de nombres réels).

Autres présentations des entiers relatifs

Les autres présentations de l'ensemble des entiers naturels que nous avons décrites donnent par symétrisation des présentations des entiers relatifs non $\mathfrak{P}$-isomorphes à la présentation standard. Nous noterons $\mathbb{Z}_1$ le symétrisé de $\mathbb{N}_1$: on obtient une présentation $\mathfrak{P}_1$-isomorphe en prenant un entier codé en unaire avec un signe[10].

Corps des fractions d'un $\mathfrak{C}$-anneau intègre

La construction du corps des fractions d'un anneau intègre M , en munissant $M \times (M - \{0\})$ de la relation d'égalité convenable, fonctionne sans problème du point de vue des $\mathfrak{C}$-structures algébriques pour les classe $\mathfrak{C}$ suivantes : $\mathfrak{P}$, $\mathfrak{P}_1$, **PSPACE** , **RES1** , $\mathbb{P}$**r** , **Rec** .

On a par contre de petits ennuis avec l'addition pour la classe $\mathfrak{P}_0$: par exemple dans le corps des fractions de $\mathbb{Z}$ l'addition est seulement dans **SPARES**(2.n) (additionner 1/1 et $1/2^n$ pour s'en convaincre).

Un $\mathfrak{P}$-anneau intègre est dit $\mathfrak{P}$-divisible lorsque le monoïde multiplicatif M - {0} est $\mathfrak{P}$-divisible . L'anneau est alors identifiable à une $\mathfrak{P}$-partie de son corps de fractions.

---

8 La première question ($\mathfrak{P}$-dénombrement) aura une réponse positive si $\mathfrak{P} = \mathcal{NP}$ (cf. n.7) . La deuxième question pourrait faire l'objet d'un divertissement mathématique.

9 Divertissement mathématique : Soit $\mathbb{Z}'$ une autre présentation des entiers relatifs et supposons que la structure :
$(\mathbb{Z}', +, -, \times$, div , mod , $<)$ soit une $\mathfrak{P}_0$-structure et $\mathbb{Z}'$ un $\mathfrak{P}$-ensemble $\mathfrak{P}$-réductible, alors la fonction $z \to z$ de $\mathbb{Z}$ vers $\mathbb{Z}'$ est-elle nécessairement un $\mathfrak{P}$-isomorphisme ?

10 Divertissement mathématique : notons $\mathbb{Z}_2$ le symétrisé de $\mathbb{N}_2$. On voit facilement que $\mathbb{N}_2$ est $\mathfrak{P}$-numérotable. Est-ce que $\mathbb{Z}_2$ est $\mathfrak{P}$-numérotable ?

$\mathbb{Q}$ comme $\mathfrak{P}_0$-structure

Si on mesure la grandeur de la fraction a/b par: $\|a/b\| := \mathbf{lg}(|a|+b)$, on constate immédiatement que:

En notant $\mathbb{Q}$ l'ensemble des rationnels présenté comme $\mathbb{Z} \times \mathbb{N}^+$ muni de la relation d'égalité convenable et de la mesure définie ci-dessus, on obtient une $\mathfrak{P}_0$-présentation $\mathfrak{P}_1$-équivalente à celle obtenue avec la mesure naturelle, et la structure ($\mathbb{Q}$, + , – , $\times$, / , Ent , < , numérateur de la fraction réduite) est une $\mathfrak{P}_0$-structure[11].

On notera $\mathbb{D}$ l'ensemble des nombres dyadiques dans sa présentation naturelle (binaire avec virgule et signe) et avec une mesure qui fait de :

$$(\mathbb{D} , + , – , \times , \text{Ent} , < , (x, n) \to x/2^n : \mathbb{D} \times \mathbb{N}_1 \to \mathbb{D})$$

une $\mathfrak{P}_0$-structure. (par exemple la mesure héritée de celle de $\mathbb{Q}$).

---

11 $\mathbb{Q}$ est $\mathfrak{P}_0$-dénombrable puisque le calcul de la réduite d'une fraction est $\mathfrak{P}_0$.
$\mathbb{Q}$ est $\mathbb{P}$ **r**-numérotable et c'est un corps naturellement primitif récursif. Donner une numérotation de $\mathbb{Q}$ revient à donner une numérotation de $\mathbb{Z} \times \mathbb{N}^+$ pour laquelle:

- (a) on sait numéroter en ordre croissant les fractions réduites, et :
- (b) on sait pour chaque fraction réduite le numéro qui lui est attribué.

$\mathbb{Q}$ est **PSPACE**-numérotable. Problème : $\mathbb{Q}$ est-il $\mathfrak{P}$-numérotable ?

B) STRUCTURES ALGEBRIQUES COMPLETEMENT $\mathcal{P}$-CALCULABLES

a) Généralités sur les structures algébriques complètement $\mathcal{P}$-calculables et sur les structures naturellement c-$\mathcal{P}$-c

Structures algébriques complètement $\mathcal{C}$-calculables

Si X est une $\mathcal{C}$-structure algébrique , avec *un nombre fini* de lois de composition, on peut définir un $\mathcal{C}$-ensemble **Calc**(X) dont les éléments sont les écritures de calculs à effectuer dans cette $\mathcal{C}$-structure. Par exemple, dans le corps $\mathbb{Q}$:

$$(1/2 +1/(3/4 +1/(5 /(6 - 17/7)))) \times (3/5 + 5/7 - 15 /(1+ 13/4))$$

Définition B.a1 :

On dira que la structure algébrique X est **complètement $\mathcal{C}$-calculable** si l'opération naturelle : "faisons la calcul indiqué" qui transforme un élément de **Calc**(X) en un élément de $X \cup \{u\}$ (union disjointe; u vaut pour "non défini") est une $\mathcal{C}$-opération[12].

Une $\mathcal{P}$-structure n'est pas nécessairement complètement $\mathcal{P}$-calculable, comme nous le verrons sur plusieurs exemples (les polynômes en présentation creuse, ou les réels algébriques en présentation naïve notamment). Cela tient à une possible explosion de la taille des objets lors des calculs successifs. On démontre par contre immédiatement.

Proposition B.a1 :

Pour qu'une $\mathcal{P}$-structure algébrique X soit complètement $\mathcal{P}$-calculable il faut et suffit que l'opération naturelle : "faisons la calcul indiqué" , de **Calc**(X) vers $X \cup \{u\}$ soit **RESP** (c.-à-d. polynomialement majorée en taille).

Toute $\mathcal{P}_0$-structure est complètement $\mathcal{P}_1$-calculable.

Toute $\mathbb{P}$**r**-structure est complètement $\mathbb{P}$**r**-calculable .

Remarque : Dans la plupart des exemples de $\mathcal{P}_0$-structures que nous étudions, on a en fait une majoration de la mesure de la sortie par la mesure de l'entrée (sans avoir à rajouter une constante), ce qui implique que la structure est en fait complètement $\mathcal{P}_0$-calculable.

Exemple : fractions continues dans $\mathbb{Q}$

Considérons **Lst**($\mathbb{Q}$) , $\mathcal{P}_0$-ensemble des listes d'éléments de $\mathbb{Q}$. On a une application "fraction continue" de **Lst**($\mathbb{Q}$) vers $\mathbb{Q}$ [13] , donnée par :

$$(q_1,q_2,...,q_n) \rightarrow q_1+1/(q_2+1/(...+1/q_n)..)$$

---

[12] On aurait une définition analogue pour une $\mathcal{C}$-structure algébrique impliquant plusieurs $\mathcal{C}$-ensembles. Par exemple avec 3 $\mathcal{C}$-ensembles X, Y, Z l'opération "faisons le calcul indiqué" a pour source l'ensemble **Calc**(X,Y,Z) analogue de **Calc**(X) , et pour but l'ensemble $X \cup Y \cup Z \cup \{u\}$ (union disjointe).

[13] En fait, cette application est définie sur des $\mathcal{P}$-parties convenables de **Lst**($\mathbb{Q}$) ; par exemple: tous les q_i sont > 0 à partir du $2^{ème}$.

En notant $[q_1;q_2,...,q_n]$ la fraction continue du 2ème membre, on obtient :

$$\| [q_1;q_2,...,q_n] \| \leq \| q_1 \| + \| q_2 \| + ... + \| q_n \|$$

puisque $\| r \| = \| 1/r \|$ et $\| a+b \| \leq \| a \| + \| b \|$. Donc, l'application "fraction continue" est une $\mathcal{P}_0$-fonction .

On peut également montrer que l'application "fraction continue" réalise une $\mathcal{P}$-équivalence entre $\mathbb{Q}$ et le $\mathcal{P}$-ensemble constitué par les développements en fraction continue standards (tous les q_i sont entiers, > 0 à partir du 2ème, et le dernier $\neq 1$). (n.9)

Caractérisation des structures algébriques complètement $\mathcal{P}$-calculables

Théorème B.a1 :

Pour qu'une structure algébrique soit complètement $\mathcal{P}$-calculable, il faut et suffit qu'elle soit $\mathcal{P}$-isomorphe à une $\mathcal{P}_0$-structure.

La condition est évidemment suffisante (cf. prop. B.a1). Supposons réciproquement que la structure (X,Y,Z) soit complètement $\mathcal{P}$-calculable, alors l'ensemble $X \cup Y \cup Z \cup \{u\}$ peut être $\mathcal{P}$-présenté par **Calc**(X,Y,Z) muni de la relation d'égalité convenable (les expressions une fois calculées sont égales), et les lois de composition peuvent être (**DT1**$\cap$ **RES0**)-présentées en les écrivant entièrement sous forme de calculs à effectuer: bref les calculs ne sont effectués qu'au moment de tester l'égalité.

Remarques :

(1) En fait seule la partie "directe" est réellement utilisée; on transforme la $\mathcal{P}$-structure en une $\mathcal{P}_0$-structure en modifiant seulement la mesure de la grandeur des objets. La partie réciproque a un intérêt plutôt théorique.

(2) Nous avons raisonné avec une structure algébrique donnée par un nombre fini de lois de compositions. Il est clair que PrB.a1 et ThB.a1 restent vrais si la structure algébrique comporte en outre un nombre fini de constantes et des relations, et si les lois de composition sont définies sur des parties définies par ces relations.

Notation abrégée : nous noterons désormais c-$\mathcal{P}$-c comme abréviation pour "complètement $\mathcal{P}$-calculable".

Propriétés de stabilité élémentaires

Les structures algébriques c-$\mathcal{P}$-c sont stables pour les constructions suivantes : produit de 2 structures ; $\mathcal{P}$-quotient d'une structure ; sous-structure $\mathcal{P}$-détachable .

Si K est un $\mathcal{P}$-anneau intègre où l'addition et le produit sont c-$\mathcal{P}$-c , il en est de même pour son corps de fractions.

NB: Pour un $\mathcal{P}$-anneau K , la condition "être c-$\mathcal{P}$-c en tant qu'anneau" est a priori plus forte que la condition "addition et produit, chacune prise isolément, sont c-$\mathcal{P}$-c dans K"[14].

Structures algébriques naturellement c-$\mathcal{P}$-c

Considérons un $\mathcal{P}$-anneau A dans lequel l'addition et la multiplication sont c-$\mathcal{P}$-c . Alors l'unique homomorphisme $f : \mathbb{Z} \to A$ est une $\mathcal{P}$-fonction: en effet f(10011001) , par exemple, est égal à :

$$1_A + 2_A \times 2_A \times 2_A + 2_A \times 2_A \times 2_A \times 2_A + 2_A \times 2_A \times 2_A \times 2_A \times 2_A \times 2_A \times 2_A .$$

---

[14] Dans le premier cas, on évalue une formule comportant des additions, soustractions ou produits. Dans le deuxième cas, on évalue le produit ou la somme d'une liste.

Or il est clair que l'écriture ci-avant a une taille polynomialement reliée à la taille de 10011001.

En langage savant, $\mathbb{Z}$ est objet initial dans la catégorie des $\mathfrak{P}$-anneaux complètement $\mathfrak{P}$-calculables. (en fait l'addition et la multiplication de A ont seulement besoin d'être, chacune de leur coté, c-$\mathfrak{P}$-c) .

En particulier, si nous considérons la structure algébrique abstraite "anneau des entiers relatifs", nous voyons que la $\mathfrak{P}$-présentation standard est $\mathfrak{P}$-initiale parmi les $\mathfrak{P}$-présentations qui en font un anneau c-$\mathfrak{P}$-c . En ce sens la $\mathfrak{P}$-présentation standard est naturellement c-$\mathfrak{P}$-c .

Cette terminologie est à rapprocher de celle que nous avons introduite en A.b lorsque nous avons parlé des structures naturellement primitives récursives.

De manière générale, nous posons les définitions suivantes:

Définition B.a2 : Une structure algébrique énumérable discrète "abstraite" (c.-à-d. abstraction faite de toute présentation de cette structure) sera dite **naturellement c-$\mathfrak{P}$-c** lorsqu'il existe un objet initial dans la catégorie suivante: les objets sont les $\mathfrak{P}$-présentations de cette structure qui la rendent c-$\mathfrak{P}$-c , les flèches sont les applications "identité" qui sont des $\mathfrak{P}$-fonctions.
Cet objet initial est alors défini de manière unique à $\mathfrak{P}$-équivalence près, et nous l'appellerons **la présentation c-$\mathfrak{P}$-c naturelle** de la structure abstraite.

Exemples : La présentation en unaire de (entiers naturels, +), les présentations en binaire de (entiers naturels, + , $\times$) et de (entiers relatifs, + , $-$, $\times$) sont les présentations c-$\mathfrak{P}$-c naturelles de ces structures algébriques. (cf. raisonnement ci-dessus pour les présentations en binaire et PrB.d2 pour la présentation en unaire)

b) Espaces vectoriels et modules libres

Généralités

Lorsque K est un anneau énumérable discret présenté, et X un ensemble énumérable discret présenté , nous réservons la notation $K^{(X)}$ pour la présentation suivante du K-module librement engendré par X : c'est la partie de **Lst**($K \times X$) , obtenue en ne gardant que les listes où tous les "coefficients" $k_i \in K$ sont non nuls, et où les $x_i \in X$ sont sans répétition (et on précise un couple (0,c) pour représenter l'élément nul).

Pour $X = \mathbb{N}_1$, (dans le cas de $\mathfrak{P}$-ensembles) , on obtient une $\mathfrak{P}$-présentation $\mathfrak{P}$-équivalente à celle obtenue sous la forme **Lst**(K) . Et dans le cas où X est fini et a n éléments, on obtient une $\mathfrak{P}$-présentation $\mathfrak{P}$-équivalente à K^n .

Les 2 propositions suivantes sont de démonstration immédiate.

Proposition B.b1 : Soit K un $\mathfrak{P}$-anneau où l'addition est c-$\mathfrak{P}$-c , et X un $\mathfrak{P}$-ensemble-discret . Alors $K^{(X)}$ est le $\mathfrak{P}$-K-module librement engendré par X dans la catégorie des $\mathfrak{P}$-K-modules où l'addition est c-$\mathfrak{P}$-c .

Proposition B.b2 : Soit K un $\mathfrak{P}$-anneau intègre où l'addition et la multiplication sont c-$\mathfrak{P}$-c , et L son corps de fractions . Alors $L^{(X)}$ est $\mathfrak{P}$-équivalent à la présentation en forme "réduite au même dénominateur" , c.-à-d. à $K^{(X)} \times (K - \{0\})$ muni de la relation d'égalité convenable .

Remarque : Lorsque la dimension est finie et fixée, les hypothèses "c-$\mathfrak{P}$-c" dans les propositions ci-dessus sont inutiles. De plus, toute application linéaire de K^n vers un $\mathfrak{P}$-K-module est une $\mathfrak{P}$-fonction , et, lorsque K est un $\mathfrak{P}$-corps, tout sous-espace libre de K^n est un $\mathfrak{P}$-sous-espace $\mathfrak{P}$-libre (par définition **un $\mathfrak{P}$-espace est $\mathfrak{P}$-libre s'il est $\mathfrak{P}$-isomorphe à un espace** $K^{(X)}$) .

Modules libres sur $\mathbb{Z}$ et $\mathbb{Q}$ comme $\mathfrak{P}_0$-structures.

Les $\mathbb{Z}$-modules $\mathbb{Z}^n$ et $\mathbb{Z}^{(\mathbb{N})}$ (présenté sous la forme **Lst**($\mathbb{Z}$)) sont des $\mathfrak{P}_0$-$\mathbb{Z}$-modules lorsqu'on les munit des mesures : $\|(a_1,a_2,...,a_n)\| = n + \mathbf{lg}(\Sigma | a_i |)$ (pour le cas **Lst**, n est la longueur de la liste)

Les $\mathbb{Q}$-espaces vectoriels $\mathbb{Q}^n$ (présenté sous la forme $\mathbb{Z}^n \times \mathbb{N}^+$) et $\mathbb{Q}^{(\mathbb{N})}$ (présenté sous la forme **Lst**($\mathbb{Z}$)$\times \mathbb{N}^+$) sont des $\mathfrak{P}_0$-$\mathbb{Q}$-espaces vectoriels lorsqu'on les munit des mesures :

$\| ((a_1,a_2,...,a_n), d) \| = n + \mathbf{lg}(d + \Sigma | a_i |)$

c) Algèbres $\mathbf{M_n}(\mathbb{Z})$, $\mathbf{M_n}(\mathbb{Q})$, $\mathbb{Z}[X]$, $\mathbb{Z}[X_1,X_2,...,X_n]$, $\mathbb{Q}(X)$, $\mathbb{Q}(X_1,X_2,...,X_n)$ comme $\mathfrak{P}_0$-structures naturellement c-$\mathfrak{P}$-c

Algèbres $\mathbf{M_n}(\mathbb{Z})$ et **Flin**($\mathbb{Z}$) comme $\mathfrak{P}_0$-structures

Les notions de $\mathbb{Z}$-algèbre unitaire et d'anneau sont identiques parce que $\mathbb{Z}$ est objet initial dans la catégorie des anneaux.

De même donc pour les notions de $\mathfrak{P}$-$\mathbb{Z}$-algèbre unitaire c-$\mathfrak{P}$-c et de $\mathfrak{P}$-anneau c-$\mathfrak{P}$-c.

Nous pouvons faire de l'anneau $\mathbf{M_n}(\mathbb{Z})$ une $\mathfrak{P}_0$-structure si nous prenons pour mesure de la matrice $A = (a_{ij})$: $\|A\| = n + \mathbf{lg}(\Sigma | a_{ij} |)$. Nous réservons la notation $\mathbf{M_n}(\mathbb{Z})$ pour cette présentation de cet anneau (ou pour une présentation $\mathfrak{P}$-équivalente).

C'est de plus une structure d'anneau naturellement c-$\mathfrak{P}$-c : en effet, toute présentation de cet anneau qui en fait un anneau c-$\mathfrak{P}$-c en fait aussi un $\mathbb{Z}$-module c-$\mathfrak{P}$-c , et la présentation $\mathbf{M_n}(\mathbb{Z})$ est librement engendrée par sa base canonique dans la catégorie des $\mathbb{Z}$-modules c-$\mathfrak{P}$-c.

Avec la même mesure, nous pouvons considérer l'algèbre **Flin**($\mathbb{Z}$) , réunion emboîtée des $\mathbf{M_n}(\mathbb{Z})$ (cf. § C.a pour les détails), et nous obtiendrons une $\mathfrak{P}_0$-structure.

Le corps $\mathbb{Q}$ comme objet initial

Considérons un $\mathfrak{P}$-corps K , de caractéristique nulle, et dans lequel l'addition et la multiplication sont c-$\mathfrak{P}$-c . Alors l'unique homomorphisme $f : \mathbb{Q} \to K$ est une $\mathfrak{P}$-fonction: cela résulte immédiatement de la proposition analogue pour $\mathbb{Z}$. En particulier:

le corps des rationnels est naturellement c-$\mathfrak{P}$-c en tant que corps.

Algèbres $\mathbf{M_n}(\mathbb{Q})$ et **Flin**($\mathbb{Q}$) comme $\mathfrak{P}_0$-structures

Nous pouvons faire de l'anneau $\mathbf{M_n}(\mathbb{Q})$ une $\mathfrak{P}_0$-structure si nous le présentons sous forme "réduite au même dénominateur" et prenons pour mesure de la matrice A représentée par le couple $((a_{ij}), d)$ de $\mathbf{M_n}(\mathbb{Z})\times \mathbb{N}^+$: $\|A\| = n + \mathbf{lg}(d + \Sigma | a_{ij} |)$. Nous réservons la

notation $\mathbf{M_n}(\mathbb{Q})$ pour cette présentation de cet anneau (ou pour toute présentation $\mathcal{P}$-équivalente, par exemple sous forme d'une liste de n^2 éléments de $\mathbb{Q}$ avec pour mesure la taille effective du mot utilisé pour représenter la matrice)[15].

Avec la même mesure, nous pouvons considérer l'algèbre **Flin**($\mathbb{Q}$) , réunion emboîtée des $\mathbf{M_n}(\mathbb{Q})$, et nous obtiendrons une $\mathcal{P}_0$-structure.

$\mathbb{Z}$ [X] comme $\mathcal{P}_0$-structure et comme objet libre à un générateur

Nous notons $\mathbb{Z}[X]$ l'anneau des polynômes à coefficients dans $\mathbb{Z}$ présenté sous la forme **Lst**($\mathbb{Z}$) (en arrêtant la liste au coefficient dominant a_d), et avec la mesure suivante:

$$\| \Sigma a_i X^i \| = d + \mathbf{lg}(\Sigma |a_i|).$$

Il est clair que cette mesure est polynomialement reliée à la taille naturelle $\Sigma \|a_i\|$. Un calcul immédiat montre de plus que ($\mathbb{Z}[X]$, + , $\times$) est alors une $\mathcal{P}_0$-structure, donc c-$\mathcal{P}$-c .

