Un (nouvel ?) algorithme pour la décomposition de Dunford effective

Jean-François Burnol, 6 avril 2017

Je me place sur un corps $\mathbf{K}$ de caractéristique nulle. Je note $\overline{\mathbf{K}}$ une clôture algébrique. Le cas de la caractéristique positive sera brièvement évoqué à la fin.

1 Décomposition de Jordan-Chevalley

Soit A un endomorphisme d'un $\mathbf{K}$-espace vectoriel V de dimension finie. La théorie des espaces caractéristiques (on se place sur $\overline{\mathbf{K}}$ pour le moment) permet de voir rapidement que l'on peut décomposer A de manière unique sous la forme $D+N$ avec $DN = ND$, D diagonalisable (sur $\overline{\mathbf{K}}$!) et N nilpotent. On prend D comme agissant sur l'espace caractéristique V_λ par la multiplication par le scalaire λ.

En fait (et l'unicité peut nous le faire anticiper, sauf qu'il y a des contre-exemples en caractéristique positive à cette « intuition »), D et N sont définis sur $\mathbf{K}$, et même mieux, D peut s'écrire comme un polynôme $D(A)$ à coefficient dans $\mathbf{K}$.

Soit $\lambda_j, 1 \leqslant j \leqslant k$ les valeurs propres et $m_j, 1 \leqslant j \leqslant k$ leurs multiplicités (ou leurs multiplicités dans le polynôme minimal, si elles sont connues, et au pire on peut toujours prendre $m_j = \dim V - (k-1)$, avec k le nombre de valeurs propres distinctes). Il suffit pour obtenir un polynôme D convenable (en l'indéterminée X) de résoudre le problème chinois

$$\forall 1 \leqslant j \leqslant k \qquad D \equiv \lambda_j \pmod{(X-\lambda_j)^{m_j}}$$

Et il faut prouver qu'il y a une solution à coefficients dans $\mathbf{K}$!

Cette résolution peut se faire de diverses manières, la plupart du temps par l'intermédiaire d'identités (ou d'une seule identité) de Bezout appropriées. Tout cela est algorithmique, *si l'on connaît les valeurs propres individuellement.* Ce qui numériquement pose de sérieux problèmes de stabilité.

Pour des raisons que j'ignore, cette décomposition est appelée communément « décomposition de Dunford », et depuis une quinzaine ou une vingtaine d'an-

nées elle est très à la mode aux oraux de l'agrégation (externe ou interne), et d'ailleurs semble-t-il même à l'écrit cette année 2017.

Dans ce contexte on voit parfois une superbe démonstration effective, qui semble provenir à l'origine de l'ouvrage *Théorie des groupes de Lie Tome II* de Claude Chevalley, paru en 1951. [1]

Cette approche fonctionne entièrement dans $\mathbf{K}[X]$ et n'a (ainsi que l'approche chinoise l'indiquait déjà) comme point de départ que le polynôme caractéristique (unitaire) P de A.

Soit $Q = P/\mathrm{PGCD}(P, P')$ le polynôme réduit unitaire possédant les mêmes racines que P dans $\overline{\mathbf{K}}$. Puis H un polynôme réalisant une identité de Bezout $HQ' + VQ = 1$.

Chevalley procède par substitutions itérées de l'indéterminée $X \leftarrow X - HQ$, ce qui définit donc un homomorphisme de $K[X]$ dans lui-même. Notons comme lui $T \mapsto s(T)$ cette transformation. Chevalley démontre que le polynôme $s^k(X)$ vérifie $Q(s^k(X)) \in (Q^{2^k})$ et est un D approprié dès que 2^k est tel que P divise Q^{2^k}.

On peut présenter les choses un peu différemment, plus à la Newton, en considérant la transformation (qui n'est *pas un morphisme*) $T \mapsto F(T) = T - H(T)Q(T)$. L'algorithme de Newton pour trouver une racine de $Q(x) = 0$ serait d'itérer $x \mapsto x - Q(x)/Q'(x)$ en partant d'un x_0 convenable. Le $H(T)$ remplace un $1/Q'(T)$ qui nous ferait quitter les polynômes, et même si l'on travaille modulo le polynôme P disons, il nous évite d'avoir à inverser $Q'(T)$ (qui change à chaque étape) dans $\mathbf{K}[X]/(P)$.