Remarquons maintenant que la taille naturelle du polynôme $P = \Sigma a_i X^i$ (écrit sous forme de la liste de ses coefficients) est elle-même polynomialement reliée à la taille de l'écriture:

$$a_0 + a_1 \times X + a_2 \times X \times X + ... + a_d \times X \times ... \times X \quad \text{dans } \mathbf{Calc}(\mathbb{Z}[X]).$$

Si maintenant A est un $\mathcal{P}$-anneau où l'addition et la multiplication sont c-$\mathcal{P}$-c, on a une $\mathcal{P}$-fonction de $\mathbb{Z}[X] \times A$ vers **Calc**(A) :

$$(P,b) \rightarrow \hat{a}_0 + \hat{a}_1 \times b + \hat{a}_2 \times b \times b + ... + \hat{a}_d \times b \times ... \times b ,$$ où $\hat{a}$, pour a dans $\mathbb{Z}$, est la "valeur" de a dans A (cf. § précédent). Il ne reste plus qu'à "faire le calcul indiqué" pour obtenir le résultat suivant:

Proposition B.c1 : Si A est un $\mathcal{P}$-anneau où l'addition et la multiplication sont c-$\mathcal{P}$-c , l'homomorphisme d'évaluation de $\mathbb{Z}[X] \times A$ vers A : $(P,b) \rightarrow P(b)$ est une $\mathcal{P}$-fonction.

De plus, si A est un $\mathcal{P}$-anneau où l'addition est c-$\mathcal{P}$-c , pour b fixé, l'homomorphisme d'évaluation en b , de $\mathbb{Z}[X]$ vers A : $P \rightarrow P(b)$ est une $\mathcal{P}$-fonction si et seulement si la fonction $n \rightarrow b^n$, de $\mathbb{N}_1$ vers B , est une $\mathcal{P}$-fonction.

En particulier, $\mathbb{Z}[X]$ est une structure naturellement c-$\mathcal{P}$-c, et dans la catégorie des $\mathcal{P}$-anneaux où l'addition et la multiplication sont c-$\mathcal{P}$-c, $\mathbb{Z}[X]$ est l'objet librement engendré par X .

Remarque : Il existe une autre présentation utile de l'anneau des polynômes à coefficients dans $\mathbb{Z}$, non $\mathcal{P}$-équivalente à la précédente . Nous notons $\mathbb{Z}[X]_c$ cet anneau lorsque le polynôme est représenté par la liste des couples (i , a_i) , en ne mentionnant que les coefficients non nuls, et i étant écrit en binaire. C'est une présentation adéquate pour calculer sur des polynômes "creux", c.-à-d. avec peu de coefficients non nuls . $\mathbb{Z}[X]_c$ est un $\mathcal{P}$-anneau , et l'homomorphisme : $P \rightarrow P$ de $\mathbb{Z}[X]$ vers $\mathbb{Z}[X]_c$ est une $\mathcal{P}$-fonction bijective, mais non une $\mathcal{P}$-équivalence .

En fait $\mathbb{Z}[X]_c$ n'est pas c-$\mathcal{P}$-c, comme le montre l'exemple du produit:

$$(1 + X).(1 + X^2).(1 + X^4)....(1 + X^{2^n}) ,$$ qui, dans $\mathbb{Z}[X]_c$, prend "beaucoup plus" de place après avoir été effectué qu'avant.

---

15 Divertissement mathématique: $\mathbb{Q}$, $\mathbf{M_n}(\mathbb{Q})$ sont-il naturellement c-$\mathcal{P}$-c en tant qu'anneau ?

$\mathbb{Z}$ [X,Y] comme $\mathfrak{P}_0$-structure et comme objet libre à deux générateurs

Nous notons $\mathbb{Z}[X,Y]$ l'anneau des polynômes à 2 indéterminées X et Y et à coefficients dans $\mathbb{Z}$, présenté sous la forme **Lst**(**Lst**($\mathbb{Z}$)) (c.-à-d. comme une liste d'éléments de $\mathbb{Z}[X]$, lorsqu'on voit $\mathbb{Z}[X,Y]$ sous la forme $\mathbb{Z}[X]$ [Y]), et avec la mesure suivante:

$$\Sigma a_{ij}.X^iY^j \text{ = degré total + } \mathbf{lg}(\ \Sigma\ |a_{ij}|\ ) .$$

Il est clair que cette mesure est polynomialement reliée à la taille naturelle $\Sigma \| a_{ij} \|$. Un calcul immédiat montre de plus que ($\mathbb{Z}[X,Y]$, + , $\times$) est alors une $\mathfrak{P}_0$-structure, donc c-$\mathfrak{P}$-c .

Nous pouvons poursuivre exactement comme au paragraphe précédent, et nous obtiendrions la proposition analogue de la même manière. En particulier :

- $\mathbb{Z}[X,Y]$ est une structure d'anneau naturellement c-$\mathfrak{P}$-c (et la présentation décrite est la présentation c-$\mathfrak{P}$-c naturelle)
- dans la catégorie des $\mathfrak{P}$-anneaux commutatifs où l'addition et la multiplication sont c-$\mathfrak{P}$-c , $\mathbb{Z}[X,Y]$ est l'objet librement engendré par X et Y .
- si A est un $\mathfrak{P}$-anneau où l'addition est c-$\mathfrak{P}$-c , pour b et c fixés qui commutent entre eux, l'homomorphisme d'évaluation en b et c , de $\mathbb{Z}[X,Y]$ vers A : $P \to P(b,c)$ est une $\mathfrak{P}$-fonction si et seulement si la fonction

  $(n,p) \to b^n.c^p$, de $\mathbb{N}_1 \times \mathbb{N}_1$ vers B , est une $\mathfrak{P}$-fonction.

On obtient les mêmes résultats pour $\mathbb{Z}[X_1,X_2,...,X_n]$. Cette méthode ne peut cependant pas se généraliser à une infinité d'indéterminées : la mesure qui fait de $\mathbb{Z}[X_1,X_2,...,X_n]$ une $\mathfrak{P}_0$-structure est toujours "la même" :

degré total + **lg**(Σ |coefficients |);

et elle est toujours polynomialement reliée à la taille concrète (longueur du mot utilisé), *mais* elle l'est de moins en moins bien au fur et à mesure que le nombre de variables augmente. (Voir cependant dans le §f : Deux remarques sur l'anneau $\mathbb{Z}[(X_i)_{i\in\mathbb{N}}]$) .

$\mathbb{Q}(X)$ comme $\mathfrak{P}_0$-structure naturellement c-$\mathfrak{P}$-c

Proposition B.c2 : Lorsqu'on présente $\mathbb{Q}(X)$ comme corps des fractions de $\mathbb{Z}[X]$, on obtient une structure c-$\mathfrak{P}$-c , et c'est la présentation c-$\mathfrak{P}$-c naturelle sur le corps abstrait $\mathbb{Q}(X)$.

Soient par ailleurs un $\mathfrak{P}$-corps K , de caractéristique nulle, et dans lequel l'addition et la multiplication sont c-$\mathfrak{P}$-c , et b un élément de K transcendant sur son sous corps premier: alors l'homomorphisme d'évaluation $F \to F(b)$ de $\mathbb{Q}(X)$ vers K est une $\mathfrak{P}$-fonction.

preuve> Dans le corps des fractions de $\mathbb{Z}[X]$, la mesure de la fraction rationnelle F = P/Q est :

$$\| P \| + \| Q \| \text{ = deg(P) + deg(Q) + } \mathbf{lg}(\ \Sigma\ |\ a_i\ |) + \mathbf{lg}(\ \Sigma\ |\ b_j\ |) ,$$

elle est polynomialement reliée à la taille concrète : $\Sigma\|a_i\| + \Sigma\|b_j\|$, mais aussi à la mesure

$$\sup(\deg(P),\deg(Q)) + \mathbf{lg}(\Sigma\ |\ a_i\ | + \Sigma\ |\ b_j\ |) .$$

Or cette dernière fait de $\mathbb{Q}(X)$ une $\mathfrak{P}_0$-structure. Ainsi, $\mathbb{Q}(X)$, présenté comme corps des fractions de $\mathbb{Z}[X]$, est c-$\mathfrak{P}$-c.
Si maintenant K et b sont comme dans l'alinéa 2 , on a l'homomorphisme d'évaluation $P \to P(b)$, avec comme source $\mathbb{Z}[X]$, qui est un $\mathfrak{P}$-homomorphisme d'après la proposition B.c1 , d'où on déduit l'analogue lorsqu'on prolonge à $\mathbb{Q}(X)$.
Enfin, en prenant comme cas particulier : pour K une $\mathfrak{P}$-présentation de $\mathbb{Q}(X)$ qui en fait une structure c-$\mathfrak{P}$-c , et pour b l'indéterminée X, on voit que l'on avait bien défini la présentation c-$\mathfrak{P}$-c naturelle du corps abstrait $\mathbb{Q}(X)$. ❑

On généraliserait sans peine ces résultats à $\mathbb{Q}[X_1,X_2,...,X_n]$ et à $\mathbb{Q}(X_1,X_2,...,X_n)$. Une mesure utilisable pour faire de $\mathbb{Q}(X_1,X_2,...,X_n)$ une $\mathfrak{P}_0$-structure est la suivante :

$$\| F \| = \| P/Q \| = \sup(\deg(P),\deg(Q)) + \mathbf{lg}(\Sigma\, |\text{coefficients}|)$$

(P et Q étant dans $\mathbb{Z}[X_1,X_2,...,X_n]$ et deg représentant le degré total)

D'autres $\mathfrak{P}_0$-structures d'anneaux

Proposition B.c3 : Toute $\mathbb{Z}$-algèbre libre K de dimension finie k (comme $\mathbb{Z}$-module) est un anneau naturellement c-$\mathfrak{P}$-c . On peut obtenir la structure c-$\mathfrak{P}$-c naturelle de K en présentant K comme un sous-module libre de $\mathbf{M_k}(\mathbb{Z})$, et alors K est une $\mathfrak{P}_0$-structure.
De plus K [X] et K [$X_1,X_2,...,X_n$] peuvent être présentées de manière à obtenir des $\mathfrak{P}_0$-structures , et ce sont les structures c-$\mathfrak{P}$-c naturelles de ces anneaux.

preuve> Si $e_1,e_2,...,e_k$ est une base de K comme $\mathbb{Z}$-module et si b est un élément de K , nous considérons la matrice B de l'application linéaire "multiplication par b " exprimée sur la base $e_1,e_2,...,e_k$, nous notons $\sigma(b)$ la somme Σ |coeffs de B| , et nous considérons la mesure $\|b\| = \mathbf{lg}(\sigma(b))$. L'homomorphisme $b \to B$ est un isomorphisme de K sur une sous algèbre K' de $\mathbf{M_k}(\mathbb{Z})$. Il faut voir que K' est une partie $\mathfrak{P}$-détachable de $\mathbf{M_k}(\mathbb{Z})$. Cela se déduit facilement du fait que tout sous espace vectoriel libre de $\mathbf{M_k}(\mathbb{Q})$ est $\mathfrak{P}$-détachable et $\mathfrak{P}$-libre . Ainsi K peut être présenté de manière à être une $\mathfrak{P}_0$-structure .

Voyons pourquoi K , ainsi présenté , est naturellement c-$\mathfrak{P}$-c en tant qu'anneau : soit K° une présentation de l'anneau en question qui en fasse un anneau c-$\mathfrak{P}$-c . Tout d'abord, en tant qu'anneau c-$\mathfrak{P}$-c , K° est une $\mathfrak{P}$-$\mathbb{Z}$-algèbre donc un $\mathfrak{P}$-$\mathbb{Z}$-module ; par ailleurs la présentation choisie est $\mathfrak{P}$-équivalente à celle de K comme $\mathbb{Z}$-module $\mathfrak{P}$-libre .
Ainsi l'application "identité" de K vers K° est-elle nécessairement une $\mathfrak{P}$-fonction.

Décrivons maintenant une $\mathfrak{P}_0$-présentation de l'anneau $K[X_1,X_2,...,X_n]$: nous présentons K comme ci dessus et $K[X_1,X_2,...,X_n]$ comme **Lst**(**Lst**(... (**Lst**(K)) ...)) (cf. $\mathbb{Z}[X,Y]$) , et nous prenons pour mesure du polynôme P le nombre $\|P\|$ = degré total + $\mathbf{lg}(\Sigma\, \sigma(b_i))$, où les b_i sont tous les coefficients , et avec $\sigma(b)$ défini ci-dessus.
Nous laissons au lecteur le soin de vérifier que c'est une $\mathfrak{P}_0$-structure , et au lecteur courageux celui de vérifier que c'est la structure d'anneau c-$\mathfrak{P}$-c naturelle. ❑

Remarques :

1) à partir de ces $\mathfrak{P}_0$-anneaux on peut en construire d'autres en utilisant les sous-anneaux $\mathfrak{P}$-détachables et les $\mathfrak{P}$-quotients . La théorie des bases standards conduit d'ailleurs au résultat suivant: tout idéal donné comme de type fini dans $\mathbb{Z}[X_1,X_2,...,X_n]$ est $\mathfrak{P}$-détachable.

2) la preuve doit être légèrement modifiée lorsque K ne possède pas de neutre pour la multiplication, car il se peut qu'on ait un b non nul pour lequel la multiplication par b soit

néanmoins égale à la fonction partout nulle: on se ramène au "bon cas" en "rajoutant" un élément 1 à K (c.-à-d. en considérant K comme une sous algèbre de l'anneau $\mathbb{Z} \times K$)

Proposition B.c4 : Soit K une $\mathbb{Q}$-algèbre qui est en outre un $\mathbb{Q}$-espace vectoriel libre de dimension finie : alors K peut être présentée de manière à être une $\mathfrak{P}_0$-structure d'anneau.
De plus K [X] , K [X_1,X_2,...,X_n] et (si K est intègre) K(X_1,X_2,...,X_n) , peuvent être présentées de manière à obtenir des $\mathfrak{P}_0$-structures .

Même principe de présentation (et de démonstration du résultat) que pour la proposition B.c3 et pour l'algèbre $\mathbb{Q}(X_1,X_2,...,X_n)$: notamment, dans le cas où K est un corps, on utilisera la présentation d'un élément de K sous forme d'une fraction de 2 "vecteurs" à coordonnées dans $\mathbb{Z}$ sur la base considérée pour obtenir un $\mathfrak{P}_0$-corps.

d) Groupes et monoïdes complètement $\mathfrak{P}$-calculables

$\mathfrak{P}_1$-monoïdes et $\mathfrak{P}_1$-groupes

L'associativité permet de donner une condition suffisante affaiblie pour le fait d'être c-$\mathfrak{P}$-c.

Proposition B.d1 : Tout $\mathfrak{P}_1$-monoïde est une structure algébrique complètement $\mathfrak{P}$-calculable. Même chose pour un $\mathfrak{P}_1$-groupe.

preuve> Soit tout d'abord (M , $\times$) un $\mathfrak{P}_1$-monoïde, et soit (u_1,u_2,...,u_n) dans **Lst**(M) une liste dont on veut calculer le produit. Soit $c \geq 1$ et $d \geq 0$ tels que

$$\| u \times v \| \leq c(\| u \| + \| v \|) + d.$$

Quitte à remplacer, le temps de la démonstration, la mesure $\| u \|$ par la mesure $\| u \|_1 = \| u \| + d$, on peut supposer que $d = 0$. Ensuite, supposons tout d'abord $n = 2^p$: on voit par récurrence sur p , en regroupant les facteurs 2 par 2 que :

$$\| u_1 \times u_2 \times ... \times u_n \| \leq c^p . \Sigma \| u_i \| .$$

Si n est quelconque, on est facilement ramené au calcul précédent (par exemple en multipliant par le neutre un nombre convenable de fois) et on a la majoration analogue :

$$\| u_1 \times u_2 \times ... \times u_n \| \leq c^{\mathbf{lg}(n)} . \Sigma \| u_i \| .$$ Or

$c^{\mathbf{lg}(n)} \leq c^{1+\log_2(n)} \leq c.n^{\log_2(c)}$. Cela montre que le produit, en tant qu'opération de **Lst**(M) vers M est **RESP** : il n'y a pas explosion de la taille lors du calcul.

Soit maintenant (G, $\times$, $x \to x^{-1}$) un $\mathfrak{P}_1$-groupe . On remarque que dans **Calc**(G) toute écriture peut être remplacée par une écriture de valeur égale (une fois le calcul effectué) et où les exposants -1 n'interviennent qu'au niveau le plus bas (c.-à-d. accolés à des éléments de G et non à des écritures comportant des produits).
On est donc ramené au cas des monoïdes. ❑

Groupes et monoïdes libres (dans la catégorie c-$\mathfrak{P}$-c)

On a immédiatement une caractérisation de $\mathbb{N}_1$ comme objet libre à un générateur dans la catégorie des $\mathfrak{P}$-monoïdes c-$\mathfrak{P}$-c et, plus généralement, de **Lst**(X) comme librement engendré par X :

Proposition B.d2 : Si $(M, \times)$ est un monoïde complètement $\mathfrak{P}$-calculable, alors la fonction $M \times \mathbb{N}_1 \to M : (b, n) \to b^n$ est une $\mathfrak{P}$-fonction. Pour b fixé, on obtient un $\mathfrak{P}$-homomorphisme : $\mathbb{N}_1$ est objet librement engendré par 1 dans la catégorie des monoïdes c-$\mathfrak{P}$-c . Et $\mathbb{N}_1$ est la présentation c-$\mathfrak{P}$-c naturelle des entiers naturels en tant que monoïde additif.

Proposition B.d3 : Soit X un $\mathfrak{P}$-ensemble-discret. Alors le monoïde **Lst**(X) est l'objet librement engendré par X dans la catégorie des monoïdes c-$\mathfrak{P}$-c (avec pour flèches les $\mathfrak{P}$-homomorphismes). Si X est fini, on obtient ainsi la présentation c-$\mathfrak{P}$-c naturelle du monoïde.
De même, **Lst**(X $\cup$ X') (où X' est une copie de X, disjointe de X) est le groupe librement engendré par X dans la catégorie des groupes c-$\mathfrak{P}$-c ; et pour X fini on obtient une structure naturellement c-$\mathfrak{P}$-c . En particulier $\mathbb{Z}_1$ est la présentation c-$\mathfrak{P}$-c naturelle du groupe des entiers relatifs.

On laisse le soin au lecteur d'énoncer les résultats analogues pour les monoïdes commutatifs et les groupes abéliens.

e) Présentations "en magma" ou "par formules"

Structures libres du point de vue complètement-$\mathfrak{C}$-calculable

Les résultats obtenus pour les anneaux $\mathbb{Z}[X_1,X_2,...,X_n]$ et pour les groupes libres sont en fait des cas particuliers d'un résultat général dans le cadre de l'"algèbre universelle" , c.-à-d. la théorie des structures algébriques qui ne font intervenir que des constantes et des lois de composition partout définies obéissant à des axiomes purement universels.

On obtient, en maths classiques, une structure librement engendrée par L en considérant le "magma" des "écritures de calculs à effectuer dans la structure qui n'impliquent que des constantes et des éléments de L " (ouf!) et en prenant pour relation d'égalité la relation d'équivalence la plus fine qui rende vraie les axiomes de la structure. Du point de vue constructif, on ne sait pas a priori si la relation d'égalité ainsi définie est la négation d'une relation de séparation, ou non. Enfin, même si la relation d'égalité est la négation d'une relation de séparation, on ne sait pas a priori si elle est décidable (c.-à-d.: si l'ensemble obtenu est discret).

Si L est un $\mathfrak{C}$-ensemble-discret, on obtiendra de la même manière une $\mathfrak{C}$-structure complètement $\mathfrak{C}$-calculable si et seulement si la relation d'équivalence obtenue (sur le $\mathfrak{C}$-ensemble formé par "les écritures de calculs etc...") est $\mathfrak{C}$-calculable. C'est de plus la structure librement engendrée par L dans la catégorie des structures algébriques "complètement $\mathfrak{C}$-calculables" du type voulu (groupe, anneau,...) . Lorsque L est fini on obtient une structure "naturellement complètement $\mathfrak{C}$-calculable" . Et l'on est évidemment intéressé à ce que la classe $\mathfrak{C}$ soit "la plus petite possible" , c.-à-d. que les calculs y soient le plus simples possibles.
Lorsque L est fini on n'a pas ipso facto, pour la structure librement engendrée par L un résultat affirmant qu'elle soit $\mathfrak{C}$-numérotable, ou même $\mathfrak{C}$-dénombrable.

Notons que notre traitement des structures c-$\mathcal{P}$-c libres a utilisé une voie plus directe bien que moins générale: au lieu de quotienter le magma des "écritures de calculs à effectuer ...." par la bonne relation d'équivalence, et de prouver que cette relation d'équivalence était $\mathcal{P}$-calculable , et de chercher enfin un système de représentants canoniques, nous avons utilisé des présentations déjà connues où chaque objet de la structure est représenté par un (ou des) élément(s) d'un $\mathcal{P}$-langage $Y \subset A^*$, ensuite nous avons montré que la présentation en question était une $\mathcal{P}$-présentation qui rendait la structure c-$\mathcal{P}$-c , et enfin qu'elle était libre du point de vue de la catégorie c-$\mathcal{P}$-c.

Remarque : Nous comprenons pourquoi la notion de structure "naturellement primitive récursive" est si efficace, en comparaison d'autres classes de constructions (je ne pense pas qu'il existe en dehors des ensembles finis de structures "naturellement de type $\mathcal{P}$"), c'est parce que pour la classe $\mathbb{P}\mathbf{r}$, la $\mathbb{P}\mathbf{r}$-calculabilité implique la $\mathbb{P}\mathbf{r}$-complète-calculabilité (proposition B.a1), et que la bonne notion est bel et bien la complète-$\mathcal{C}$-calculabilité (pour les structures algébriques).
Quant à la classe $\mathcal{P}_{00} := \mathcal{P} \cap$ **SPACERES**(n) , elle vérifie la même propriété que la classe $\mathbb{P}\mathbf{r}$ (remarque après la prop. B.a1) mais les lois de composition dans "le magma" en question sont seulement a priori $\mathcal{P}_0$, ce qui empêche un traitement général de la question. Notons cependant que ($\mathbb{N}$, + , $\times$) est "presque" naturellement de type $\mathcal{P}_{00}$: si **N'** est une $\mathcal{P}_{00}$-présentation de cette structure où la mesure de 1 est 1 , alors l'application identité de $\mathbb{N}$ vers **N'** est une $\mathcal{P}_1$-fonction : en effet, 2 = 1 + 1 est de mesure au plus 2 dans **N'** , ensuite on calcule dans **N'** un nombre en binaire par l'algorithme de Horner et on voit qu'un nombre de longueur n en binaire sera au maximum de mesure 3.n dans **N'**.

Présentations "en magma" ou "par formules"

Les structures libres construites précédemment sont des cas particuliers des présentations "en magma", définies ci-après.

Etant donné un ensemble dénombrable X avec une structure algébrique abstraite donnée par un nombre fini de lois de composition et de constantes, et par des relations, si X' est une partie $\mathcal{C}$-présentée de X , qui engendre X , on peut présenter X en utilisant la partie de **Calc**(X) ne faisant intervenir que des constantes et des éléments de X' . Pour cette présentation, les lois de composition sont dans $\cup_c$ **DTIME**(n+c) . Mais il reste le problème de l'égalité dans X et des autres relations faisant partie de la structure, qui peuvent ne pas être $\mathcal{C}$-décidables, ni même **Rec**-décidables

Nous appellerons cette présentation la présentation en magma (ou encore "par formules") sur le système générateur X' .

Si on a un ensemble X donné par une $\mathcal{C}$-présentation, et si on le munit d'une structure algébrique au moyen de lois de composition, on appellera présentation par formules de X la présentation par formules sur le système générateur X lui-même. La structure algébrique est complètement $\mathcal{C}$-calculable si et seulement si le $\mathcal{C}$-ensemble X est $\mathcal{C}$-équivalent à sa présentation par formules.

Exemples :

(1) La présentation par formules de ($\mathbb{Z}[T]$; + , − , $\times$) sur le système générateur (0 , 1 , T) est $\mathcal{P}$-équivalente à la présentation naturelle.

(2) Si nous considérons sur le $\mathcal{P}$-ensemble précédent $\mathbb{Z}[T]$ la structure algébrique (+ , − , $\times$, $P \to P^2$) avec la présentation par formules correspondante, nous obtenons une "généralisation" de la présentation creuse (on autorise en effet des exposants en binaire non seulement pour T , mais pour tout polynôme déjà écrit). Nous noterons $\mathbb{Z}[T]_m$ cette

présentation. Elle n'est sans doute pas bien adaptée aux calculs formels généraux, notamment pour ce qui concerne la relation d'égalité et la division euclidienne. Elle est par contre très bien adaptée à l'évaluation dans un anneau fini K, ou, plus généralement, dans un $\mathcal{P}$-anneau K où les lois $+, -, \times$ et l'élévation au carré seraient $\mathcal{P}_0$.

Ceci confirme l'appréciation selon laquelle la présentation d'une structure algébrique doit être choisie en fonction des calculs qu'on désire effectuer.

f) Algèbre d'un monoïde A[M], algèbres de polynômes

Algèbre d'un monoïde A[M]

Proposition B.f1 : Soit A un $\mathcal{P}$-anneau commutatif où l'addition est c-$\mathcal{P}$-c et M un $\mathcal{P}$-monoïde. On présente l'anneau $A[M]$ comme la $\mathcal{P}$-partie de **Lst**$(A \times M)$ formée par les listes d'éléments (a_i, m_i) avec $a_i \neq 0$ (sauf pour représenter 0) et sans répétition sur les m_i. On obtient ainsi un $\mathcal{P}$-anneau où l'addition est c-$\mathcal{P}$-c. De plus, si B est un $\mathcal{P}$-anneau où l'addition est c-$\mathcal{P}$-c, si $f : A \to B$ est un $\mathcal{P}$-homomorphisme d'anneau, $g : M \to B$ un $\mathcal{P}$-homomorphisme de M dans $(B, \times)$ et si tout $f(a)$ commute avec tout $g(m)$, alors l'homomorphisme canonique ("d'évaluation") de $A[M]$ vers B qui factorise f et g est un $\mathcal{P}$-homomorphisme.

Démonstration immédiate. Le caractère c-$\mathcal{P}$-c de l'addition est indispensable pour montrer que le produit dans $A[M]$ est bien une $\mathcal{P}$-fonction (lorsqu'on "regroupe" les coefficients d'un même m) et pour montrer que l'homomorphisme "d'évaluation" est une $\mathcal{P}$-fonction.

La présentation proposée pour $A[M]$ est donc "naturelle", à $\mathcal{P}$-isomorphisme près. En langage des catégories (et dans le cas des A-algèbres unitaires) : dans la catégorie des "$\mathcal{P}$-A-algèbres unitaires où l'addition est c-$\mathcal{P}$-c ", le foncteur d'oubli vers les $\mathcal{P}$-monoïdes (obtenu en ne conservant que la structure multiplicative) possède un adjoint à gauche .

Terminologie: Nous utilisons A-algèbre pour A-algèbre associative, non forcément unitaire. L'anneau A, lui, est supposé commutatif.

Remarque : En fait la commutativité de A n'est pas essentielle: lorsque A n'est pas commutatif, on peut construire de la même manière un anneau $A[M]$ où les $m \in M$ commutent avec les $a \in A$. La proposition B.f1 resterait inchangée.

Algèbres A[X]

Nous supposons toujours que A est un $\mathcal{P}$-anneau commutatif où l'addition est c-$\mathcal{P}$-c .

Il existe au moins 2 présentations de $A[X]$ intéressantes: la première est sous la forme **Lst**(A) (on écrit tous les coefficients jusqu'à celui de degré maxi) et la seconde est la présentation creuse, pour le cas où on estime que la plupart des coefficients sont nuls, sous la forme **Lst**$(A \times \mathbb{N})$, et on écrit uniquement les coefficients non nuls, en signalant l'exposant en binaire.

Nous réservons la notation $A[X]$ pour la première présentation: cette présentation donne une $\mathcal{P}$-A-algèbre $\mathcal{P}$-isomorphe à $A[\mathbb{N}_1]$. La 2ème, que nous noterons $A[X]_c$ donne une $\mathcal{P}$-A-algèbre $\mathcal{P}$-isomorphe à $A[\mathbb{N}]$. (calculs immédiats)

Proposition B.f2 : Soient A un $\mathcal{P}$-anneau commutatif où l'addition est c-$\mathcal{P}$-c et B une $\mathcal{P}$-A-algèbre unitaire où l'addition est c-$\mathcal{P}$-c.

1) si $b \in B$ est tel que la fonction $\mathbb{N}_1 \to B : n \to b^n$ soit une $\mathcal{P}$-fonction, alors l'homomorphisme "d'évaluation en b" : $P \to P(b)$ de $A[X]$ vers B est une $\mathcal{P}$-fonction.
2) si l'application $\mathbb{N}_1 \times B \to B : (n,b) \to b^n$ est une $\mathcal{P}$-fonction, alors la fonction d'évaluation : $(P,b) \to P(b)$ de $A[X] \times B$ vers B est une $\mathcal{P}$-fonction. (ce sera le cas si la multiplication dans B est c-$\mathcal{P}$-c).

preuve> Le 1) est un cas particulier de la proposition B.f1. Le 2) revient à introduire b comme paramètre: démonstration immédiate. ❑

Remarques :

1) il ne semble pas que la propriété pour le produit d'être c-$\mathcal{P}$-c passe de A à $A[X]$
2) en remplaçant $\mathbb{N}_1$ par $\mathbb{N}$ et $A[X]$ par $A[X]_c$ on obtient une proposition analogue ... mais il est bien rare que la fonction $\mathbb{N} \to B : n \to b^n$ soit une $\mathcal{P}$-fonction. (il y a le cas des corps finis)
3) la commutativité de A n'est pas indispensable: cf. la remarque après la prop. B.f1

Algèbres $A[X_1,X_2,...,X_n]$

Les algèbres $A[X][Y]$, $A[Y][X]$ sont $\mathcal{P}$-isomorphes à l'algèbre du monoïde $\mathbb{N}_1 \times \mathbb{N}_1$. On notera $A[X,Y]$ pour toute $\mathcal{P}$-présentation $\mathcal{P}$-isomorphe à l'une de ces 3.

On obtient immédiatement une proposition analogue à la précédente. Et on peut généraliser pour les anneaux de polynômes à un nombre fini de variables: en particulier:

Proposition B.f3 : Soient A un $\mathcal{P}$-anneau commutatif où l'addition est c-$\mathcal{P}$-c et B une $\mathcal{P}$-A-algèbre unitaire commutative où l'addition et le produit sont c-$\mathcal{P}$-c. Alors l'évaluation :

$A[X_1,X_2,...,X_n] \times B^n \to B : \quad (P, (b_1,b_2,...,b_n)) \to P(b_1,b_2,...,b_n)$ est une $\mathcal{P}$-fonction.

Deux remarques sur l'anneau $\mathbb{Z}[(X_i)_{i \in \mathbb{N}}]$

Il s'agit de l'anneau des polynômes à coefficients dans $\mathbb{Z}$ avec une infinité d'indéterminées. C'est donc la $\mathbb{Z}$-algèbre $A = \mathbb{Z}[M]$ du monoïde $M = \mathbb{N}_1^{(\mathbb{N})}$, et nous pouvons considérer la présentation correspondante. On n'obtient pas une structure c-$\mathcal{P}$-c: cf. le produit $(X_1+X_2) \times (X_3+X_4) \times ... \times (X_{2k-1}+X_{2k})$ qui occupe "beaucoup" d'espace une fois développé.

La première remarque est que, pour un $\mathcal{P}$-anneau K, il revient au même d'affirmer qu'addition et produit sont c-$\mathcal{P}$-c ou que l'évaluation des polynômes est une $\mathcal{C}$-opération, c.-à-d. : $A \times K^{(\mathbb{N})} \to K : (P, (k_i)_{i \in \mathbb{N}}) \to P((k_i)_{i \in \mathbb{N}})$ est une $\mathcal{P}$-opération.
On notera a contrario que le fait que K soit c-$\mathcal{P}$-c en tant qu'anneau signifie que l'évaluation de *toute formule* (et pas seulement les polynômes) est une $\mathcal{P}$-opération.

Deuxième remarque: si nous présentons l'anneau $\mathbb{Z}[(X_i)_{i \in \mathbb{N}}]$ au moyen de la présentation par formules sur le système générateur $\mathbb{Z} \cup \{ X_i ; i \in \mathbb{N} \}$ (lui même codé comme réunion disjointe de $\mathbb{Z}$ et $\mathbb{N}$), il y a moyen de deviner en temps polynomial si 2

expressions (indiquant des calculs à effectuer dans $\mathbb{Z}[(X_i)_{i \in \mathbb{N}}]$ représentent des éléments distincts de $\mathbb{Z}[(X_i)_{i \in \mathbb{N}}]$, en effet :

a) le degré du polynôme en chaque X_i ainsi que le nombre de X_i est majoré par la taille de la formule

b) deux polynômes à k variables de degrés $\leq d$ en chaque variable sont distincts si et seulement si ils sont évalués distincts en un k-uple $\in \{0,1,...,d\}^k$

c) l'évaluation d'une formule dans $\mathbb{Z}$ est un $\mathcal{P}$-calcul.

Il suffit donc de deviner un "point" où les deux expressions prennent des valeurs différentes. Ainsi, si $\mathcal{P} = \mathcal{NP}$, l'anneau $\mathbb{Z}[(X_i)_{i \in \mathbb{N}}]$ possèderait une $\mathcal{P}$-présentation qui le rendrait c-$\mathcal{P}$-c [16].

g) Pourquoi $\mathbb{Z}$ marche-t-il si bien ?

Introduction

Nous avons établi le caractère c-$\mathcal{P}$-c de $\mathbb{Z}$-modules, d'anneaux et de corps construits à partir de $\mathbb{Z}$ en utilisant systématiquement l'argument suivant : lorsqu'on remplace la mesure "naturelle" par la mesure $n + \mathbf{lg}(\Sigma|\text{coefficients}|)$, où n est le nombre de coefficients dans $\mathbb{Z}$ nécessaires à la description de l'objet considéré, les lois de composition considérées deviennent $\mathcal{P}_0$. Tout cela marche bien "parce que" majorer la grandeur en valeur absolue d'un entier permet de majorer la place occupée par l'entier en écriture binaire. Le raisonnement par exemple serait complètement en défaut si on prenait des coefficients rationnels au lieu de prendre des coefficients entiers.

L'idée pour généraliser les résultats obtenus à partir de $\mathbb{Z}$ doit donc être cherchée un peu plus loin: nos raisonnements sont "trop" simples pour pouvoir être généralisés parce qu'ils utilisent des propriétés trop fortes de $\mathbb{Z}$.

Le rêve serait de démontrer un théorème du genre: si K est un anneau où l'addition et le produit sont c-$\mathcal{P}$-c, alors il en est de même pour **Flin**(K) et pour K[X] (on sait déjà que, pour K intègre, il en est de même pour le corps des fractions de K). Cela semble improbable.

Nous pouvons cependant démontrer un théorème analogue pour une certaine classe de $\mathcal{P}$-anneaux qui possèdent des propriétés de majorations assez fortes pour la mesure de la somme de 2 éléments.

Majoration pour l'addition itérée

Lemme 1 : Si (K,+) est un monoïde $\mathcal{P}$-présenté où est vérifiée l'inégalité:

$$\| a + b \| \leq \sup(\| a \|, \| b \|) + C$$

alors pour $(u_1, u_2, \ldots, u_n)$ dans **Lst**(K), on a l'inégalité:

$$\| u_1 + u_2 + \ldots + u_n \| \leq \sup(\| u_i \|) + C.\mathbf{lg}(n-1)$$

preuve>

– si $n = 2^k$, alors $\mathbf{lg}(n-1) = k-1$, démonstration par récurrence sur k immédiat

---

[16] Divertissement mathématique: si l'égalité est $\mathcal{P}$-testable (dans l'anneau $\mathbb{Z}[(X_i)_{i \in \mathbb{N}}]$ muni de la présentation par formules ci-dessus) alors $\mathcal{P} = \mathcal{NP}$.

– si $n = 2^k + m$, avec $0 < m < 2^k$, on peut supposer (récurrence) l'inégalité vraie pour m , et elle passe à n , puisque $\mathbf{lg}(n-1) = k$ et $\mathbf{lg}(m) < k$. ❑

Définition des $\mathfrak{P}_0$-anneaux

Définition B.g1 : Un $\mathfrak{P}$-anneau K sera appelé un **$\mathfrak{P}_0$-anneau** lorsque:

1) K est $\mathfrak{P}$-dénombrable
2) l'addition vérifie la majoration suivante:
$$\| a + b \| \leq \sup(\| a \| , \| b \|) + C$$
3) la multiplication est c-$\mathfrak{P}$-c

Majoration pour les déterminants

Proposition B.g1 : Soit K un $\mathfrak{P}_0$-anneau commutatif. On représente une matrice carrée de $\mathbf{M_n}(K)$ par la liste de ses n^2 coefficients, (on peut prendre pour mesure de la matrice (u_{ij}) le nombre $s = \max(n,\sup(\|u_{ij}\|))$. La fonction déterminant est **RESP** (cette fonction est définie sur l'ensemble des listes à n^2 éléments de K , pour n variable, ensemble qui représente la réunion disjointe des $\mathbf{M_n}(K)$)

Remarque : on établira en C que, sous certaines hypothèses supplémentaires, la fonction déterminant est alors une $\mathfrak{P}$-fonction. (cf. prop. C.b2, Th C.b1 et C.d1)

preuve> Puisque le produit est c-$\mathfrak{P}$-c, il existe un polynôme Q tel que Q(s) majore la mesure de tout produit de n facteurs pris parmi les u_{ij}. Donc on obtient par le lemme 1 les majorations:
$$\| \det((u_{ij})) \| \leq \mathbf{lg}(n!).Q(s) \leq n.\mathbf{lg}(n).Q(s) \leq (X^2Q)(s)$$ ❑

Propriétés de stabilité des $\mathfrak{P}_0$-anneaux

Proposition B.g2 :

Si (K , +, × , 0 , 1) est un $\mathfrak{P}_0$-anneau, alors il en est de même pour:

– tout sous anneau qui est une partie $\mathfrak{P}$-détachable de K
– tout quotient $\mathfrak{P}$-dénombrable de K par un idéal $\mathfrak{P}$-détachable
– $\mathbf{M_n}(K)$ et **Flin**(K) (réunion emboîtée des $\mathbf{M_n}(K)$)
– $K[X_1,X_2,...,X_n]$
– K [M] , si M est un monoïde $\mathfrak{P}$-dénombrable c-$\mathfrak{P}$-c qui possède "peu d'objets de petite taille" (c.-à-d. : il existe un polynôme fixé Q tel que les objets sous forme réduite canonique et de taille inférieure à p sont en nombre au plus Q(p))

(Dans les trois derniers cas la mesure de l'objet x est précisée dans la démonstration)

Remarques :

1) le caractère $\mathfrak{P}_0$, ne se conserve par contre pas par passage au corps des fractions

2) en fait **Flin**(K) ne possède pas d'élément neutre pour la multiplication, ce n'est donc pas un anneau, ... mais il est $\mathfrak{P}_0$,

preuve> Les 2 premières stabilités sont évidentes.
Voyons $\mathbf{M_n}(K)$: reprenons la mesure décrite dans la prop. B.g1 . Pour l'addition de 2 matrices, la majoration est immédiate.
Il reste à voir que le produit :

$$((U_1, U_2, \ldots, U_p)) \rightarrow U_1 \times U_2 \times \ldots \times U_p,$$

de $\mathbf{Lst}(\mathbf{M_n}(K))$ vers $\mathbf{M_n}(K)$ est **RESP** (cf. prop. B.a1). Or chaque coefficient du produit $U_1 \times U_2 \times \ldots \times U_p$ est égal à une somme de n^{p-1} produits de p coefficients des matrices U_k, et $\mathbf{lg}(n^{p-1}) \simeq (p-1).\mathbf{lg}(n)$. Le calcul de majoration est donc analogue à celui fait pour le déterminant.
Comme nous avons intégré n au calcul de majoration, il vaut également pour le produit dans $\mathbf{Flin}(K)$, réunion emboîtée des $\mathbf{M_n}(K)$.
Raisonnements et calculs analogues pour K[X] , avec la mesure

$$\|Q\| = \max(\deg(Q), \sup(\|\text{coefficients}\|)).$$

Puis récurrence pour $K[X_1,X_2,\ldots,X_n]$.
Le dernier cas est une généralisation du précédent, puisque $K[X_1,X_2,\ldots,X_n]$ peut être considéré comme la K-algèbre du monoïde additif $M = \mathbb{N}_1^n$ qui vérifie les hypothèses convenables.
Nous présentons K[M] comme expliqué en f), avec pour mesure:

$$\|\Sigma\, a_i\, m_i\| = \sup(\|a_i\|, \|m_i\|, n).$$

La majoration pour l'addition est immédiate. Il nous faut de plus une majoration polynomiale pour la mesure du produit itéré: soit

$$\prod_{i=1}^{k} x_i = \prod_{i=1}^{k} \sum_{j=1}^{n_i} a_{i,j} \,.\, m_{i,j} = \sum_{j=1}^{n} b_j \,.\, m_j$$

$$\text{avec } b_j = \sum a_{1,j_1}.a_{2,j_2}\ldots.a_{k,j_k}$$

somme étendue aux $(j_1,j_2,\ldots,j_k)$ vérifiant $m_{1,j_1}.m_{2,j_2}\ldots m_{k,j_k} = m_j$
Le coefficient b_j de m_j est une somme possédant moins de $n_1.n_2\ldots n_k$ termes, ce qui donne une majoration convenable de sa taille:

$$\|b_j\| \leq P(\max(k, \sup(\|a_{i,j'}\|))) + C.k.\sup(\mathbf{lg}(n_{j'})) \leq T(\max(k,\sup(\|x_i\|)))$$

où P et T sont des polynômes fixés.
Enfin, il nous faut une majoration de n , c.-à-d. : qu'il n'y ait pas trop de termes $b_j.m_j$, nous utilisons pour cela le fait que M possède "peu d'objets de petite taille" : en effet on a

$$\|m_i\| \leq R(\max(k, \sup(\|m_{i,j}\|)))\ ,$$

où R est un polynôme fixé, ceci parce que M est un monoïde c-$\mathcal{P}$-c, et donc: $n < Q(R(\max(k,\sup(\|m_{i,j}\|)))$, et Q(R) est un polynôme fixé. ❑

Remarque : le calcul de majoration dans $\mathbf{M_n}(K)$ ci-dessus suggère qu'un exemple d'anneau K où + et × seraient c-$\mathcal{P}$-c sans que la même propriété soit vérifiée pour $\mathbf{M_2}(K)$, pourrait être cherché du coté d'un anneau où l'on aurait "assez souvent" $\|x + y\| \geq \|x\| + \|y\|$.