Bref, considérons l'itérée F^m de la transformation à la Newton, *spécialement dans le cas avec point de départ* X. Elle nous donnera :

$$F(F(\dots(F(F(X)))\dots))$$

Mais cette formule est aussi construite non pas en appliquant F à « l'extérieur », mais en substituant de manière itérée $X \leftarrow F(X)$ à « l'intérieur », ce

1. Je remercie Mme Blanc-Centi et M. Olivier Serman pour les références que voici :
— Daniel Ferrand, *Une méthode effective pour la décomposition de Dunford*, Préparation à l'agrégation, Université de Rennes, 2003.
http://agreg-maths.univ-rennes1.fr/documentation/docs/Jordan.algor.pdf,
— P. Saux Picart *Cours de calcul formel. Algorithmes fondamentaux*. Ellipses, 1999.
— D. Couty, J. Esterle, R. Zarouf, *Décomposition effective de* Jordan-Chevalley *et ses retombées en enseignement*.
https://www.math.u-bordeaux.fr/~jesterle/Jordan-Chevalley.pdf

qui est exactement la tranformation de Chevalley.

À chaque itération (j'évite le cas trivial $\deg Q = 1$) on multiplie le degré par $\deg H + \deg Q$, et a priori $\deg H$ ne peut sauf cas spécial pas être pris inférieur à $\deg Q - 1$, donc au bout de m itérations on a affaire à des polynômes de degrés $(2\deg Q - 1)^m$, explosion exponentielle.

Évidemment dans la pratique on travaillera dans $\mathbf{K}[X]/(P)$, en réduisant modulo P à chaque itération. Il y a une subtilité ici : $P(X - HQ)$ est en effet divisible par P. Soit λ une racine de P et m sa multiplicité. Comme $(X-\lambda)^m$ divise P dans $\overline{\mathbf{K}}[X]$, $(X - HQ - \lambda)^m$ divise $P(X - HQ)$. Mais $X - \lambda$ divise Q, donc $(X-\lambda)^m$ divise $P(X - HQ)$ et par conséquent P divise $P(X - HQ)$ dans $\mathbf{K}[X]$.

D'ailleurs, dans l'esprit de la stabilité de la méthode Newton, il devrait suffire de faire la première étape modulo Q^2, la seconde modulo Q^4, la troisième modulo Q^8 etc... [2]

La méthode par substitution de Chevalley *possède en effet cette stabilité numérique*. Car nous avons là un *morphisme*, donc si avant d'itérer une seconde fois on modifie additivement par un Q^2Z, à la m^e étape on aura donc modifié additivement par $Q(s^{m-1}(X))^2 Z(s^{m-1}(X))$. Or Chevalley prouve que $Q(s^{m-1}(X))$ est divisible par $Q^{2^{m-1}}$, donc l'erreur propagée est divisible par Q^{2^m} et au final elle disparaît modulo P.

La même stabilité numérique fonctionne dans la variante qui fait $T \mapsto F(T) = T - H(T)Q(T)$, avec $T = X$ comme point de départ (ou un polynôme qui lui est congru modulo Q). Je ne donne pas les détails.

2 Une autre construction de D

Le but de cette fiche est d'expliquer un autre algorithme, beaucoup moins rusé que celui de Chevalley-Hensel-Newton !

On note $\lambda_1, \ldots, \lambda_k$ les racines (qui sont simples) de Q. Soit n le maximum de leurs multiplicités (ou n'importe quel entier plus grand) en tant que racines de P (ou du polynôme minimal de A, si on connaît ce dernier). La formule (où le dénominateur est en effet un endomorphisme inversible)

2. La toute première étape $X - HQ$ est déjà modulo Q^2, mais plus après car $(2\deg Q - 1)^m$ l'emporte (largement) sur $2^m \deg Q$.

$$D_n = \frac{\sum_j \lambda_j \prod_{i\neq j}(A-\lambda_i)^n}{\sum_j \prod_{i\neq j}(A-\lambda_i)^n}$$

donne le D de la décomposition de Dunford, $A = D+N$ avec D diagonalisable dans une clôture algébrique, $DN = ND$ et N nilpotent. Voir

http://jf.burnol.free.fr/agreg170405Dunford.pdf

Voici comment calculer à partir de Q et n les polynômes en A qui figurent au numérateur et au dénominateur. Et donc au passage de vérifier qu'ils sont à coefficients dans le corps de base (ce dernier point est déjà expliqué dans la référence ci-dessus).