Quelques exemples de $\mathcal{P}_0$,-anneaux

Nous pouvons compter parmi les $\mathcal{P}_0$,-anneaux les anneaux suivants:

– $\mathbb{Z}$, $\mathbf{M_n}(\mathbb{Z})$, $\mathbf{Flin}(\mathbb{Z})$, $\mathbb{Z}[X_1,X_2,\ldots,X_k]$ pour leur présentation naturelle, et avec les mesures définies en c) (indicateur polynomialement relié à: nombre de coefficients + $\mathbf{lg}(\Sigma|\text{coefficients}|)$)

– tout anneau fini

– tout anneau qui est un $\mathbb{Z}$-module libre de dimension finie: il est en effet isomorphe à un sous anneau $\mathcal{P}$-détachable de $\mathbf{M_n}(\mathbb{Z})$ (cf. prop. B.c3), on le munit de la présentation

correspondant à cette sous-structure: en particulier les anneaux d'entiers dans les corps de nombres.

– tout anneau construit à partir de l'un des précédents par l'une des constructions autorisées par la proposition B.g2

Nous donnons maintenant un exemple de $\mathfrak{P}_0$,-anneau qui est une $\mathbb{Q}$-algèbre mais qui n'est pas de type fini en tant que $\mathbb{Q}$-algèbre.

Ceci en application de la dernière propriété de stabilité énoncée en B.g2 : si nous considérons le monoïde additif de $\mathbb{Q}_1$ (corps des fractions de $\mathbb{Z}_1$), nous voyons qu'il répond à l'hypothèse "peu d'objets de petite taille"; cependant l'addition n'est pas c-$\mathfrak{P}$-c ; on peut néanmoins considérer des sous groupes additifs de $\mathbb{Q}_1$ qui sont c-$\mathfrak{P}$-c : par exemple les sous-groupes T_r obtenus en imposant que le dénominateur de la fraction soit une puissance d'un entier r fixé. L'algèbre $K[T_r]$ obtenue est l'algèbre des polynômes à coefficients dans K et avec des exposants k/r^n (r fixé) pour X. Lorsque $K = \mathbb{Q}$, certains quotients de cette algèbre sont des extensions infinies de $\mathbb{Q}$ où l'addition et le produit sont c-$\mathfrak{P}$-c : par exemple, en remplaçant X par 2 , c.-à-d. en faisant le quotient par l'idéal engendré par $X - 2$. En quotientant par un idéal convenable contenant $X - 1$, on obtient une extension infinie engendrée par des racines de l'unité.

Structure de $\mathfrak{P}$ -calculabilité naturelle dans les anneaux commutatifs de présentation finie

D'après la théorie des bases standards, tout idéal de type fini de $\mathbb{Z}[X_1,X_2,...,X_n]$ est une $\mathfrak{P}$-partie de cet anneau (pour sa $\mathfrak{P}$-présentation naturelle).

Comme par ailleurs l'anneau $\mathbb{Z}[X_1,X_2,...,X_n]$ est l'objet librement engendré par les X_i dans la catégorie des $\mathfrak{P}$-anneaux où addition et produit sont c-$\mathfrak{P}$-c, on obtient le résultat suivant:

> Tout anneau commutatif A de présentation finie est naturellement c-$\mathfrak{P}$-c; on peut prendre comme $\mathfrak{P}$-présentation naturellement c-$\mathfrak{P}$-c , sa $\mathfrak{P}$-présentation comme quotient de $\mathbb{Z}[X_1,X_2,...,X_n]$.
> Plus généralement: si A est un anneau commutatif engendré par n éléments $a_1,a_2,...,a_n$ qui est $\mathfrak{P}$-présenté de manière que l'addition et le produit soient c-$\mathfrak{P}$-c, alors la $\mathfrak{P}$-présentation de A comme quotient de $\mathbb{Z}[X_1,X_2,...,X_n]$ (via l'homomorphisme d'évaluation $X_i \to a_i$) est naturellement c-$\mathfrak{P}$-c.
> De plus cette présentation en fait à la fois un $\mathfrak{P}_0$-anneau où les déterminants sont $\mathfrak{P}$-calculables[17], et, s'il est $\mathfrak{P}$-dénombrable, un $\mathfrak{P}_0$,-anneau.

[17] En effet les déterminants sont $\mathfrak{P}$-calculables dans $\mathbb{Z}[X_1,X_2,...,X_n]$ comme nous le verrons dans le § C.

C) ALGÈBRE LINÉAIRE EN TEMPS POLYNOMIAL

Introduction

L'algèbre linéaire est essentiellement l'étude des systèmes d'équations linéaires.

Lorsqu'on se situe dans un corps où l'égalité est décidable, le problème est entièrement résolu, du point de vue mathématique, soit par la méthode du pivot de Gauss, soit, dans le cas commutatif, par la méthode des déterminants et les formules de Cramer.

Que se passe-t-il du point de vue calculatoire ?

La méthode du pivot utilise peu de calculs : le nombre d'opérations arithmétiques élémentaires (addition, multiplication, division, test d'égalité à 0) pour traiter une matrice $n \times n$ est majoré par un polynôme en n.

Les formules de Cramer donnent quant à elles, dans un $\mathcal{P}_0$-corps, une solution **DTIME**((n+2)!) du problème, si l'on s'en tient aux formules de définition explicites des déterminants. Par exemple elle est totalement impraticable pour une matrice 20×20. Par contre elle donne des renseignements d'ordre théorique décisifs, à savoir que le fonctionnement des systèmes d'équations linéaires est gouverné par des polynômes en les coefficients du système (les déterminants justement).

Par ailleurs, les formules de Cramer montrent que, lorsque la fonction déterminant est $\mathcal{P}$-calculable, les systèmes d'équations linéaires sont $\mathcal{P}$-résolubles, même si la méthode est incontestablement plus lourde que celle du pivot.

Il reste à déterminer des conditions suffisantes faciles à vérifier pour la $\mathcal{P}$-calculabilité des déterminants. On trouve grosso-modo que la $\mathcal{P}$-calculabilité des déterminants équivaut au fait que le produit des matrices est complètement $\mathcal{P}$-calculable (cf. prop. C.b1 et Th C.b1). Or cette propriété est vérifiée pour les anneaux les plus couramment étudiés (cf. § B f), et elle est de plus très stable.

Vu l'intérêt "pratique" de la méthode du pivot, il est intéressant d'étudier sous quelles conditions elle est praticable en temps polynomial, c.-à-d. sans explosion de la taille des coefficients. C'est ce que nous faisons au § d), où nous exposons la méthode de Bareiss.

La méthode du pivot, quoiqu'utilisant peu d'opérations arithmétiques élémentaires, n'est pas garantie a priori contre une explosion de la taille des coefficients. Si par exemple on se situe dans le $\mathcal{P}$-corps $\mathbb{Q}((X_i)_{i \in \mathbb{N}})$, et qu'on veuille traiter par la méthode du pivot une matrice $n \times n$ dont les coefficients sont des X_i distincts, on fera un calcul purement formel, et on retombera sur les formules de Cramer, avec un calcul plus long que celui donné par les formules de définition des déterminants[18]. Phénomène plus grave encore: si on applique la méthode du pivot à une matrice à coefficients dans $\mathbb{Q}$ sans simplifier les fractions obtenues au fur et à mesure des calculs, la taille des coefficients explosera.

Or, si on examine l'évolution des coefficients d'une matrice triangulée par la méthode du pivot, on s'aperçoit que tous les coefficients successifs peuvent s'exprimer comme quotients de déterminants extraits de la matrice de départ. La morale est qu'on est a priori garanti contre une

[18] Le corps $\mathbb{Q}((X_i)_{i \in \mathbb{N}})$ cité en exemple ne semble pas pouvoir être rendu complètement $\mathcal{P}$-calculable par une présentation adéquate: cf. fin du § B f

explosion de la taille des coefficients dans la méthode du pivot si on sait majorer la taille des déterminants.

Autrement dit: dans un $\mathfrak{P}$-corps $\mathfrak{P}$-dénombrable le seul obstacle à la $\mathfrak{P}$-résolubilité des systèmes d'équations linéaires (et au calcul en temps polynomial des déterminants) par la méthode du pivot provient éventuellement de l'impossibilité de majorer polynomialement la taille des déterminants : l'algèbre linéaire sur un $\mathfrak{P}$-corps $\mathfrak{P}$-dénombrable est en temps polynomial si et seulement si la fonction dét est **RESP** (polynomialement majorée en taille du résultat). (Th C.d1)

Dans le § a) nous étudions la propriété pour un anneau d'être **Mat-c$\mathfrak{P}$c**, c.-à-d. que le produit matriciel y est complètement $\mathfrak{P}$-calculable. Elle équivaut à l'inversibilité en temps polynomial des matrices triangulaires avec des 1 sur la diagonale, et possède une forte stabilité.

Dans le § b) nous étudions la propriété pour un anneau commutatif d'être **Det-c$\mathfrak{P}$c**, c.-à-d. avoir les déterminants $\mathfrak{P}$-calculables , et nous montrons l'équivalence avec la propriété d'être **Mat-c$\mathfrak{P}$c** dans le cas des $\mathfrak{P}$-$\mathbb{Q}$-algèbres. Il est d'ailleurs probable que l'équivalence puisse être démontrée sans restriction aucune.

Dans le § c) consacré aux $\mathfrak{P}$-corps commutatifs, nous montrons l'équivalence entre **Det-c$\mathfrak{P}$c**, la $\mathfrak{P}$-calculabilité des relations de dépendance linéaire entre vecteurs et la $\mathfrak{P}$-résolubilité des systèmes d'équations linéaires. Nous montrons alors la $\mathfrak{P}$-calculabilité de la géométrie des sous-espaces de dimension finie. Nous établissons enfin quelques nouvelles propriétés de stabilité pour les anneaux **Det-c$\mathfrak{P}$c**.

Dans le § d) nous exposons la méthode de Bareiss, qui peut être vue soit comme une méthode de calculs de déterminants, soit comme une méthode du pivot "améliorée". Pour que cette méthode fonctionne en temps polynomial, il suffit que l'on soit dans un $\mathfrak{P}$-anneau intègre $\mathfrak{P}$-dénombrable où les divisions exactes peuvent être effectuées en temps polynomial.

a) Calcul matriciel sur un $\mathfrak{P}$-anneau

Matrices sur un $\mathfrak{P}$-anneau K

Nous nous intéressons à la complexité de calculs impliquant des matrices $A = (a_{ij})$ de K^{hxc}, les nombres de lignes et de colonnes h et c n'étant pas fixés a priori.

Il est naturel de prendre pour mesure de la grandeur de A le nombre $\| A \| = \Sigma \| a_{ij} \|$. Nous noterons n_A le sup de h et c , et s_A le sup des $\| a_{ij} \|$. La mesure A est polynomialement reliée à $n_A + s_A$. Si nécessaire, nous précisons h_A et c_A au lieu de h et c .

Il est pratique d'utiliser un ensemble **Mat**(K) , réunion disjointe des K^{hxc}. Nous pouvons par exemple réaliser cet ensemble sous la forme d'une $\mathfrak{P}$-partie de **Lst**(**Lst**(K)) : une matrice est vue comme la liste de ses vecteurs colonnes V_1 , V_2 , ... , V_c qui sont eux mêmes des éléments de **Lst**(K) : $V_j = (a_{1j} , a_{2j} , ... , a_{lj})$.

L'ensemble **Mat**(K) est muni de 2 lois de composition + et $\times$ non partout définies, mais définies sur des $\mathfrak{P}$-parties convenables de **Mat**(K) $\times$ **Mat**(K).

Un élément de **Mat**(K) peut servir à représenter une application linéaire de K^c vers K^h ou un système de h vecteurs de K^c. En outre en modifiant la relation d'égalité, cette même matrice peut servir à représenter des objets de différents ensembles:

– une application linéaire de $K^{(\mathbb{N}_1)}$ vers $K^{(\mathbb{N}_1)}$, espace vectoriel[19] $\mathfrak{P}$-présenté par **Lst**(K) muni de la relation d'égalité qui identifie une liste de c éléments à toute liste plus longue obtenue en rajoutant des 0 à la fin: nous noterons **Flin**(K) l'ensemble obtenu à partir de **Mat**(K) en changeant de la même manière la relation d'égalité . Lorsque K est commutatif, **Flin**(K) est une K-algèbre[20] sans élément neutre pour la multiplication. Il est clair que **Flin**(K) est un $\mathfrak{P}$-ensemble.

– un sous-espace vectoriel de K^h : celui engendré par les c vecteurs colonnes de la matrice. On ne peut dire a priori si l'ensemble obtenu , que nous noterons **Fsv**(K) , muni de la présentation ainsi décrite, est un $\mathfrak{P}$-ensemble.

– un sous-espace vectoriel de $K^{(\mathbb{N}_1)}$: nous noterons **Sv**(K) l'ensemble de ces sous-espaces, muni de cette présentation. C'est l'ensemble de tous les sous-espaces vectoriels finiment engendrés de $K^{(\mathbb{N}_1)}$.

Nous noterons **Lin**(K) l'ensemble des applications linéaires, de $K^{(\mathbb{N}_1)}$ vers $K^{(\mathbb{N}_1)}$, de la forme a.I + M , où $a \in K$ et $M \in$ **Flin**(K), présenté sous la forme $K \times$ **Flin**(K) . Ceci revient à rajouter l'élément neutre manquant à **Flin**(K) . Lorsque K est commutatif c'est une K-algèbre unitaire.

Proposition C.a1 :

Les 4 propriétés suivantes du $\mathfrak{P}$-anneau K sont équivalentes:

i. l'addition dans K est complètement $\mathfrak{P}$-calculable

ii. le produit dans **Mat**(K) est une $\mathfrak{P}$-fonction

iii. le produit dans **Flin**(K) est une $\mathfrak{P}$-fonction

iv. **Lin**(K) est un $\mathfrak{P}$-anneau

v. K[X] est un $\mathfrak{P}$-anneau

Si ces propriétés sont vérifiées l'addition est c-$\mathfrak{P}$-c dans **Mat**(K) , **Lin**(K) , **Flin**(K) et K[X].

preuve>

Il est clair que ii. , iii. et iv. sont équivalentes;

L'implication ii. $\Rightarrow$ i. se voit en multipliant un vecteur ligne (1 , 1 ,..., 1) par un vecteur colonne $(a_1 , a_2 , ... , a_c)$; l'implication i $\Rightarrow$ ii. s'obtient par un calcul immédiat.

L'implication i. $\Rightarrow$ v. a été démontrée en prop. B.f1; l'implication v. $\Rightarrow$ i. se démontre en considérant le coefficient de degré c-1 dans le polynôme produit du polynôme de coefficients (1 , 1 ,..., 1) par celui de coefficients $(a_1 , a_2 , ... , a_c)$. ❑

Inversion des matrices triangulaires et calculs de produits itérés de matrices

Nous noterons **Trimat**(K) l'ensemble des matrices carrées triangulaires supérieures de K , avec uniquement des 1 sur la diagonale . Une matrice $n \times n$ de **Trimat**(K) peut s'écrire $A = I - U$ avec $U^n = 0$ et admet une inverse $A^{-1} = I + U + U^2 + ... + U^{n-1}$.

L'ensemble **Trimat**(K) ainsi présenté est manifestement un $\mathfrak{P}$-ensemble.

---

19 bien que K ne soit pas nécessairement un corps, nous employons le mot espace vectoriel que le lecteur voudra bien lire "module libre" (ou même "module à gauche libre" dans le cas non commutatif)

20 rappel : nous utilisons "K-algèbre" pour K-algèbre associative, non forcément unitaire, et avec K commutatif seulement.

Théorème C.a1 :

Les 4 propriétés suivantes du $\mathcal{P}$-anneau K sont équivalentes :

i. l'inversion dans **Trimat**(K) est une $\mathcal{P}$-fonction

ii. le produit dans **Mat**(K) est complètement $\mathcal{P}$-calculable

iii. le produit dans **Flin**(K) est complètement $\mathcal{P}$-calculable

iv. le produit dans **Lin**(K) est complètement $\mathcal{P}$-calculable

Lorsque c'est vérifié, l'addition et le produit dans K , **Mat**(K), **Flin**(K), **Lin**(K) et K[X] sont complètement $\mathcal{P}$-calculables.

preuve>

ii. $\Rightarrow$ i. : l'addition dans K est complètement $\mathcal{P}$-calculable d'après la proposition C.a1, elle l'est aussi dans **Mat**(K) , et dans ce cas, vu que le produit est également complètement $\mathcal{P}$-calculable, la formule ci-dessus donnant A^{-1} est le programme d'un $\mathcal{P}$-calcul.

i. $\Rightarrow$ ii. :

– montrons d'abord que le produit dans K est complètement $\mathcal{P}$-calculable. On considère le système d'équations $x_1 = a_1 . x_2$, $x_2 = a_2 . x_3$, ... , $x_j = a_j . x_{j+1}$, $x_{j+1} = 1$; il se résout en inversant la matrice triangulaire supérieure avec les $-a_i$ au dessus de la diagonale. Or cette matrice est $\mathcal{P}$-reliée à la liste $(a_1 , a_2 , ... , a_j)$.

– montrons ensuite que le produit dans **Mat**(K) est complètement $\mathcal{P}$-calculable: nous relisons la démonstration que nous venons de faire en interprétant les a_i comme les matrices carrées dont le produit est à calculer et les x_i comme des matrices carrées inconnues: on obtient la solution par inversion d'une matrice triangulaire constituée des blocs I sur la diagonale, $-a_i$ au dessus de la diagonale et 0 ailleurs.

On peut présenter ce même argument comme suit: si L est l'anneau des matrices carrées $n \times n$ sur K l'inversion dans **Trimat**(L) se déduit immédiatement de l'inversion dans **Trimat**(K).

On notera que le passage de la liste des matrices à multiplier à la matrice triangulaire constituée de blocs est bien de type $\mathcal{P}$.

– montrons maintenant que l'addition est complètement $\mathcal{P}$-calculable dans K: il suffit de multiplier les matrices triangulaires 2×2 ayant pour coefficient au dessus de la diagonale les a_i qu'on veut additionner.

ii. et iii. sont clairement équivalents,

iv. implique iii. (clair)

iii $\Rightarrow$ iv. : supposons qu'on ait un produit d'éléments $(a_i.I + M_i)$ à calculer dans **Lin**(K) : soit n le sup des n_{M_i}, on effectue le produit des matrices $(a_i.I_n + M_i)$ dans l'anneau des matrices carrées $n \times n$, on obtient une matrice P ; effectuons par ailleurs le produit des a_i dans K , on obtient un élément a , on écrit P sous forme $a. I_n + M$, et le produit à calculer dans **Lin**(K) n'est autre que a.I + M

Enfin si ii. est vérifiée on obtient que la multiplication dans K[X] est complètement $\mathcal{P}$-calculable comme suit:

si $P_1 , P_2 , ... , P_j$ sont les polynômes à multiplier, de degrés $d_1 , d_2 , ... , d_j$, et si $n = 1+ d_1+ d_2 + ... + d_j$, on considère, sur l'espace de dimension n formé par les polynômes de degré $n – 1$, et pour la base canonique, les matrices des applications linéaires : multiplication par P_i tronquée éventuellement au degré $n – 1$. Le produit des matrices correspond au produit des polynômes, et le polynôme produit se lit sur la $1^{ère}$ colonne de la matrice produit. Il suffit donc de vérifier que le passage de la liste $[P_1 , P_2 , ... , P_j]$ à la liste des matrices $n \times n$ correspondantes est bien de type $\mathcal{P}$. ❑.

Remarques :

– divertissement mathématique : si le produit dans K[X] est c-$\mathcal{P}$-c, alors il en est de même dans **Mat**(K) ?

– lorsque K est un $\mathcal{P}$-corps vérifiant les propriétés équivalentes de la proposition, l'inversion des matrices est également une $\mathcal{P}$-fonction sur l'ensemble des matrices triangulaires avec des coefficients tous non nuls sur la diagonale.

Le théorème C.a1 nous conduit à poser la définition suivante:

Définition C.a1 : Soit K un $\mathcal{P}$-anneau.

On dira que **le calcul des matrices dans K est complètement en temps polynomial**, ou encore que K est **Mat-c$\mathcal{P}$c** lorsqu'il vérifie les propriétés équivalentes énoncées au théorème C.a1.

On notera qu'en calcul purement formel le produit des matrices n'est pas c-$\mathcal{P}$-c (on peut le voir en multipliant n matrices 2×2) et que donc un anneau peut a priori être c-$\mathcal{P}$-c sans être **Mat-c$\mathcal{P}$c** . Problème ouvert : fournir un exemple concret où cette situation se produirait. (cf. à ce sujet le § B.g)

Stabilité de la classe des anneaux **Mat-c$\mathcal{P}$c**

La classe des anneaux **Mat-c$\mathcal{P}$c** est très stable, comme en témoigne la proposition suivante.

Proposition C.a2 : Soit K un anneau **Mat-c$\mathcal{P}$c** , alors sont également **Mat-c$\mathcal{P}$c** les anneaux suivants :

i. tout sous anneau de K qui est une partie $\mathcal{P}$-détachable de K
ii. tout $\mathcal{P}$-quotient de K
iii. l'anneau $\mathbf{M_n}$(K) des matrices carrées $n \times n$ à coefficients dans K
iv. **Lin**(K)
v. $K[X_1,X_2,...,X_n]$

et, lorsque K est commutatif

vi. le localisé en S de K , si S est une partie multiplicative $\mathcal{P}$-détachable de K ne contenant pas de diviseur de 0 .
vii. le corps des fractions de K , si K est intègre
viii. toute K-algèbre unitaire de dimension finie, si K est intègre et $\mathcal{P}$-divisible.

Remarques :

1) les anneaux que l'on peut construire à partir de $\mathbb{Z}$ et des anneaux finis par enchaînement de constructions correspondant aux stabilités ci-dessus énoncées forment un stock assez important.

2) pour que le quotient d'un $\mathcal{P}$-anneau K par un idéal bilataire soit un $\mathcal{P}$-quotient , il faut et il suffit que l'idéal soit $\mathcal{P}$-détachable.

preuve>

i. et ii. sont immédiats;

iii. se voit en "juxtaposant" les coefficients d'une matrice $h \times c$ à coefficients dans $\mathbf{M_n}$(K) de manière à en faire une matrice $h.n \times c.n$ à coefficients dans K , on est ramené à

effectuer des produits dans **Mat**(K) puis à réinterpréter le résultat en le décomposant en blocs $n \times n$.

vi. Tout d'abord l'addition dans K_S est c-$\mathcal{P}$-c : pour additionner une liste de fractions, on les réduit au même dénominateur (or le produit dans S est c-$\mathcal{P}$-c) puis on additionne les numérateurs. Cet argument revient à dire qu'en calcul purement formel, l'addition des fractions est c-$\mathcal{P}$-c.
Que le produit soit c-$\mathcal{P}$-c dans **Mat**(K_S) résulte du fait qu'on obtient une $\mathcal{P}$-présentation $\mathcal{P}$-équivalente à **Mat**(K_S) en prenant **Mat**(K) $\times$ S , où le couple (A,d) représente la matrice (1/d).A à coefficients dans K_S . On termine en remarquant que le produit est c-$\mathcal{P}$-c dans **Mat**(K) et dans S.

vii. est un cas particulier de vi.

viii. se déduit de iii. et i. lorsque K est un $\mathcal{P}$-corps commutatif parce qu'une K-algèbre de dimension finie n est canoniquement isomorphe à une sous-algèbre de dimension n de $\mathbf{M_n}$(K): or toutes les applications linéaires entre espaces de dimensions finies sont des $\mathcal{P}$-fonctions et dans un espace vectoriel K^m , tout sous espace de dimension n est $\mathcal{P}$-détachable parce qu'il est noyau d'une application linéaire.
Lorsque K est intègre et $\mathcal{P}$-divisible, l'argument s'applique au corps des fractions L de K. Une fois le calcul fait dans L , on sait revenir dans K puisque K est supposé $\mathcal{P}$-divisible.
Remarque : peut on trouver un argument plus général qui s'applique à toute K-algèbre unitaire de dimension finie ?

iv. On raisonne essentiellement comme pour le théorème C.a1 : pour effectuer le produit d'une liste de matrices à coefficients dans **Lin**(K), on considère le sup n des n_{Mi} où les a_i. I + M_i sont tous les coefficients de toutes les matrices de la liste et on effectue le produit de la liste des matrices correspondantes dont les coefficients "a_i. I_n + M_i" sont dans $\mathbf{M_n}$(K) (cf. iii.) ; on écrit le résultat sous forme d'une matrice dont les coefficients sont de la forme a.I_n + M , (le a étant à chaque fois obtenu en effectuant le produit des matrices correspondantes et dont les coefficients sont les a_i. I_n) ; le résultat dans **Lin**(K) est la matrice "traduite" de celle obtenue en remplaçant chaque coefficient a. I_n + M (qui est un élément de $\mathbf{M_n}$(K)) par le coefficient a. I + M (qui est dans **Lin**(K)). La chose importante à vérifier est que le passage de "la liste des matrices à coefficients dans **Lin**(K)" à "la liste des matrices à coefficients dans $\mathbf{M_n}$(K) " est bien de classe $\mathcal{P}$. Cela revient à rajouter tout plein de 0 et de a_i ... mais on se convaincra sans difficulté que ça reste polynomialement majoré en taille.

v. On démontre le résultat pour K[X] et on raisonne comme au théorème C.a1 . Si [A_1,A_2,...,A_n] est une liste de matrices de **Mat**(K[X]) à multiplier, notons p_{ijk} le coefficient en position i,j de la matrice A_k et soit d_k le degré maxi des p_{ijk} pour k fixé. Alors dans le produit A_1.A_2.....A_n , le degré maxi d'un coefficient est d = d_1+d_2+...+d_n . Soit d' = d + 1 , on considère dans **Mat**($\mathbf{M_{d'}}$(K)) les matrices B_1, B_2, ..., B_n dont les coefficients b_{ijk} sont les matrices des applications linéaires " produit par p_{ijk} tronqué éventuellement au degré d' " . On effectue le produit des B_k puis on retraduit les coefficients du résultat dans K[X] . On vérifie que le passage de la liste [A_1,A_2,...,A_n] à la liste [B_1,B_2,...,B_n] est bien de classe $\mathcal{P}$, c.-à-d. ici essentiellement que c'est **RESP**. ❑

Exemples d'anneaux **Mat-c$\mathcal{P}$c**

Les $\mathcal{P}_{\mathbf{0'}}$-anneaux sont **Mat-c$\mathcal{P}$c** d'après le proposition B.g2. Il y a donc $\mathbb{Z}$, les anneaux d'entiers dans les corps de nombre, les anneaux finis, puis les anneaux de polynômes sur ces anneaux, et tous $\mathcal{P}$-quotients de ces derniers.

Aux $\mathcal{P}_{\mathbf{0'}}$-anneaux, nous pouvons ensuite rajouter tous ceux qu'on obtient en utilisant les

propriétés de stabilité énoncées en C.a2: notamment les localisés et corps de fractions qui ne peuvent être obtenus par B.g2.

Inversion de matrices

Définition C.a2 : On dira qu'un $\mathcal{P}$-anneau (commutatif ou non) K est **Inv-c$\mathcal{P}$c** lorsque les matrices carrées inversibles forment une $\mathcal{P}$-partie de **Mat**(K) , et que l'inversion des matrices carrées inversibles est une $\mathcal{P}$-fonction. On dira également : "**les matrices inversibles de Mat(K) sont $\mathcal{P}$-inversibles**" .

Remarque : On aura en particulier: les éléments inversibles de K forment une $\mathcal{P}$-partie de K , et le calcul de l'inverse d'un inversible est une $\mathcal{P}$-fonction.
De plus les matrices de **Trimat**(K) sont inversibles, et K est donc **Mat-c$\mathcal{P}$c**.

Proposition C.a3 : Soit K un anneau **Inv-c$\mathcal{P}$c** , alors sont également **Inv-c$\mathcal{P}$c** les anneaux suivants :

i. tout sous anneau de K qui est une partie $\mathcal{P}$-détachable de K
ii. l'anneau $\mathbf{M_n}$(K) des matrices carrées $n \times n$ à coefficients dans K
iii. **Lin**(K)
iv. $K[X_1,X_2,\ldots,X_n]$: lorsque K est commutatif et intègre
v. toute K-algèbre unitaire de dimension finie K' (c.-à-d.: K' est un K-module libre de dimension finie): lorsque K est commutatif, intègre et $\mathcal{P}$-divisible

preuve>

le i. est immédiat.
ii. et iii. se vérifient en inversant une matrice composée de blocs $n \times n$.
v. se déduit de ii. et i. comme à la proposition C.a2

Nous montrons iv. tout d'abord pour K[X] . Si B est la matrice inverse d'une matrice A à coefficients dans K[X] , nous pouvons majorer a priori le degré des coefficients de B par un entier d polynomialement relié à la taille de A , puisque B est (à un scalaire multiplicatif près) la matrice transposée des cofacteurs de A . Nous procédons alors comme pour la proposition C.a2: nous "remplaçons" chaque coefficient polynôme Q par la matrice de l'application linéaire "produit par Q éventuellement tronqué au degré d". Nous avons donc remplacé la matrice A à coefficients dans K[X] par une matrice formée de blocs $d' \times d'$ ($d' = d+1$) à coefficients dans K . Il nous reste à tester si la matrice obtenue est inversible dans **Mat**(K), et, si c'est le cas, à examiner les blocs $d' \times d'$ extraits de la matrice inverse pour vérifier s'ils sont de la forme voulue.
Pour $K[X_1,X_2,\ldots,X_n]$, nous pouvons procéder par récurrence sur n. ❑

Un résultat sur les anneaux commutatifs intègres $\mathcal{P}$-divisibles

Proposition C.a4 : Supposons K intègre $\mathcal{P}$-divisible et **Mat-c$\mathcal{P}$c** , soit L son corps de fractions (K est identifiable à une partie $\mathcal{P}$-détachable de L). Alors:

- La division euclidienne dans L[X] est une $\mathcal{P}$-fonction de $L[X] \times L[X]$ vers $(L[X] \times L[X]) \cup \{u\}$ (u pour le cas où on divise par 0) .
- Les anneaux K[X] et L[X] sont $\mathcal{P}$-divisibles .
- Les anneaux $K[X_1,X_2,\ldots,X_n]$ et $L[X_1,X_2,\ldots,X_n]$ sont $\mathcal{P}$-divisibles .

preuve> Soient 2 polynômes A et B , de degrés d et d + d' , avec d' ≥ 0 . Diviser A par B revient à exprimer linéairement A sur la base 1 , X , ... , X^{d-1} , B , B.X , ... , B.$X^{d'}$ (dans l'espace des polynômes de degré ≤ d + d') . Or cette base est triangulaire par rapport à la base canonique (sur laquelle est exprimé A), avec des coefficients tous non nuls sur la diagonale (1 ou le coefficient dominant de B). La matrice correspondante est donc $\mathfrak{P}$-inversible .
Le reste suit immédiatement. (la récurrence fonctionne grâce à la proposition précédente C.a2 v.) ❑

b) Cas commutatif : déterminants, formules de Cramer et inversions de matrices

$\mathfrak{P}$-calculabilité des déterminants

Définition C.b1 : On dira qu'un $\mathfrak{P}$-anneau commutatif K est **Det-c$\mathfrak{P}$c** lorsque la fonction "déterminant" , (définie sur la $\mathfrak{P}$-partie convenable de **Mat**(K)), est une $\mathfrak{P}$-fonction. On dira également : "**les déterminants sont $\mathfrak{P}$-calculables dans K**".

Définition C.b2 : On dira qu'un $\mathfrak{P}$-anneau commutatif K est **Inv-1-c$\mathfrak{P}$c** lorsque les matrices de déterminant égal à 1 forment une $\mathfrak{P}$-partie de **Mat**(K) , et que l'inversion des matrices carrées de déterminant égal à 1 est une $\mathfrak{P}$-fonction. On dira également : "**les matrices de Mat(K) de déterminant 1 sont $\mathfrak{P}$-inversibles**" .

Proposition C.b1 : Soit K un anneau commutatif **Det-c$\mathfrak{P}$c** , alors :

i K est également **Inv-1-c$\mathfrak{P}$c** et **Mat-c$\mathfrak{P}$c**

De plus sont alors également **Det-c$\mathfrak{P}$c** :

ii. tout sous anneau de K qui est une partie $\mathfrak{P}$-détachable de K

iii. tout $\mathfrak{P}$-quotient de K

iv. le localisé en S de K , si S est une partie multiplicative $\mathfrak{P}$-détachable de K ne contenant pas de diviseur de 0 .

preuve>

le i. se déduit des formules de Cramer et du théorème C.a1 ;

le ii. et le iii. sont immédiats

le iv. résulte du fait que la "réduction au même dénominateur" de tous les coefficients d'une matrice de **Mat**(K_S) est une $\mathfrak{P}$-opération. ❑

Le cas des $\mathfrak{P}$-$\mathbb{Q}$-algèbres : la méthode de Leverrier

Théorème C.b1 : Soit K une $\mathfrak{P}$-$\mathbb{Q}$-algèbre unitaire et commutative.

Alors les propriétés suivantes sont équivalentes:

i. le produit dans **Mat**(K) est c-$\mathfrak{P}$-c (c.-à-d. K est **Mat-c$\mathfrak{P}$c**)

ii. les déterminants sont $\mathfrak{P}$-calculables dans K

iii. l'inversion des matrices triangulaires supérieures avec des 1 sur

la diagonale est un $\mathcal{P}$-calcul

iv. les matrices de **Mat**(K) de déterminant 1 sont $\mathcal{P}$-inversibles

Lorsque les inversibles de K forment une $\mathcal{P}$-partie, sur laquelle le calcul de l'inverse est un $\mathcal{P}$-calcul, ces propriétés sont en outre équivalentes à la suivante:

v. les matrices inversibles de **Mat**(K) sont $\mathcal{P}$-inversibles

preuve>

i. et iii. sont équivalents d'après le théorème C.a1.

ii. implique iv. et v. par les formules de Cramer

iv. et v. impliquent séparément iii.

Il reste à voir que i. implique ii., c.-à-d. en gros à calculer un déterminant en n'utilisant que des produits de matrices: la **méthode de Leverrier**, dont le seul inconvénient est d'utiliser des divisions par des entiers, convient pour les $\mathbb{Q}$-algèbres. Soit A une matrice carrée $n \times n$ à coefficient dans K (supposé **Mat-c$\mathcal{P}$c**), soit $P(X) = X^n - (a_1.X^{n-1} + a_2.X^{n-2} + ... + a_n)$ son polynôme caractéristique, et soit S_i la "somme des puissances i-èmes des valeurs propres" (cela "a un sens" même si K n'est pas intègre: S_i est une fonction polynôme (à coefficients entiers) des a_j donnée par les formules de Newton).

Alors S_i est la trace de A^i (il s'agit d'une identité algébrique, et il suffit donc qu'elle soit vraie dans le cas d'un corps algébriquement clos). Le calcul $A \longrightarrow [S_1,S_2,... ,S_n]$ est donc un $\mathcal{P}$-calcul. Ensuite il reste à calculer les a_j par les formules de Newton, qui s'écrivent matriciellement:

$$\begin{vmatrix} 1 & 0 & 0 & \cdots & 0 \\ S_1 & 2 & 0 & \cdots & 0 \\ S_2 & S_1 & 3 & \cdots & 0 \\ S_3 & S_2 & S_1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \end{vmatrix} \begin{vmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ \vdots \end{vmatrix} = \begin{vmatrix} S_1 \\ S_2 \\ S_3 \\ S_4 \\ \vdots \end{vmatrix}$$

etc

Il s'agit donc de résoudre un système linéaire triangulaire dont les coefficients sont $\mathcal{P}$-donnés en fonction de $[S_1,S_2,... ,S_n]$.

En multipliant la i-ème ligne par 1/i, on est ramené à inverser une matrice de **Trimat**(K), puis à multiplier l'inverse obtenue par le vecteur colonne du second membre.

La multiplication par 1/i est un $\mathcal{P}$-calcul parce que K est une $\mathcal{P}$-$\mathbb{Q}$-algèbre. L'inversion dans **Trimat**(K) et le produit dans **Mat**(K) sont des $\mathcal{P}$-calculs parce que K est **Mat-c$\mathcal{P}$c**.

❑

Problème ouvert : Dans tout anneau commutatif **Mat-c$\mathcal{P}$c** les déterminants sont $\mathcal{P}$-calculables ?

Remarques :

1) tout $\mathcal{P}$-corps **Mat-c$\mathcal{P}$c** de caractéristique nulle est une $\mathcal{P}$-$\mathbb{Q}$-algèbre puisque $\mathbb{Q}$ est objet initial dans la catégorie (cf. B.c))

2) en combinant les théorèmes C.b1, C.b2 et les propriétés de stabilité pour le caractère **Det-c$\mathcal{P}$c** (cf. prop. C.b1, C.c5 et C.c6), on obtiendra un bon stock d'anneaux **Det-c$\mathcal{P}$c**.

3) la méthode de Leverrier est souvent présentée sous une forme améliorée dite **méthode de Faddev** :

$$\begin{array}{lll} A_1 = A & a_1 = tr(A_1) & B_1 = A_1 - a_1 I \\ A_2 = A B_1 & a_2 = tr(A_2) / 2 & B_2 = A_2 - a_2 I \\ A_3 = A B_2 & a_3 = tr(A_3) / 3 & B_3 = A_3 - a_3 I \\ \ldots\ldots\ldots & \ldots\ldots\ldots\ldots & \ldots\ldots\ldots \\ A_n = A B_{n-1} & a_n = tr(A_n) / n & B_n = A_n - a_n I = 0 \end{array}$$

Cette méthode peut être utilisée sous les mêmes hypothèses qui rendent la méthode de Leverrier en temps polynomial, en rajoutant toutefois une hypothèse de $\mathfrak{P}$-réductiblité. En effet, les a_i sont convenablement majorés en taille et on a l'égalité :

$$\begin{aligned} A_i &= A (A (\ldots A (A - a_1 I) - a_2 I)\ldots) - a_{i-1} I) \\ &= A^i - (a_1 A^{i-1} + a_2 A^{i-2} + \ldots + a_{i-1} A) \end{aligned}$$

Donc si on suit l'algorithme de Fadeev en réduisant chaque A_i et chaque a_i intermédiaires obtenus, la taille du calcul est convenablement maîtrisée.

4) la méthode de Fadeev s'applique également avec un anneau commutatif **Mat-c$\mathfrak{P}$c** $\mathfrak{P}$-réductible K où la division par un entier, quand elle est possible, est unique[21], et réalisée par une opération en temps polynomial.

La méthode de Samuelson

La méthode de Samuelson (cf. [**Sam**] ou [**Ber**]) est une méthode qui permet de calculer le polynôme caractéristique d'une matrice de manière récurrente.

Pour une matrice A à n lignes et n colonnes, on écrit :

$$A = \begin{array}{|c|c|} \hline a_{1,1} & R \\ \hline S & M \\ \hline \end{array}$$

Si $p(\lambda) = \sum_{i=0}^{n} p_{n-i}.\lambda^i = \det (A - \lambda)$ $(p_0 = (-1)^n)$ et

$$q(\lambda) = \sum_{i=0}^{n-1} q_{n-1-i}.\lambda^i = \det (M - \lambda.I) \quad (q_0 = (-1)^{n-1})$$

La matrice adjointe de $(A - \lambda.I)$ est donnée par

$$adj(A - \lambda.I) = - \sum_{k=2}^{n} (M^{k-2}.q_0 + M^{k-3}.q_1 + \ldots + I.q_{k-2}) \lambda^{n-k}$$

Et $p(\lambda)$ est donné par :

$$p(\lambda) = (a_{1,1} - \lambda)\, q(\lambda) + R \,.\, adj(A - \lambda.I) \,.\, S$$

On en déduit immédiatement la :

---

21 c.-à-d: K est sans torsion en tant que $\mathbb{Z}$-module

Proposition C.b2 : Soit K un anneau commutatif **Mat-c$\mathcal{P}$c** , $\mathcal{P}$-réductible où les coefficients du polynôme caractéristique sont polynomialement majorés en taille , alors K est **Det-c$\mathcal{P}$c**.

Si les déterminants sont $\mathcal{P}$-majorés, ils sont $\mathcal{P}$-calculables ?

Le résultat proposé ci-dessus en interrogation fait l'objet du:

Problème ouvert : Si K est un $\mathcal{P}$-anneau commutatif $\mathcal{P}$-réductible où les déterminants sont polynomialement majorés en taille, alors ils sont $\mathcal{P}$-calculables ?

Nous démontrerons le résultat dans trois cas particuliers: lorsque K est intègre et $\mathcal{P}$-divisible (cf. Th. C.d1, via la méthode de Bareiss), lorsque K est un anneau où la division par un entier, quand elle est possible, est unique, et réalisée par une opération en temps polynomial (Th. C.b3, via la méthode de Fadeev), et lorsque K est un anneau où les coefficients du polynôme caractéristique sont polynomialement majorés en taille (Th C.b2, via la méthode de Samuelson).