On a noté $\overline{\mathbf{K}}$ une clôture algébrique de $\mathbf{K}$. Dorénavant notre point de départ est un polynôme $Q \in \mathbf{K}[X]$, à racines simples dans $\overline{\mathbf{K}}$. On posera formellement $U_0 = \log Q$, puis moins formellement $U_1 = Q'$ et plus généralement

$$U_n = Q^n (\log Q)^{(n)} = Q^n \left(\frac{Q'}{Q}\right)^{(n-1)}$$

Les dérivées sont par rapport à l'indéterminée X.

Comme fraction rationnelle dans $\overline{\mathbf{K}}(X)$, on a évidemment :

$$U_n = (-1)^{n-1}(n-1)!\cdot Q^n \cdot \sum_j (X-\lambda_j)^{-n}\,,$$

formule qui montre que U_n est un polynôme. Cela se confirme par la récurrence

$$\boxed{U_{n+1} = QU_n' - nQ'U_n} \qquad U_1 = Q' \qquad U_2 = QQ'' - (Q')^2$$

Je pose maintenant

$$\boxed{V_n = XU_n + (n-1)QU_{n-1}} \qquad V_1 = XU_1 \qquad V_2 = XU_2 + QU_1$$

de sorte que nous avons ici à nouveau des polynômes de $\mathbf{K}[X]$ et que dans $\overline{\mathbf{K}}(X)$ on peut écrire, pour $n \geqslant 2$:

$$\frac{V_n}{Q^n} = X(-1)^{n-1}(n-1)!\sum_j (X-\lambda_j)^{-n} - (-1)^{n-1}(n-1)!\sum_j (X-\lambda_j)(X-\lambda_j)^{-n}$$

$$V_n = (-1)^{n-1}(n-1)!\cdot Q^n \cdot \sum_j \lambda_j (X-\lambda_j)^{-n}\,.$$

Il faut faire attention au cas $n = 1$: $\frac{V_1}{Q} = X\frac{U_1}{Q} = \deg Q + \sum_j \lambda_j (X-\lambda_j)^{-1}$.

Nous définissons D_n comme la fraction rationnelle $\frac{V_n}{U_n}$ de $\mathbf{K}(X)$. Ce qui nous donne les formules :

$$D_1 = \frac{V_1}{U_1} = X$$
$$D_n = \frac{V_n}{U_n} = X + \frac{(n-1)U_{n-1}}{U_n} Q \qquad (n \geqslant 2)$$

Théorème. *Le polynôme* $E_n = Q(D_n)U_n^{\deg Q}$ *est dans* $Q^n\mathbf{K}[X]$.

Preuve. Pour $n = 1$, $E_1 = Q \cdot (Q')^{\deg Q}$. Pour $n \geqslant 2$, on commence par travailler dans $\overline{\mathbf{K}}[X]/(Q^n)$, on note π_j les morphismes naturels vers les $\overline{\mathbf{K}}[X]/((X-\lambda_j)^n)$. On a $E_n = \prod_j (V_n - \lambda_j U_n)$. Or, par les formules précédentes :

$$U_n = (-1)^{n-1}(n-1)! \sum_j \prod_{i \neq j} (X - \lambda_i)^n$$
$$V_n = (-1)^{n-1}(n-1)! \sum_j \lambda_j \prod_{i \neq j} (X - \lambda_i)^n$$

d'où il résulte $\pi_j(V_n) = \lambda_j \pi_j(U_n)$ pour tout j. Et par conséquent $\pi_j(E_n) = 0$, pour tout j. Et donc E_n est un multiple dans $\overline{\mathbf{K}}[X]$ du produit $\prod_j (X - \lambda_j)^n = Q^n$. Mais comme E_n et Q^n sont dans $\mathbf{K}[X]$, c'est que $E_n \in Q^n\mathbf{K}[X]$. □

Les degrés (en caractéristique nulle) de nos polynômes sont : $\deg U_n = n(\deg Q - 1)$ et $\deg V_n \leqslant n(\deg Q - 1)$.

Revenons au contexte d'un endomorphisme A sur un K espace vectoriel V de dimension finie. Concrètement A nous sera donné par une matrice. On calcule P son polynôme caractéristique et Q le polynôme réduit. On choisit n comme le plus petit entier tel que P divise Q^n.

Si $n = 1$ il n'y a rien à faire ($D = A$, $N = 0$), donc je supposerai $n \geqslant 2$ dans la description qui suit.

On calcule les polynômes U_{k-1}, U_k jusqu'à $k = n$ par les formules de récurrence débutant avec $U_1 = Q'$.

Le polynôme U_n est premier avec Q^n, comme on peut s'en convaincre par le fait que les $\pi_j(U_n)$ sont tous inversibles (avec les notations de la preuve ci-dessus).

On peut donc par une identité de Bezout trouver un polynôme W_n qui en représente l'inverse de U_n modulo Q^n (ou même seulement modulo P).

L'endomorphisme $N = -(n-1)W_n(A)U_{n-1}(A)Q(A)$ est évidemment nilpotent. L'endomorphisme $D(A) = A - N$ vérifie par le théorème :

$$Q(D(A)) = 0$$

Il est donc diagonalisable sur $\overline{\mathbf{K}}$ (ce que l'on sait déjà depuis longtemps, par les considérations d'espaces caractéristiques et la façon dont on a construit V_n et U_n). Et il a été exprimé comme un polynôme en A à coefficients dans $\mathbf{K}$.

Si l'on n'a pas besoin de l'expression polynomiale pour D, on peut aussi calculer l'inverse de la matrice $U_n(A)$ directement.

3 Un exemple numérique (avec Maple)

```
> Q:=(x-1)*(x-2)*(x-3)
                    (x - 1) (x - 2) (x - 3)

> P:=Q**3;
                           3        3        3
                  (x - 1)  (x - 2)  (x - 3)

> U1:=diff(Q,x);
      (x - 2) (x - 3) + (x - 1) (x - 3) + (x - 1) (x - 2)

> U1:=simplify(U1);
                             2
                        3 x  - 12 x + 11

> Qprime:=U1:

> U2:=simplify(Q*diff(U1,x)-Qprime*U1);
                     4       3       2
                -3 x  + 24 x  - 72 x  + 96 x - 49

> U3:=simplify(Q*diff(U2,x)-2*Qprime*U2);
```

```
       6       5        4         3         2
    6 x  - 72 x  + 366 x  - 1008 x  + 1590 x  - 1368 x + 502
```

```
> gcdex(U3,P,x,'W3');
                                1
```

```
> W3;
 945  8   945  7   51621  6   49023  5   904701  4   161901  3
 --- x  - --- x  + ----- x  - ----- x  + ------ x  - ------ x
 256      16        128        32         256          32

      140235  2   16785     6805
    + ------ x  - ----- x + ----
        32          8        16
```

```
> D3:=rem(x+2*W3*U2*Q,P,x);
15  7   105  6   609  5   945  4   6755  3   3465  2   945
-- x  - --- x  + --- x  - --- x  + ---- x  - ---- x  + --- x - 105
8        4        4        2        8         4         2
```

```
> A:=evalm([[1,5,7,0,0,0,0,0,0], [0,1,-3,0,0,0,0,0,0], [0,0,1,0,0,0,0,0,0],
            [0,0,0,2,-3,4,0,0,0], [0,0,0,0,2,1,0,0,0], [0,0,0,0,0,2,0,0,0],
            [0,0,0,0,0,0,3,-1,1], [0,0,0,0,0,0,0,3,-2], [0,0,0,0,0,0,0,0,3]]);
```

```
> evalm(subs(x=A,D3));
```