Proposition C.b3 : Soit K un $\mathcal{P}$-anneau commutatif $\mathcal{P}$-réductible où la fonction déterminant est **RESP** , alors K est **Mat-c$\mathcal{P}$c**.

preuve> Montrons tout d'abord que l'addition dans K est complètement $\mathcal{P}$-calculable:
Il suffit de montrer que l'addition itérée est **RESP**, or le déterminant de la matrice ci-dessous est égal à la somme a + b + c ... + k :

$$\begin{vmatrix} a & 1 & 1 & \cdots & 1 \\ -b & 1 & 0 & \cdots & 0 \\ -c & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ -k & 0 & 0 & \cdots & 1 \end{vmatrix}$$

Donc, l'addition itérée est **RESP** si on fait suivre chaque addition (dans une addition itérée) par une "réduction" du résultat (l'anneau est supposé $\mathcal{P}$-réductible).
On démontre de même que le produit dans K est c-$\mathcal{P}$-c en considérant le déterminant d'une matrice diagonale.
Voyons maintenant le produit matriciel. Tout d'abord le produit de 2 matrices est $\mathcal{P}$-calculable parce que l'addition est c-$\mathcal{P}$-c (prop. C.a1). Par ailleurs l'inversion dans **Trimat**(K) est **RESP** puisque la fonction déterminant est **RESP** . Le même raisonnement qui dans la preuve du Th C.a1, montrait que: " l'inversion dans **Trimat**(K) est $\mathcal{P}$ " implique " le produit dans **Mat**(K) est c-$\mathcal{P}$-c " ; ce même raisonnement montre maintenant que le produit dans **Mat**(K) est **RESP**. ❑

En combinant les propositions C.b2 et C.b3 on obtient immédiatement le :

Théorème C.b2 : Soit K un $\mathcal{P}$-anneau commutatif $\mathcal{P}$-réductible où les coefficients du polynôme caractéristique sont polynomialement majorés en taille, alors K est **Det-c$\mathcal{P}$c** (par la méthode de Samuelson).

Théorème C.b3 :

Soit K un $\mathfrak{P}$-anneau commutatif $\mathfrak{P}$-réductible où la division par un entier, quand elle est possible, est unique, et réalisée par une opération en temps polynomial . Supposons en outre que les déterminants sont polynomialement majorés en taille. Alors les déterminants sont $\mathfrak{P}$-calculables dans K (par la méthode de Fadeev).

preuve> On applique la proposition C.b3 et la remarque 4) qui suit le théorème C.b1. ❑

c) Systèmes linéaires à coefficients dans un $\mathfrak{P}$-corps commutatif

Dans ce § , K désignera un $\mathfrak{P}$-anneau commutatif intègre et $\mathfrak{P}$-divisible, et L son corps de fractions. Un cas particulier est celui où K est un $\mathfrak{P}$-corps, et L = K .

Dépendance linéaire, inversion de matrices, déterminants

Dans la définition qui suit, nous notons **Col**(K) la $\mathfrak{P}$-partie de **Mat**(K) formée des matrices à une seule colonne.

Définition C.c1 : On dira qu'un $\mathfrak{P}$-anneau commutatif intègre et $\mathfrak{P}$-divisible K est **Dep-c$\mathfrak{P}$c** lorsque les relations de dépendance linéaires entre vecteurs peuvent être $\mathfrak{P}$-calculées au sens suivant : il existe une $\mathfrak{P}$-opération D de **Mat**(K) vers **Col**(K) $\cup$ {u} vérifiant:

- si D(M) = u , les vecteurs colonnes de la matrice M sont linéairement indépendants
- si D(M) = V est un vecteur colonne, alors $V \neq 0$ et M.V = 0 : c.-à-d. que les coefficients de V définissent une relation de dépendance linéaire entre les vecteurs colonnes de la matrice M.

On dira encore "**la dépendance linéaire est $\mathfrak{P}$-calculable dans K**".

La morale de la proposition qui suit est essentiellement que tout calcul systématique d'inverses de matrices contient (de manière éventuellement cachée) un calcul de déterminants, et que ce fait s'étend aux calculs en temps polynomial.

Proposition C.c1 : Soient K et L comme précisés au début du § , alors les propriétés suivantes sont équivalentes :

i. K est **Det-c$\mathfrak{P}$c**
ii. K est **Dep-c$\mathfrak{P}$c**
j. L est **Det-c$\mathfrak{P}$c**
jj. L est **Dep-c$\mathfrak{P}$c**
jjj. L est **Inv-c$\mathfrak{P}$c**

preuve> i. et j. sont clairement équivalents (cf. prop. C.b1)
ii. et jj. de même (par les procédés de réduction au même dénominateur)
j. $\Rightarrow$ jjj. par les formules de Cramer

jjj. $\Rightarrow$ L est **Mat-c$\mathcal{P}$c** (cf. Th. C.a1)

jjj. $\Rightarrow$ jj. : dans la matrice M à h lignes et c colonnes , on cherche tout d'abord un coefficient non nul (h.c tests) , puis une matrice 2×2 extraite de M , contenant ce coefficient non nul , et inversible ((h-1).(c-1) tests) , puis, si on a trouvé, une matrice 3×3 extraite de M , contenant la matrice précédemment trouvée, et inversible ((h-2).(c-2) tests) . On continue jusqu'à constater l'indépendance linéaire des vecteurs colonnes , ou dans le cas contraire l'indépendance de $h' < h$ vecteurs colonnes et le fait que tout autre vecteur colonne dépend linéairement de ces h' qu'on a déterminés : dans ce cas, pour obtenir une relation de dépendance linéaire on utilise la dernière matrice inversible trouvée P (une matrice $h' \times h'$) , si W est un des vecteurs liés aux h' vecteurs en question , on extrait W' de W (en ne gardant que les coefficients des lignes intervenant dans P), et on calcule $W'.P^{-1}$. (les détails laissés au lecteur)

jj. $\Rightarrow$ jjj. immédiat , donc en particulier jj. $\Rightarrow$ L est **Mat-c$\mathcal{P}$c**.

jj. $\Rightarrow$ j. : on considère la matrice carrée dont on veut trouver le déterminant comme la matrice d'une application linéaire f de K^n vers K^n , on va $\mathcal{P}$-construire une base (en utilisant le fait que L est **Mat-c$\mathcal{P}$c**) f_1 , f_2 , ... , f_n , par rapport à laquelle l'expression de f sera particulièrement simple, et le déterminant immédiatement calculable. On commence par $f_1 = e_1$, de la base canonique, on continue avec $f(f_1) = f_2$, $f(f_2) = f_3$, ... tant que ces vecteurs sont indépendants. Supposons qu'on ait déjà construit jusqu'à f_j et que $f(f_j)$ soit dépendant des précédents . Alors on prendra pour f_{j+1} le premier vecteur de la base canonique indépendant de $f_1....f_j$, et on recommence à partir de là le même processus.
Les vecteurs de la base obtenue, sont tous (en tant que vecteurs colonnes) extraits des matrices A, A^2,...,A^n. Il est donc clair que la matrice de f sur cette base est donnée par un $\mathcal{P}$-calcul (vu l'hypothèse jj.), et son déterminant est égal au produit de quelques uns de ces éléments. (cf. exemple ci-dessous, où on a mis des "blocs" en évidence en les séparant par des blancs)

A =

. . . . a	. . . x	. x
1 . . . x	. . . x	. x
. 1 . . x	. . . x	. x
. . 1 . x	. . . x	. x
. . . 1 x	. . . x	. x
. . . . .	. . . b	. x
. . . . .	1 . . x	. x
. . . . .	. 1 . x	. x
. . . . .	. . 1 x	. x
. . . . .	. . . .	. c
. . . . .	. . . .	1 x

les points représentent des 0

les croix représentent des coefficients non précisés

det(A) = a.(-b).(-c)

Systèmes linéaires à coefficients dans un $\mathcal{P}$-corps commutatif

Un système de c équations linéaires à h inconnues dans L est donné par :

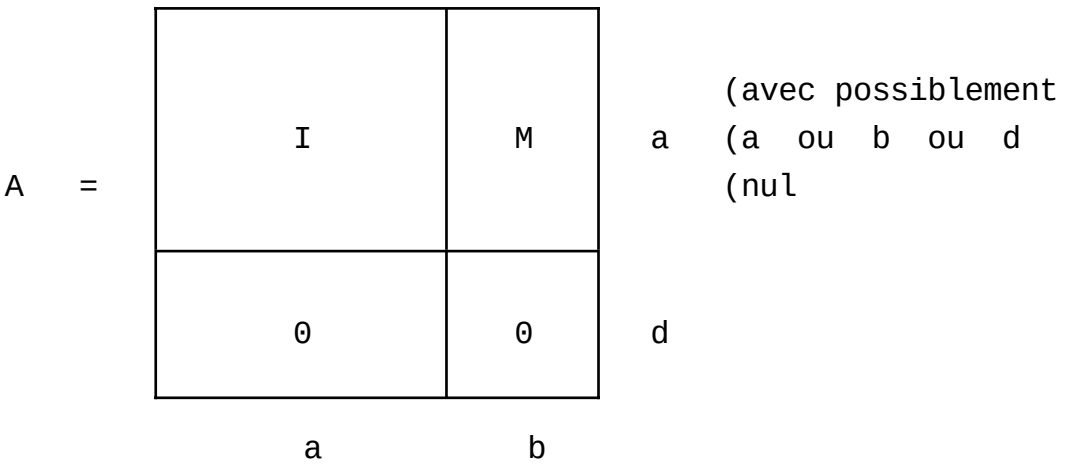
- une matrice $A = (a_{ij})$ de L^{hxc} **Mat**(L)
- un vecteur colonne $V = (b_i)$ de L^h **Col**(L)

Le système d'équations ainsi représenté est, pour i de 1 à h : $\Sigma_j \; a_{ij}. x_j = b_i$

Le système d'équations est équivalent à l'équation matricielle $A.X = V$.

Les systèmes d'équations linéaires sur L forment un $\mathcal{P}$-ensemble, que nous noterons **Syslin**(L).

Un système linéaire sur L est dit **trivial** si la matrice A est de la forme:



De manière générale, lorsque L est un corps discret, on sait que tout système linéaire sur L est équivalent à un système trivial, à une permutation des inconnues près; résultat qu'on peut obtenir par la méthode du pivot de Gauss.

Un **système linéaire résolu** sur L est donné par :

- un système linéaire trivial sur L : (T , W)
- l'indication de la permutation des colonnes à effectuer: par exemple sous la forme d'une matrice de permutation P.

Au système linéaire résolu sur (T , W , P) correspond le système linéaire (T.P , W) . L'ensemble des systèmes linéaires résolu sur L est un $\mathcal{P}$-ensemble.

Lorsqu'un système linéaire sur L est sous forme résolue, il est immédiat de déterminer s'il est impossible, s'il a une solution unique, ou si on peut choisir arbitrairement un certain nombre d'inconnues, et d'exprimer les autres en fonction de celles choisies.

Définition C.c2 : On dira que les systèmes linéaires sont $\mathcal{P}$-résolubles dans L s'il existe une $\mathcal{P}$-opération qui transforme tout système linéaire en un système linéaire résolu équivalent.

Proposition C.c2 : Pour tout $\mathcal{P}$-corps commutatif L , les propriétés suivantes sont équivalentes:

- les systèmes linéaires sont $\mathcal{P}$-résolubles dans L
- la dépendance linéaire est $\mathcal{P}$-calculable dans L
- les déterminants sont $\mathcal{P}$-calculables dans L
- les matrices inversibles sont $\mathcal{P}$-inversibles dans L

preuve> vu la prop. C.c1 les 3 dernières propriétés sont équivalentes.
Si L est **Dep-c$\mathcal{P}$c**, et si on veut résoudre un système linéaire (A , V) , on considère les vecteurs colonnes de la matrice A , on en extrait un système libre maximal. Si V est linéairement indépendant de ce système libre, le système linéaire de départ est impossible. Dans le cas contraire, les variables correspondant aux vecteurs colonnes ne faisant pas partie du système libre maximal choisi peuvent être choisies librement. Et il est immédiat de déterminer le "système linéaire résolu" équivalent au système de départ à partir de l'expression des vecteurs colonnes considérés en fonction des vecteurs du système libre maximal.
Si maintenant les systèmes linéaires sont $\mathcal{P}$-résolubles dans L, il est immédiat que L est **Dep-c$\mathcal{P}$c** : l'indépendance linéaire de k vecteurs revient à l'impossibilité d'exprimer linéairement chaque vecteur en fonction des précédents, c.-à-d. à l'impossibilité pour k systèmes linéaires etc ... ❑

Géométrie des sous-espaces

On considère maintenant le calcul "géométrique" dans **Sv**(L) , **Fsv**(L) .

Proposition C.c3 : Soit L un $\mathcal{P}$-corps commutatif **Det-c$\mathcal{P}$c**.

i. L'égalité dans **Sv**(L) et **Fsv**(L) est $\mathcal{P}$-décidable. Et il y a une $\mathcal{P}$-opération qui associe à tout élément de **Sv**(L) ou de **Fsv**(L) une base de cet espace.
ii. La somme et l'intersection sont complètement $\mathcal{P}$-calculables dans **Sv**(L) et **Fsv**(L)
iii. La fonction $f \longrightarrow Im(f)$ de **Mat**(L) vers **Fsv**(L) est $\mathcal{P}$-calculable
iv. La fonction $f \longrightarrow Ker(f)$ de **Mat**(L) vers **Fsv**(L) est $\mathcal{P}$-calculable

preuve> le i. est laissé au lecteur; le iii. est trivial; que la somme de sous-espaces soit complètement $\mathcal{P}$-calculable est
également trivial; pour l'intersection nous utiliserons un peu de dualité:

Lemme:

La fonction : E $\longrightarrow$ orthogonal de E
(sous-espace de K^h) (dans le dual de K^h identifié à K^h)
de **Fsv**(L) vers **Fsv**(L) est une $\mathcal{P}$-fonction.

Il est clair que ce lemme implique que l'intersection est complètement $\mathcal{P}$-calculable dans **Fsv**(L) , d'où ensuite dans **Sv**(L).
Par ailleurs le lemme est équivalent à l'affirmation que la fonction Ker de **Mat**(L) vers **Fsv**(L) est une $\mathcal{P}$-fonction. Mais calculer le noyau d'une application linéaire f de matrice A n'est rien d'autre que résoudre le système linéaire A.X = 0 (détails laissés au lecteur). ❑

Calculs dans les anneaux de polynômes

Proposition C.c4 : Soit L un $\mathcal{P}$-corps commutatif **Det-c$\mathcal{P}$c**. Alors:

– L'interpolation est une $\mathcal{P}$-fonction de **Lst**(L $\times$ L) vers L[X] .
– La relation de Bezout dans L[X] est $\mathcal{P}$-calculable.

preuve> L'interpolation est la fonction qui associe à une liste de couples (x_0,y_0), (x_1,y_1), ... , (x_d,y_d) (avec les x_i 2 à 2 distincts) l'unique polynôme P de L[X] qui vérifie $deg(P) \leq d$ et $P(x_i) = y_i$ pour i de 0 à d . Il s'agit en fait de résoudre un système d'équations linéaires dont les coefficients sont les x_{ij} (pour i et j de 0 à d), avec les y_i au second membre. C'est donc une $\mathcal{P}$-fonction.

Pour ce qui concerne la relation de Bezout dans L[X] , il s'agit encore de résolution de systèmes linéaires : cf. par exemple [**ALFA**] p 211-216. ❑

Stabilité **Det-c$\mathcal{P}$c** pour des anneaux de polynômes

Proposition C.c5 : Soit L un $\mathcal{P}$-corps commutatif **Det-c$\mathcal{P}$c**, corps des fractions de K , $\mathcal{P}$-divisible. Supposons de plus L $\mathcal{P}$-infini, (c.-à-d. : il existe une $\mathcal{P}$-fonction injective de $\mathbb{N}_1$ vers L).
Alors les déterminants sont $\mathcal{P}$-calculables par interpolation dans $K[X_1, X_2,... ,X_n]$ et $L[X_1,X_2,... ,X_n]$.

preuve> Voyons que K[X] est **Det-c$\mathcal{P}$c** . Cela permettra de conclure pour $K[X_1,X_2,...,X_n]$ par récurrence : on rappelle que $K[X_1,X_2,...,X_n]$ est $\mathcal{P}$-divisible (prop. C.a4)).

Comme K[X] est une partie $\mathfrak{P}$-détachable de L[X] , il suffit de traiter ce dernier cas.
Pour calculer le déterminant d'une matrice à coefficients dans L[X] , on donne une majoration d de son degré (par ex la somme des sup des degrés dans chaque colonne) puis on calcule le polynôme par interpolation en d + 1 points distincts, d'où la nécessité, pour rester dans la classe des $\mathfrak{P}$-calculs, de disposer d'une $\mathfrak{P}$-fonction injective $\mathbb{N}_1$ vers L . Pour calculer la valeur du polynôme "déterminant" en l'un de ces d + 1 points, il faut évaluer chaque coefficient de la matrice en ce point, puis calculer dans L le déterminant de la matrice obtenue. Tout ceci reste un $\mathfrak{P}$-calcul. ❑

Remarques:

1) Si L est un corps fini, on peut voir que les déterminants sont $\mathfrak{P}$-calculables dans $L[X_1,X_2,...,X_n]$ de différentes manières possibles:
– si $L = \mathbf{F_p}$, p premier, L[X] est un $\mathfrak{P}$-quotient de $\mathbb{Z}[X]$. Or $\mathbb{Z}[X]$ est **Det-c$\mathfrak{P}$c** (par l'argument précédent, ou bien par le Th C.b1 appliqué à $\mathbb{Q}[X]$, ou bien par la proposition C.b2).
– dans le cas général, on peut appliquer un argument du même type, en remplaçant $\mathbb{Z}$ par une extension finie . Le plus simple est d'invoquer la proposition C.b2 ou le Th C.d1 à venir.

2) Tout $\mathfrak{P}$-corps commutatif L qui est **Det-c$\mathfrak{P}$c** et de caractéristique nulle est $\mathfrak{P}$-infini, et les calculs de polynômes par interpolation peuvent être faits pour des x entiers: en effet l'homomorphisme canonique $\mathbb{Z} \to L$ est une $\mathfrak{P}$-fonction puisque L est **Mat-c$\mathfrak{P}$c** et que $\mathbb{Z}$ est initial parmi les anneaux où addition et produit sont c-$\mathfrak{P}$-c.

Stabilité **Det-c$\mathfrak{P}$c** pour les extensions finies

Proposition C.c6 : Soit L un $\mathfrak{P}$-corps commutatif **Det-c$\mathfrak{P}$c**.
Soit L' une algèbre de dimension finie n sur L qui est de plus un corps, commutatif ou non. Alors L' est **Inv-c$\mathfrak{P}$c** (pour sa présentation comme L-espace vectoriel de dimension finie n). Si L' est commutatif, il est **Det-c$\mathfrak{P}$c**

preuve> Le corps L' est $\mathfrak{P}$-isomorphe à une sous-L-algèbre $\mathfrak{P}$-détachable de $\mathbf{M_n}(L)$ (cf. la preuve de la proposition C.a2 viii). Il suffit donc d'appliquer la proposition C.a3.❑

d) Evolution des coefficients dans la méthode du pivot (méthode de Bareiss)

Nous en venons à l'analyse concrète de la méthode du pivot.

Nous sommes intéressés par un critère permettant d'assurer que la méthode du pivot, économique en nombre d'opérations arithmétiques élémentaires (nettement plus efficace de ce point de vue que la méthode de Leverrier utilisée au Th C.b1) ne conduit pas à une explosion des coefficients.

L'analyse que nous faisons de la méthode du pivot est essentiellement la même que celle de Gantmacher dans [**Gan**] chapitre 2 . Nous en déduisons une présentation "pédagogique" de la méthode dite de Bareiss (cf. [**Bar**]). Il s'avère que la méthode de Bareiss était peut-être connue de Sylvester et sûrement de Aitken (cf. [**Ait**]).

Nous obtenons essentiellement la même condition suffisante pour la $\mathfrak{P}$-calculabilité des déterminants dans un $\mathfrak{P}$-anneau K, qu'au Théorème C.b2 .

Nous avons besoin dans les 2 cas de supposer la $\mathfrak{P}$-réductibilité de K et la $\mathfrak{P}$-majoration des déterminants en taille.
Alors que le Th C.b1 s'applique à toutes les $\mathfrak{P}$-$\mathbb{Q}$-algèbres, la méthode du pivot ne s'applique qu'avec des anneaux intègres (mais sans hypothèse de caractéristique nulle).
D'autre part la méthode "améliorée" à la Bareiss (qui est nécessaire pour éviter l'explosion de la taille des coefficients), exige en plus que l'anneau soit $\mathfrak{P}$-divisible.
En un sens, il est d'ailleurs peu surprenant qu'un gain dans la vitesse du calcul soit compensé par des hypothèses renforcées sur l'anneau K et la $\mathfrak{P}$-calculabilité dans l'anneau K.

L'exemple de $\mathbb{Z}$: résolution (dans $\mathbb{Q}$) d'un système linéaire à coefficients dans $\mathbb{Z}$

Un système linéaire de Nlin équations à Ncol inconnues peut être considéré comme donné par une matrice C (de type Nlin $\times$ Ncol) et un vecteur colonne "second membre" B (à Nlin coefficients).

On peut désirer traiter plusieurs seconds membres simultanément, de sorte que B serait une matrice avec Nsm colonnes (par exemple, si C est une matrice carrée, on peut prendre pour B la matrice carrée I, ce qui conduit directement au calcul de l'inverse de C).
L'inconnue est alors une matrice X de type Ncol $\times$ Nsm pour laquelle on demande que soit réalisée l'égalité C.X = B .

Présentation des coefficients:

Les coefficients sont des nombres rationnels. Décidons de représenter les systèmes linéaires successifs avec un dénominateur fixé dans chaque ligne.

Nous utiliserons pour cela une seule matrice A , à coefficients entiers, avec Nlin lignes et 1+Ncol+Nsm colonnes numérotées de 0 à Ncol+Nsm: dans la colonne 0 nous mettrons le dénominateur commun à la ligne correspondante.