Le polynôme D3

$$\frac{15\,x^7}{8}-\frac{105\,x^6}{4}+\frac{609\,x^5}{4}-\frac{945\,x^4}{2}+\frac{6755\,x^3}{8}-\frac{3465\,x^2}{4}+\frac{945\,x}{2}-105$$

permet de trouver la partie diagonalisable de toute matrice annulée par $(X-1)^3(X-2)^3(X-3)^3$, et pas seulement comme dans l'exemple ci-dessus pour les matrices ayant ce polynôme comme polynôme caractéristique (unitaire). À propos je ne me suis pas vraiment fatigué pour trouver une matrice avec ce polynôme caractéristique mais bon ça marche, le $D_3(A)$ en est bien la partie diagonale. Vérifions d'ailleurs qu'il résout le problème chinois :

```
> rem(D3,(x-1)**3,x);
                                1
```

```
> rem(D3,(x-2)**3,x);
                                   2
> rem(D3,(x-3)**3,x);
                                   3
```

4 Un deuxième exemple

On part de $Q = 1 + X + X^3 + X^2 + X^4$, dont les racines sont les racines quintiques de l'unité, et on traite le cas de la multiplicité deux, pour faire simple.

En suivant les étapes on (Maple) aboutit à $D_2 \equiv \frac{-1}{5}X^6 + \frac{6}{5}X \pmod{Q^2}$. Considérons la matrice

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & -2 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & -3 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & -4 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -5 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & -4 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -2 \end{pmatrix}$$

dont le polynôme caractéristique est Q^2. La partie diagonalisable (sur $\mathbf{C}$) donnée par la formule $D_2(A)$ est :

$$D = \begin{pmatrix} 0 & 0 & \frac{1}{5} & \frac{-2}{5} & \frac{1}{5} & 0 & 0 & \frac{-4}{5} \\ \frac{6}{5} & 0 & \frac{2}{5} & \frac{-3}{5} & 0 & \frac{1}{5} & 0 & \frac{-8}{5} \\ 0 & \frac{6}{5} & \frac{3}{5} & \frac{-4}{5} & 0 & 0 & \frac{1}{5} & \frac{-12}{5} \\ 0 & 0 & 2 & -1 & 0 & 0 & 0 & -3 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & -4 \\ 0 & 0 & \frac{4}{5} & \frac{-3}{5} & \frac{4}{5} & 0 & 0 & \frac{-16}{5} \\ \frac{-1}{5} & 0 & \frac{3}{5} & \frac{-2}{5} & 0 & \frac{4}{5} & 0 & \frac{-12}{5} \\ 0 & \frac{-1}{5} & \frac{2}{5} & \frac{-1}{5} & 0 & 0 & \frac{4}{5} & \frac{-8}{5} \end{pmatrix}$$

et on (Maple) peut vérifier qu'en effet $Q(D) = 0$ comme matrice et que $(A - D)^2 = 0$.

5 Une note sur la caractéristique positive

La méthode fonctionne si A annule un Q^n avec n au plus égal à la caractéristique p et $Q \in \mathbf{K}[X]$. Certains s'inquièteront peut-être que je ne demande pas $n < p$, mais pour les contre-exemples du type multiplication par X dans $\mathbf{F}_p(T)[X]/(X^p - T)$, il faut voir que A annule Q^p avec $Q = X - T^{1/p}$ mais que ce dernier n'est pas dans $\mathbf{K}[X]$. Donc il n'y a pas à s'inquiéter que le $N = A - T^{1/p}$ de Dunford ne soit pas défini sur $\mathbf{K}$. Ceci ne contredit pas nos constructions autorisant $n = p$, car celles-ci exigent un $Q \in \mathbf{K}[X]$ pour débuter.

Dunford n'est pas limité à $n \leqslant p$ et la formule de

http://jf.burnol.free.fr/agreg170405Dunford.pdf

que l'algorithme de cette fiche rend effective n'est pas elle non plus limitée à $n \leqslant p$, simplement la construction algorithmique effective exposée ici ne fonctionne plus pour obtenir des expressions polynomiales pour le numérateur et le dénominateur, lorsque $n > p$.