Un exemple pour voir :

Nous allons voir maintenant sur un exemple "comment les choses se passent". Cet exemple a été choisi "au hasard", et aucune permutation de lignes ou de colonnes n'intervient. Au départ, les coefficients sont entiers, c.-à-d. que dans la colonne "dénominateurs" il n'y a que des 1.

DEPART

dénominateurs	matrice 5 x 5					second membre
1	9	7	8	5	6	4
1	12	3	56	84	75	10
1	35	62	14	18	23	11
1	20	3	6	5	4	7
1	51	23	51	42	2	57

après le 1er pivot

1	9	7	8	5	6	4
9	0	-57	408	696	603	42
9	0	313	-154	-13	-3	-41
9	0	-113	-106	-55	-84	-17
9	0	-150	51	123	-288	309

On a donc, normalement, des dénominateurs égaux à 9 sur les lignes 2, 3, 4, 5. On s'attend a priori à obtenir, après le 2ème pivot, des dénominateurs égaux à 9×57 ; mais on a l'agréable surprise de voir que tous les numérateurs (par exemple 57×154 - 313×408) sont multiples de 9, et le dénominateur 57 suffit pour les lignes 3, 4, 5 :

après le 2ème pivot

1	9	7	8	5	6	4
9	0	-57	408	696	603	42
-57	0	0	-13214	-24123	-20952	-1201
-57	0	0	5794	9087	8103	635
-57	0	0	6477	10821	11874	-1257

On s'attend a priori à obtenir, après le 3ème pivot, des dénominateurs égaux à 57×13214; mais on a l'agréable surprise de voir que tous les numérateurs (par exemple 13214×9087 - 24123×5794) sont multiples de 57, et le dénominateur 13214 suffit pour les lignes 4, 5 .

De même après le 4ème pivot, tous les numérateurs de la 5ème ligne seront multiples de 13214, et le dénominateur 345492 suffira :

après le 3ème pivot

1	9	7	8	5	6	4
9	0	-57	408	696	603	42
-57	0	0	-13214	-24123	-20952	-1201
-13214	0	0	0	-345492	-251278	25128
-13214	0	0	0	-232561	371876	-427875

après le 4ème pivot

1	9	7	8	5	6	4
9	0	-57	408	696	603	42
-57	0	0	-13214	-24123	-20952	-1201
-13214	0	0	0	-345492	-251278	25128
-345492	0	0	0	0	14145425	-11629422

Nous allons maintenant expliquer l'origine de ces simplifications automatiques.

Nous supposons tout d'abord que les pivots qui se présentent successivement en position (k,k) sont tous non nuls.

Nous notons $a_{k,ij}$ le coefficient rationnel dans la matrice C_k transformée de la matrice C après le $k^{ème}$ pivot.

Pour i et j > k , nous notons $C_{k,ij}$ la matrice extraite de la matrice C_k sur les lignes 1,2,...,k,i et sur les colonnes 1,2,...,k,j.

La matrice $C_{k,ij}$ est une matrice surtriangulaire, son déterminant est égal au produit de ses éléments diagonaux. Mais le produit des k premiers éléments sur la diagonale est aussi le déterminant de la matrice $C_{k-1,kk}$, et on obtient l'égalité : $a_{k,ij}.\det(C_{k-1,kk}) = \det(C_{k,ij})$.

Maintenant nous remarquons que les matrices $C_{k-1,kk}$ et $C_{k,ij}$ sont obtenues à partir des matrices correspondantes extraites de la matrice de départ C au moyen d'une succession de transformation élémentaires qui ne modifient pas les déterminants.

Ainsi $d_k = \det(C_{k-1,kk})$ est un entier, déterminant de la matrice extraite de C sur les lignes 1,2,...,k et sur les colonnes 1,2,...,k , et pourra servir de dénominateur commun pour les lignes k+1,...,Nlin de la matrice C_k.

Nous pouvons donc organiser le traitement algorithmique de manière à donner d_k pour dénominateur commun aux coefficients des lignes k+1,..., Nlin de la matrice C_k comme suit:

Module de traitement du pivot n° Npiv

Description des variables utilisées

```
matrices d'entiers
A        :    matrice contenant les coefficients des systèmes linéaires
              successifs. Les seconds membres sont stockés dans les
              colonnes  Ncol+1 à Ncol+Nsm.  Dans la colonne  0  on met le
              dénominateur commun à la ligne concernée. Le nombre de
              colonnes effectivement utilisées dans la matrice A est
              Ncol+Nsm+1.

compteurs
Npiv     :    numéro du pivot
Nlin     :    nombre de lignes effectivement utilisées dans  A c.-à-d.
              nombre d'équations du système linéaire
Ncol     :    nombre d'inconnues du système linéaire
Nsm      :    nombre de colonnes dans le second membre
I        :    indices pour les lignes dans les boucles
J        :    indices pour les colonnes dans les boucles

entiers
Piv      :    numérateur du pivot
Coef     :    coefficient en situation  I, Npiv  (avant traitement)
Denm     :    dénominateur du pivot
MODULE  TRAITERPIVOT
        annulation des coefficients en dessous du pivot par
        manipulations élémentaires de lignes
               Variables
              entrées      : Nlin, Ncol, Nsm
              itératives   : A, Npiv
              locales      : I, J, Piv, Coef, Denm
Début
Piv ⟵ A(Npiv,Npiv) ;
Pour  I  de  Npiv + 1  à  Nlin  faire
   Début
   Coef ⟵  A(I,Npiv) ;  Denm   ⟵ A(Npiv,0) ;
   A(I,Npiv) ⟵ 0      ;  A(I,0) ⟵ Piv ;
   Pour  J  de  Npiv + 1  à  Ncol+Nsm  faire
       A(I,J)  ⟵  (Piv × A(I,J) - Coef × A(Npiv,J))/Denm ;
   fin ;
Npiv ⟵ Npiv+1
fin
```

L'exemple que nous avons donné "pour voir" a été traité par l'algorithme ci-dessus. On avait $d_1 = 9$, $d_2 = -57$, $d_3 = -13124$, $d_4 = -345492$, $d_5 = 14145425$ qui est le déterminant de la matrice de départ.

A chaque étape, on a effectué les simplifications automatiques (la division par Denm dans l'algorithme, qui donne toujours un résultat entier) sans se préoccuper des simplifications éventuellement plus poussées dues "au hasard" (par exemple toutes les fractions de la 4ème ligne après le 3ème pivot auraient pu être simplifiées par 2).

L'algorithme est correct (si Piv est non nul) parce qu'il augmente Npiv de 1 tout en conservant l'affirmation suivante vraie: "les lignes Npiv, Npiv+1, ..., Nlin sont écrites avec pour dénominateur commun d_k , où k = Npiv-1". (en convenant que $d_0 = 1$). Ainsi les divisions par Denm donnent bien à chaque fois un résultat entier.

Nous remarquons également que l'algorithme ne fait aucune différence entre la partie "1er membre C" et la partie "2ème membre B" de la matrice A ; les arguments concernant l'existence de simplifications automatiques s'appliquent donc aussi bien au second membre.

Insistons sur le fait que le traitement des coefficients successifs "avec divisions automatiques" fournit en position i , j , après traitement du kème pivot, (où k < i et k < j) le coefficient $\det(C_{k,ij})$ extrait de la matrice de départ (et il y a, en colonne "dénominateurs", en position i , 0 le déterminant $\det(C_{k-1,kk})$); c.-à-d. que tous les coefficients qui apparaissent sont des déterminants extraits de la matrice de départ.

On peut remarquer enfin que $\det(C_{k-1,kk})$ n'avait pas besoin en fait d'être stocké en colonne 0 puisqu'il est déjà en position k-1,k-1 .

De l'influence éventuelle des permutations de lignes et colonnes:

Nous avons raisonné jusqu'à présent en supposant que les pivots successifs qui se présentent sur la diagonale sont non nuls. Nous allons voir maintenant ce qui se passe lorsqu'on est obligé de permuter des lignes ou/et des colonnes pour ramener un pivot non nul en position convenable.

Nous supposons Nlin, Ncol, Nsm donnés et nous notons PivLin(A,Npiv) la transformation subie par A et Npiv lorsqu'on exécute le module TRAITERPIVOT . Nous notons EchLin(A,i_1,i_2) la transformation sur la matrice A consistant à échanger les lignes i_1 et i_2 , et EchCol(A,j_1,j_2) la transformation sur la matrice A consistant à échanger les colonnes j_1 et j_2.

On constate sans difficulté que: si i_1 et i_2 sont > Np alors les transformations PivLin(A,Np) et EchLin(A, i_1, i_2) commutent entre elles. De même: si j_1 et j_2 sont > Np alors les transformations PivLin(A,Np) et EchCol (A, j_1, j_2) commutent entre elles.

Or, lorsqu'on déplace un pivot non nul pour l'amener dans la position Npiv , Npiv les transformations PivLin déjà effectuées l'ont été avec des numéros de pivot Np < Npiv, et le pivot déplacé est en situation i_2 , j_2 avec i_2 et $j_2 \geq$ Npiv .

Ainsi, du point de vue des transformations subies par A, toutes les transformations EchLin et EchCol auraient pu avoir été effectuées avant les transformations PivLin , de manière à trouver systématiquement des pivots non nuls en bonne position sur la diagonale. Ceci montre que l'algorithme de triangulation par la méthode du pivot, avec le module TRAITERPIVOT décrit précédemment, est correct (les divisions par Denm sont toujours des divisions exactes en entiers), même si on effectue des échanges de lignes et/ou des échanges de colonnes entre les transformations PivLin successives, à condition que les échanges portent sur des lignes (ou colonnes) de numéros strictement supérieurs à ceux des pivots déjà traités.

De plus, le coefficient en position i , j , après traitement du $k^{ème}$ pivot, (où $k < i$ et $k < j$), est égal, au signe près, à un déterminant extrait de la matrice de départ, à savoir le déterminant extrait sur les lignes (resp. colonnes) du départ qui, après les échanges de lignes (resp. colonnes), se retrouvent (juste après le traitement du $k^{ème}$ pivot) en positions 1, 2, ..., k, i (resp. 1, 2, ..., k, j); le signe étant donné par la somme des parités des permutations subies. (même remarque pour la colonne "dénominateurs")

Signalons pour terminer que la colonne 0 où nous avons placé les dénominateurs s'avère en fait superflue puisque les dénominateurs successifs sont 1 puis les coefficients diagonaux de la matrice A transformée: dans TRAITERPIVOT, on peut remplacer l'affectation Denm ⟵ A(Npiv,0) par Denm ⟵ A(Npiv-1,Npiv-1) (sauf Denm ⟵ 1 pour Npiv = 1).

Résolution du système triangulé; de nouvelles simplifications automatiques:

Discutons tout d'abord, pour simplifier, le cas où la matrice C de départ est de rang Nlin.

Nous commençons par "oublier" la colonne 0 de notre matrice A: dans la mesure où nous nous préoccupons seulement de résoudre le système linéaire, peu importe si nous multiplions les coefficients d'une ligne par leur dénominateur commun.

Si nous avions à résoudre dans $\mathbb{Q}$ un système triangulaire "arbitraire" à coefficients entiers, de la forme:

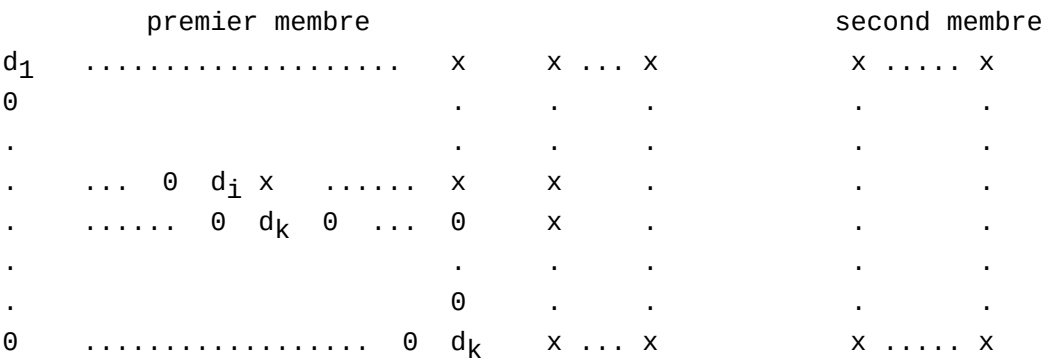
premier membre									second membre
d_1	x	.....		x		x ... x			x x
0	d_2	x	.....	x		x ... x			x x
.	0			.		.			. .
.	.			.		.			. .
.	.			x		.			. .
0	0	.....	0	d_k		x ... x			x x

nous serions obligés de prévoir pour les solutions des dénominateurs égaux à d_k, $d_k d_{k-1}$, ... , $d_k d_{k-1} ... d_1$ sur les lignes k, k-1, ... ,1.

Mais le système triangulaire auquel nous avons affaire n'est pas n'importe quel système triangulaire. Nous pouvons profiter du fait que nous savons que les solutions de notre système triangulé peuvent être mises sous forme de quotient de déterminants entiers (des déterminants extraits de la matrice de départ C), le dénominateur étant justement égal, au signe près, au coefficient d_k.

Nous résolvons donc le système par substitution, en partant de la dernière ligne et en remontant, (ce qui revient à faire subir à A quelques manipulations élémentaires de lignes pour remplacer la partie triangulaire par une partie diagonale), en sachant qu'en fin de compte on pourra se ramener à des d_k sur la diagonale avec une matrice à coefficients tous entiers.

Ainsi, si, avant le traitement de la $i^{ème}$ ligne, notre système a la forme:



nous aurions a priori, après traitement, un $d_i\ d_k$ sur la diagonale pour pouvoir conserver tous les coefficients de la $i^{ème}$ ligne entiers, mais nous savons que d_k suffira, et donc tous les coefficients calculés en ligne i seront sûrement multiples de d_i.

Ceci nous conduit donc au module suivant pour résoudre le système triangulé:

Module de résolution du système triangulé

Description des variables utilisées

```
matrice d'entiers
A   : matrice contenant les coefficients des systèmes linéaires successifs.

compteurs
Ncol : nombre d'inconnues du système linéaire
Nsm  : nombre de colonnes dans le second membre
I,I1 : indices pour les lignes dans les boucles
J    : indices pour les colonnes dans les boucles
Rang : rang de la matrice du premier membre

entiers
Di   : Ième élément sur la diagaonale (avant traitement)
Det  : déterminant de la matrice carrée extraite de rang  Rang
Asom : variable pour calculer une somme itérée
```

```
MODULE  TRIANGSOL
        la matrice est ramenée à une forme complètement résolue ,
        c.-à-d. diagonale pour les inconnues principales. La diagonale
        est remplie de Det et tous les coefficient sont entiers.
              Variables
             entrées      : Ncol, Nsm, Rang, Det
             itératives   : A
             locales      : I, I1, J, Di, Asom
Début
Pour  I  de  Rang-1  à  1  en descendant  faire
   Début
   Di ⟵ A(I,I) ; A(I,I) ⟵ Det ;
   Pour  J  de  Rang+1  à  Ncol+Nsm  faire
       Début
       Asom  ⟵  A(I,J) × Det  ;
       Pour  I1  de  I+1  à  Rang  faire
                                  Asom ⟵ Asom-A(I1,J) × A(I,I1);
       A(I,J) ⟵ Asom/Di ;
       fin;
   Pour  I1 de  I+1  à  Rang  faire  A(I,I1) ⟵ 0 ;
   fin
fin
```

On pourra remarquer que si le système est de rang strictement inférieur à Nlin, le module TRIANGSOL le transforme également en un système équivalent dont les coefficients restent entiers, puisque l'on ne tient pas compte des lignes Rang+1 ... Nlin.

On notera enfin que tous les coefficients calculés pendant l'exécution de TRIANGSOL sont, encore une fois, égaux, au signe près, à des déterminants extraits de la matrice de départ, puisque la solution théorique donne des quotients de 2 déterminants dont le $2^{ème}$ est égal, au signe près, au coefficient sur la diagonale, qui sert justement de dénominateur.

La méthode du pivot améliorée (à la Bareiss)

La méthode du pivot décrite ci-dessus dans $\mathbb{Z}$ est "améliorée" en ce sens que même si nous n'avions pas de $\mathcal{P}$-calcul de la réduite d'une fraction dans $\mathbb{Q}$, nous pourrions la pratiquer sans explosion de la taille des coefficients, alors que la méthode du pivot "ordinaire", directement dans $\mathbb{Q}$, et sans réduction systématique des fractions obtenues, conduirait, elle, à une explosion de la taille des coefficients.

Ici, nous n'avons pas pratiqué une réduction systématique de toutes les fractions obtenues, mais nous avons pratiqué toutes les réductions "automatiques" possibles (ce qui réclame seulement que la division exacte soit un $\mathcal{P}$-calcul dans $\mathbb{Z}$). Et cela a suffi pour éviter l'explosion des coefficients. Or il est en général bien plus facile d'avoir une division exacte en temps polynomial dans un anneau intègre, plutôt que le calcul en temps polynomial d'une forme réduite (presque) canonique pour les fractions dans le corps des fractions: le passage de l'anneau intègre à son corps des fractions ne conserve pas a priori le caractère $\mathcal{P}$-dénombrable ou $\mathcal{P}$-réductible.

Nous donnons maintenant une description précise de la méthode du pivot améliorée pour la résolution d'un système d'équations linéaires à coefficients dans K et inconnues dans L, lorsque K est un $\mathcal{P}$-anneau intègre, $\mathcal{P}$-divisible et $\mathcal{P}$-réductible.

Description détaillée de la méthode

Nous explicitons le caractère $\mathcal{P}$-réductible de K par la donnée d'une $\mathcal{P}$-opération $\mathrm{Red} : K \longrightarrow K$, avec $x =_K \mathrm{Red}(x)$ pour $x \in K$.

Nous procédons alors comme suit:

- D'abord on triangule au moyen du module TRAITERPIVOT, avec les précisions suivantes:

* Avant le traitement du $(k+1)^{ème}$ pivot, on cherche un coefficient non nul dans la partie utile restante de la matrice (c'est un $\mathcal{P}$-calcul parce que le test d'égalité à 0 est $\mathcal{P}$. Puis on peut opérer à loisir une permutation quelconque sur les lignes de numéro > k , et pareil pour les colonnes, notamment dans le but de ramener en position k+1 , k+1 un coefficient non nul qui va servir de pivot. (il est recommandé de garder en mémoire la permutation subie par les lignes (resp. colonnes) depuis le départ.

* Dans TRAITERPIVOT lui-même, on remplace l'affectation:

$$\mathtt{A(I,J)} \leftarrow \mathtt{(\ Piv} \times \mathtt{A(I,J)} - \mathtt{Coef} \times \mathtt{A(Npiv,J)\ )/Denm}\ ,$$

par l'affectation:

$$\mathtt{A(I,J)} \leftarrow \mathtt{Red(\ (\ Piv} \times \mathtt{A(I,J)} - \mathtt{Coef} \times \mathtt{A(Npiv,J)\ )/Denm\ )}$$

- Après avoir triangulé jusqu'à épuisement des pivots non nuls, on exécute TRIANGSOL avec les précisions suivantes: on remplace l'affectation:

$$\mathtt{Asom} \leftarrow \mathtt{Asom\ -\ A(I1,J)} \times \mathtt{A(I,I1)}\ ,$$

par l'affectation: $\mathtt{Asom} \leftarrow \mathtt{Red(\ Asom\ -\ A(I1,J)} \times \mathtt{A(I,I1)\ )}$;

et l'affectation: $\mathtt{A(I,J)} \leftarrow \mathtt{Asom/Di}\ ,$

par l'affectation: $\mathtt{A(I,J)} \leftarrow \mathtt{Red(Asom/Di)}$

Le Théorème concernant la méthode de Bareiss

Théorème C.d1 :

Lorsqu'on traite un système d'équations linéaires par la méthode du pivot améliorée, tous les coefficients qui sont calculés sont égaux, au signe près, à des déterminants extraits de la matrice de départ.

Supposons que K soit un $\mathcal{P}$-anneau intègre, $\mathcal{P}$-divisible et $\mathcal{P}$-réductible, et soit L son corps de fractions . Alors la résolution dans le $\mathcal{P}$-corps L d'un système linéaire à coefficients dans K par la méthode du pivot améliorée est un $\mathcal{P}$-calcul si et seulement si la fonction "déterminant" est **RESP** dans K , c.-à-d. ssi les déterminants sont polynomialement majorés en taille.

En particulier le calcul du déterminant (et de l'inverse) d'une matrice par la méthode du pivot améliorée est un $\mathcal{P}$-calcul si et seulement si les déterminants sont polynomialement majorés en taille.

Remarques:

1) lorsque K est $\mathcal{P}$-réductible (en particulier s'il est $\mathcal{P}$-dénombrable) nous pouvons donc rajouter une nouvelle propriété équivalente à celles énoncées à la proposition C.c2 : les déterminants sont polynomialement majorés en taille.

2) on se reportera au § B.g pour obtenir un bon stock d'anneaux où la fonction déterminant est **RESP**

3) pour un système linéaire à coefficients dans L, on est facilement ramené au cas du théorème C.c1 par une réduction préalable de toutes les fractions au même dénominateur: la multiplication dans K est en effet c-$\mathcal{P}$-c, puisqu'elle est **RESP** (cf.: déterminant d'une matrice diagonale)

4) si L est lui-même $\mathcal{P}$-réductible, on déduit facilement du théorème C.c1 que la méthode du pivot "ordinaire", avec réduction systématique de toute fraction après calcul, est un $\mathcal{P}$-calcul si et seulement si la fonction déterminant est **RESP** (dans K , donc aussi dans L ici). Cependant, il est en général beaucoup plus économique de travailler avec K : par exemple si K = $\mathbb{Z}$ ou $\mathbb{Z}[X]$, la division exacte dans K est nettement plus rapide que le calcul du pgcd dans K ; or la réduction d'une fraction nécessite un tel calcul de pgcd.

preuve> Tous les coefficients calculés, sont polynomialement majorés en taille à partir de la taille des données: en effet ils sont égaux, au signe près, et sous forme réduite, à des déterminants extraits de la matrice de départ .

Le nombre de coefficients calculés est également polynomialement majoré à partir de la taille des données.

Le seul problème est donc de vérifier que tous les éléments de K calculés au cours de TRAITERPIVOT et TRIANGSOL restent polynomialement majorés en taille: <u>après</u> TRAITERPIVOT ou TRIANGSOL, tout va bien. Que se passe-t-il <u>pendant</u> ? Pendant TRAITERPIVOT on effectue 2 multiplications, une soustraction et une division exacte à partir de coefficients sous forme réduite, puis on réduit le résultat obtenu. Ceci reste polynomialement majoré puisque K est un $\mathcal{P}$-anneau. Pendant TRIANGSOL, c'est le même raisonnement, mais cette fois-ci, il y a une addition itérée (au maximum Nlin fois) portant sur des produits de 2 éléments réduits égaux à des déterminants de matrices extraites de la matrice de départ. Or nous avons déjà établi le résultat adéquat pour l'addition itérée à la proposition C.b2 . ❑

Notes

n.1 §A.a : propriétés de la classe de constructions $\mathfrak{C}$, quelques précisions

NB : il est préférable de lire cette note après avoir lu le § A b)

Nous considérons 3 symboles spéciaux servant à écrire des listes : **[** , **]** , **;** encore appelés **scl** (symboles constructeurs de listes).

Si A ne contient aucun **scl**, l'ensemble **Lst** (A*), des listes d'éléments de A* , peut être réalisé comme une partie du langage A°* (où A° est la réunion de A et des **scl**).
Si X_1 , X_2 ,..., X_n sont des parties de A*, l'ensemble $X_1 \times X_2 \times \ldots \times X_n$ peut être réalisé comme une partie de **Lst**(A*) (listes convenables de n éléments).

Nous supposons qu'aucun alphabet désigné par A , B , C ne contient de **scl**.

Si X est un ensemble, **Lsp**(X) , ensemble des "lispes" d'éléments de X , est défini récursivement par :

Lst'(X) := **Lst** (X) $\cup$ X
Lsp(X) := **Lst'**(X) $\cup$ **Lst'**(**Lst'**(X)) $\cup$ **Lst'**(**Lst'**(**Lst'**(X))) ...

L'ensemble **Lsp**(A*) peut être réalisé comme une partie de A°* . Cette partie est **DT1**-détachable. Un mot de **Lsp**(A*) peut être lu sans ambiguïté comme liste de mots de **Lsp**(A*) , et sans ambiguïté comme lispe d'éléments de A* . En particulier, les opérations de **Lsp**(A*) vers **Lsp**(A*) : "1er mot de la liste" et "liste privée du 1er mot" sont bien définies, ce sont même des $\mathfrak{C}$-opérations.

Pour conserver cette propriété de lisibilité, nous allons restreindre notre "univers" . Nous posons d'abord la :

Définition n.1 : Un $\mathfrak{C}$-préensemble X est donné lorsque :

- on considère un alphabet A ne contenant pas de **scl**
- on considère une $\mathfrak{C}$-opération P_X de **Lsp**(A*) vers {**oui**,**non**}

Les éléments de X sont les mots m de **Lsp**(A*) pour lesquels $P_X(m)$ = oui . Nous dirons que X est un $\mathfrak{C}$-préensemble construit sur A[22] .

Convention : dans la suite, lorsque nous parlons d'une $\mathfrak{C}$-partie d'un langage L* , nous supposons toujours (implicitement ou explicitement) qu'elle est présentée comme un $\mathfrak{C}$-préensemble construit sur un alphabet A (donc en particulier L = A° pour un alphabet A, et les mots de X sont tous dans **Lsp**(A*))

Nous sommes maintenant en mesure de préciser l'énoncé des propriétés de stabilité de la classe $\mathfrak{C}$, et d'en tirer quelques conséquences (admises implicitement dans le texte) .

Nous commençons par préciser une condition concernant la mesure $\| \ \|_X$ pour la grandeur des éléments d'un $\mathfrak{C}$-préensemble X construit sur A . Notons $\| \ \|_{A^*}$ la mesure naturelle (longueur du mot). Nous supposons que nous avons toujours:

- l'identité $I : x \to x$ de $(X, \| \ \|_{A^*})$ vers $(X, \| \ \|_X)$ est une $\mathfrak{C}$-opération

La stabilité pour la composition des opérations et celle pour la définition par cas ne posent pas problème.

Nous donnons par contre des précisions en ce qui concerne la stabilité pour **Lst** . Nous devons tout d'abord énoncer la propriété de stabilité suivante:

---

[22] Nous disons $\mathfrak{C}$-préensemble, plutôt que $\mathfrak{C}$-ensemble, parce que ne sont définies, ni l'égalité de X , ni la mesure de la grandeur de ses éléments.

– si X est un $\mathfrak{C}$-préensemble construit sur A, alors $\mathbf{Lst}(X)$ est un $\mathfrak{C}$-préensemble
construit sur A.

Par ailleurs, lorsqu'on a défini une mesure $\| \|_X$ pour la grandeur des éléments de X, il faut considérer que :

– la mesure de l'élément $[x_1,x_2,...,x_n]$ de $\mathbf{Lst}(X)$ est définie par :
$$\| [x_1,x_2,...,x_n] \|_{\mathbf{Lst}(X)} := \| x_1 \|_X + \| x_2 \|_X + ... + \| x_n \|_X$$

Les propriétés de stabilité suivantes sont alors immédiates:

$\mathfrak{C}$-parties: si Z_1 et Z_2 sont des $\mathfrak{C}$-parties de X, il en est de même pour $Z_1 \cup Z_2$, $Z_1 \cap Z_2$ et $X - Z_1$.

$\mathfrak{C}$-produits: si X est un $\mathfrak{C}$-préensemble construit sur A, et Y est un $\mathfrak{C}$-préensemble construit sur B, alors $X \times Y$ est un $\mathfrak{C}$-préensemble construit sur $A \cup B$.

opérations élémentaires portant sur les listes: les opérations élémentaires suivantes sont des $\mathfrak{C}$-opérations:

– les applications $\mathbf{Lst}(\mathbb{N}) \longrightarrow \mathbb{N}^k$: k premiers éléments de la liste, éventuellement complétée par des 0
– les injections canoniques $\mathbb{N}^k \longrightarrow \mathbf{Lst}(\mathbb{N})$
– l'application $\mathbf{Lst}(N) \times \mathbf{Lst}(\mathbb{N}) \longrightarrow \mathbf{Lst}(\mathbb{N})$: concaténation de 2 listes
– l'application $\mathbf{Lst}(\mathbb{N}) \longrightarrow \mathbf{Lst}(\mathbb{N})$: retrait du premier élément d'une liste

Remarque : si ce n'est essentiellement pour des raisons de commodité, on pourrait d'ailleurs admettre une bonne fois pour toutes un seul alphabet A, ce qui ferait de tous les $\mathfrak{C}$-préensembles des $\mathfrak{C}$-parties de "l'univers" $\mathbf{Lsp}(A^*)$.

n.2 §A.b : $\mathfrak{C}$-équivalences entre les différents A^*, et avec différentes présentations de $\mathbb{N}$

Les résultats affirmés dans le § "quelques $\mathfrak{C}$-équivalences" résultent essentiellement de l'existence d'algorithmes rapides (**DTNLG**) pour la multiplication des entiers en binaire. On pourra par exemple consulter [**DACA**] pour la preuve du caractère **DTNLG** d'un changement de base de numération.

Lorsque nous considérons un entier n écrit en base b, la longueur du mot qui le représente est à peu près proportionnelle à $\mathbf{lg}(n)$ (sa longueur lorsqu'il est écrit en base 2) dans le rapport $\log(2)/\log(b)$. Le changement de base de numération est donc $\mathbf{DTNLG_1}$ (et, avec une modification convenable de la mesure de la taille pour les entiers en base b, il est $\mathbf{DTNLG_0}$)

Par ailleurs, on constate facilement que "$\mathbb{N}$ en base b" est **DT0**-équivalent à A^*, où A est un alphabet à b lettres. Considérons ces lettres comme représentant les chiffres 0, 1, ..., $b-1$. Associons au mot m de longueur k : $a_1a_2...a_k$ l'entier $u(m)$ qui s'écrit $1a_1a_2...a_k$ en base b. Soit alors $num(m)$ le numéro de m lorsqu'on numérote les $u(m)$ en ordre croissant.

On obtient par un petit calcul: $num(m) = u(m) + (1 + b + ... + b^{k-1}) - b^k$, et il est clair que le calcul de $num(m)$ à partir de m, et vice versa, sont dans **DT0**.

n.3 §A.b : produit de 2 $\mathfrak{C}$-ensemble-discrets comme produit au sens des catégories

Tout d'abord, les projections canoniques $X \times Y \longrightarrow X$ et $X \times Y \longrightarrow Y$ sont dans **DT0**. D'autre part, si $f : Z \longrightarrow X$ et $g : Z \longrightarrow Y$ sont dans la classe $\mathfrak{C}$, vue la stabilité de $\mathfrak{C}$ pour les listes, nous savons que $f \times g : Z \times Z \longrightarrow X \times Y$ est dans $\mathfrak{C}$.
Vue la stabilité de $\mathfrak{C}$ pour la composition, nous obtenons donc : si la classe $\mathfrak{C}$ contient les applications diagonales $Z \longrightarrow Z \times Z$ le produit de 2 $\mathfrak{C}$-ensemble-discrets est bien le

produit au sens de la catégorie des $\mathfrak{C}$-ensemble-discrets Ce sera le cas lorsque $\mathfrak{C}$ contient **DT1** , mais pas pour la classe $\mathfrak{P}_0$ par exemple.

n.4 §A.b : structures algébriques avec des axiomes "purement universels"

Nous considérons qu'une structure algébrique (sur un ensemble discret) est donnée par un certain nombre de relations (unaires, binaires...) décidables, par un certain nombre de constantes, et par un certain nombre de lois de compositions non nécessairement "partout définies": mais le domaine de définition doit être décidé par l'une des relations faisant partie de la structure.

Les axiomes liant ces éléments de structure sont dits purement universels, s'ils affirment que certaines égalités (écrites en utilisant exclusivement les constantes et lois de composition de la structure) sont vérifiées en tout point d'une partie décidée par l'une des relations de la structure.

Dans ce cas on a immédiatement une $\mathfrak{C}$-version de la structure considérée, en demandant que les relations de la structure soient $\mathfrak{C}$-décidables et que les lois de composition soient des $\mathfrak{C}$-fonctions.

Par exemple on a une formulation purement universelle de la notion de corps en utilisant les constantes 0 et 1, la partie $K-\{0\}$, les lois $+$, $\times$, $x \longrightarrow -x$, et $x \longrightarrow 1/x$, et des axiomes évidents.

L'une des principales difficultés pour un traitement constructif de l'algèbre discrète vient de l'impossibilité de formuler certaines notions classiques sous forme purement universelle (notamment la notion de noethériannité, qui n'est même pas formulable "au premier ordre"[23]), d'où la difficulté de donner une traduction "calculatoire" de certaines définitions classiques.

Notons que dans la formulation constructive de la notion d'anneau factoriel A , la décomposition en facteurs premiers est une "loi de composition" avec pour ensemble d'arrivée **Lst**(A) . Dans les premières versions du Moderne Algebra de Van der Waerden, un corps est appelé "factoriel" si l'anneau des polynômes à une indéterminée est factoriel au sens constructif.

n.5 §A.b : les structures algébriques récursivement présentées dans [F-S] **(article de Frölich et Shepherdson sur les procédures effectives en théorie des corps)**

L'article en question est sans doute le premier texte systématique sur l'étude des extensions de corps du point de vue de la récursivité. Dans [**F-S**] une structure algébrique "effective" est donnée par un ensemble énuméré, avec une relation d'égalité récursivement décidable (dans l'énumération considérée). Les lois de composition définissant la structure sont vues comme des relations (binaires, ternaires ... $z = x + y$ par exemple), de sorte qu'une loi de composition est dite "effective" si son graphe est récursivement décidable.

Dans la mesure où il s'agit de lois de composition partout définies, ou définies sur des parties récursivement décidables, on obtient bien la même notion que celle de structure algébrique récursivement présentée (c.-à-d. encore de **Rec**-structure) que nous avons définie.

Dans cet article sont définis 2 corps récursifs K et L avec les propriétés suivantes:

K[X] est récursivement factoriel, L[X] ne l'est pas

K et L sont isomorphes

Evidemment K et L ne sont pas récursivement isomorphes, et la preuve de l'existence d'un isomorphisme entre K et L est non constructive.

---

23 C'est à dire au moyen d'une formule du premier ordre portant sur des variables dans la structure algébrique considérée.

Noter cependant que la notion de noetheriannité a néanmoins reçu un traitement constructif entièrement satisfaisant dans le cas des anneaux commutatifs discrets. cf. [**CAL**]

n.6 §A.b : les structures algébriques de type fini sont "naturellement primitives récursives"

NB : il est préférable de lire cette note après avoir lu le § B a)

Une structure algébrique (X,Y,Z) est de type fini si tout objet peut être obtenu à partir des constantes et d'un nombre fini d'éléments $a_1,a_2,...,a_n$ en utilisant de manière répétée les lois de composition.

Considérons alors la partie T de **Calc**(X,Y,Z) (cf. §B.a) où seules interviennent les constantes et les éléments $a_1,a_2,...,a_n$: on obtient, en prenant la relation d'égalité convenable, une présentation de $X \cup Y \cup Z$, pour laquelle les lois de composition sont $\mathbb{P}\mathbf{r}$, et même **DT0** . Mais il reste le problème de l'égalité dans T , qui peut n'être pas $\mathbb{P}\mathbf{r}$, ni même **Rec** . Et pareil pour les autres relations faisant partie de la structure.

Si (X,Y,Z) était au départ une $\mathbb{P}\mathbf{r}$-structure, alors il est clair que la relation d'égalité dans T (et les autres relations faisant partie de la structure) sont $\mathbb{P}\mathbf{r}$, et que la bijection naturelle de **Calc**(X,Y,Z) vers $X \cup Y \cup Z$ est une $\mathbb{P}\mathbf{r}$-fonction.

Cette présentation naturelle est $\mathbb{P}\mathbf{r}$-équivalente à la présentation de départ si et seulement si on peut retrouver, par un calcul $\mathbb{P}\mathbf{r}$, une manière d'écrire n'importe quel objet x à partir des constantes et des éléments en nombre fini considérés: c.-à-d. si la structure, avec sa présentation, est "de type fini de manière $\mathbb{P}\mathbf{r}$" .

On remarquera qu'il semble difficile d'obtenir une structure algébrique qui serait "intrinsèquement $\mathbb{P}\mathbf{r}$ " au sens suivant : 2 $\mathbb{P}\mathbf{r}$-présentations de la structure sont nécessairement $\mathbb{P}\mathbf{r}$-isomorphes . (sauf dans le cas des structures finies) . Par contre les structures algébriques récursivement présentées de type fini sont "intrinsèquement récursives" (au même sens que ci-dessus).

n.7 §A.c : rapports entre $\mathbb{P}$-dénombrabilité et $\mathbb{P} = \mathcal{N}\mathbb{P}$?

On l'implication :

si $\mathbb{P} = \mathcal{N}\mathbb{P}$, alors tout $\mathbb{P}$-ensemble est $\mathbb{P}$-dénombrable.

Soit en effet X un $\mathbb{P}$-ensemble et (f,r) une $\mathbb{P}$-énumération de X.

Pour $n , p \in \mathbb{N}$ définissons :

$$g(n,p) := \begin{cases} 0 & \text{si } f(n) = u \text{ ou } f(p) = u \text{ ou } f(n) \neq f(p) \\ n - p & \text{sinon} \end{cases}$$

Pour n fixé tel que $f(n) \neq u$, g(n,p) est maximum pour la 1ère valeur de p vérifiant $f(p) = f(n)$, et la connaissance de ce maximum permet de retrouver p .

Si donc on définit $h(n,p) := \sup\{g(n,q) , q \leq p\}$ on a le dénombrement (f,r') de X donné par : $r'(x) := f(n - h(n,n))$, où $n := r(x)$.

Or $\mathbb{P} = \mathcal{N}\mathbb{P}$ équivaut au fait que la fonctionnelle **Sup** qui fait passer de g à h transforme toute $\mathbb{P}$-fonction en une $\mathbb{P}$-fonction.

Notons enfin qu'il est probable qu'on ait l'implication réciproque : si tout $\mathbb{P}$-ensemble est $\mathbb{P}$-dénombrable, alors $\mathbb{P} = \mathcal{N}\mathbb{P}$.

n.8 §B.a : $\mathbb{Q}$ est $\mathbb{P}$-isomorphe à sa présentation en fraction continue standard

Il reste à montrer que le passage du rationnel $q = a/b$ à la liste des entiers constituant son **dfc** (développement en fraction continue) standard est une $\mathbb{P}$-fonction. Or le calcul du **dfc** se fait par divisions successives, et n'est rien d'autre que l'algorithme d'Euclide pour le pgcd du numérateur et du dénominateur. Si c est le sup de la valeur absolue du numérateur et du dénominateur, les entiers du **dfc** sont tous inférieurs à c (pour le premier: en valeur absolue) et leur nombre est majoré par 2.**lg**(c) : le pire cas est obtenu avec les **dfc** dont tous les termes sont égaux à 1 (cf. par ex D. Knuth [**ACP 4**] p 343)

BIBLIOGRAPHIE

[**Ait**] On the evaluation of determinants, the formation of their adjugates, and the practical solution of simultaneous linear equations.
Aitken A. C.
Proc. Edinburgh Math. Soc. ser 2 III , 207-219 , (1932)

[**ALFA**] Algèbre (cours de mathématiques, tome 1)
J. Lelong-Ferrand, J.-M. Arnaudiès
(Dunod; 1974)

[**ACP4**] The Art of Computer Programming (vol 2).
Chap 4: Arithmetic Seminumerical Algorithms. 2ème édition
D. E. Knuth
(Addison-Wesley; 1973)

[**Bar**] Sylvester's Identity and Multistep Integer-Preserving Gaussian Elimination
Bareiss E. H.
Math. Comp. 22 565-578 (1968)

[**Ber**] On computing the determinant in small parallel time using a small number of processors . **Berkovitz S. J**.
Information Processing Letters 18 n°3 147-150 (1984) .

[**CA**] Constructive Analysis
E. Bishop, D. Bridges
(Springer-Verlag; 1985)

[**CAL**] A Course in Constructive Algebra
R. Mines, F. Richman, W. Ruitenburg
(Springer-Verlag; Universitext; 1988)

[**CASAC**] Computer Algebra: Symbolic and algebraic computation
Edited by Buchberger, Collins and Loos
(Springer-Verlag; 1982)

[**CFA**] Constructive Functional Analysis
D. Bridges
(Pitman, London; 1979)

[**DACA**] The Design and Analysis of Computer Algorithms
A.V. Aho, J. E. Hopcroft, J. D. Ullman
(Addison-Wesley; 1974)

[**F-S**] Effective procedures in Field Theory
A. Frölich, J. C. Shepherdson
Philos. Trans. Roy. Soc. London (Ser A) 284 (1955) 407-432

[**FCM**] Foundations of Constructive Mathematics
M. Beeson
(Springer -Verlag; 1985)

[**Gan**] Théorie des Matrices
Gantmacher F. R.
DUNOD (1966) (traduit du russe)

[**ITALC**] Introduction to the Theory of Automata, Languages and Computability
J. E. Hopcroft, J. D. Ullman
(Addison-Wesley; 1979)

[**Sam**] A method for determining explicitly the coefficients of the characteristic equation .
Samuelson P. A.
Ann. Math. Stat. 13 (1942) 424-429.

INDEX

Rec	:	A 5	:	classe des opérations récursives
RES0	:	A 5	:	$\cup_c$ **SPACERES**(n+c)
RES1	:	A 5	:	**SPACERES**(O(n))
RESP	:	A 5	:	$\cup_b$ **SPACERES**(O(n^b))
séparation	:	intro 3		
SPACERES(f(n))	:	A 5	:	la mesure de la taille du résultat est majoré par f(n), où n est la mesure de la taille de l'entrée
Sv(L)	:	C 35		
Syslin(L)	:	C 45	:	ensemble des systèmes d'équations linéaires à coefficients dans L
systéme linéaire résolu	:	C 46		
Trimat(K)	:	C 35	:	ensemble des matrices carrées n x n supérieures, à coeffs dans K , avec des 1 sur la diagonale (réunion disjointe sur les n)
$\mathbb{Z}$	:	A 15	:	entiers relatifs présentés en binaire
$\mathbb{Z}_1$	:	A 15	:	entiers relatifs présentés en unaire
$\mathbb{Z}[X]$	:	B 21	:	polynômes en présentation "dense"
$\mathbb{Z}[X]_c$	:	B 21	:	polynômes en présentation "creuse"

CALCULABILITE DANS LES STRUCTURES ALGEBRIQUES DENOMBRABLES