2.11 Quand Newton décide de faire de l'algèbre : décomposition de Jordan-Dunford-Chevalley ou quelque chose comme ça (150, 152, 154, 156)

Dans ce développement, je détaille une version très générale du théorème de décomposition de Dunford, qui aurait dû avoir le nom Jordan-Chevalley d'après Matthieu Romagny (qui est une source pour ce développement), avec un algorithme de calcul effectif, basé sur la méthode de Newton, qui fut la démonstration originelle de Chevalley. On introduit alors la notion de *corps parfait* et d'endomorphisme *semi-simple*.

Définition 2.23 (Corps parfait)**.** Un corps k est dit *parfait* si l'une des deux conditions suivantes est satisfaite :

1. $\mathrm{car}(k) = 0$,
2. $\mathrm{car}(k) > 0$ et le morphisme de Frobenius est surjectif, et donc est un automorphisme.

Remarque 2.11.1. *Une définition équivalente, qui peut se retrouver dans le Gozard [12] est qu'un corps k est dit parfait si tout polynôme irréductible $P \in k[X]$ est tel que $P' \neq 0$ ou, de manière équivalente, si tout polynôme irréductible de $k[X]$ est à racines simples dans un corps de décomposition. Il faut avoir en tête des exemples et des contre-exemples de corps parfaits en caractéristique non-nulle :*

- *Les corps finis sont parfaits,*
- *Si p est un nombre premier, le corps $\mathbb{F}_p(T)$ n'est pas parfait. En effet, l'indéterminée T n'a pas de racine p-ième.*

Définition 2.24 (Endomorphisme semi-simple)**.** Soient k un corps parfait et E un k-espace vectoriel de dimension finie. On dit qu'un endomorphisme $u \in \mathscr{L}(E)$ est *semi-simple* s'il vérifie l'une des conditions équivalentes suivantes :

1. Tout sous-espace vectoriel de E stable par u possède un supplémentaire stable par u,
2. u est diagonalisable dans une extension de k,
3. Le polynôme minimal $\pi_u \in k[X]$ de u est sans facteur carré, c'est-à-dire que si $P \in k[X]$ est un polynôme irréductible tel que $P \mid \pi_u$, alors $P^2 \nmid \pi_u$.

Remarque 2.11.2. *Les équivalences ne sont pas forcément évidentes à montrer, mais ce n'est pas le but de ce développement ! Vous pourrez retrouver une preuve dans [18]. Nous n'utiliserons que la troisième caractérisation ici.*

Théorème 2.25 (Décomposition de Dunford/Jordan-Chevalley)**.** Soient k un corps parfait et E un k-espace vectoriel de dimension finie. Alors pour tout $u \in \mathscr{L}(E)$, il existe d'uniques endomorphismes $s, n \in \mathscr{L}(E)$ tels que :

- s est semi-simple,
- n est nilpotent,
- $u = s + n$,
- $s \circ n = n \circ s$.

De plus, $s, n \in k[u]$ et $\pi_s \mid \pi_u$.

Démonstration. **Étape 1 : Unicité** La partie la plus simple est de prouver l'unicité. Si $(s, n), (s', n') \in \mathscr{L}(E)^2$ sont deux couples d'endomorphismes vérifiant les hypothèses du théorème, alors, on a :

$$s' - s = n - n'.$$

On a également que s' et s commutent puisque ce sont deux polynômes en u. (cette propriété est gratuite d'après le théorème !) Ainsi, en se plaçant dans un corps de décomposition de π_u par exemple, on a que s et s' sont tous deux

diagonalisables. Ainsi, ils sont diagonalisables dans une même base et donc $s'-s$ est diagonalisable dans cette même base. De même, n et n' commutent et donc $n-n'$ est nilpotente. Ainsi, $s'-s=n'-n$ est à la fois diagonalisable et nilpotente, c'est donc l'endomorphisme nul ! Donc $s=s'$ et $n=n'$.

Étape 2 : L'existence par la méthode de Newton L'idée est la suivante : si $u \in \mathscr{L}(E)$ est tel que :

$$\pi_u = \prod_{i=1}^{r} P_i^{\alpha_i}$$

avec $P_i \in k[X]$ irréductible et $\alpha_i \in \mathbb{N}^*$, on veut trouver un polynôme P sans facteur carré qui divise π_u et un endomorphisme s tel que $P(s)=0$, de sorte que s soit semi-simple. On va pas trop se casser la tête ! On prendra :

$$P = \prod_{i=1}^{r} P_i$$

aussi appelé *radical* du polynôme π_u. Comment trouver un zéro de P ? Avec la méthode de Newton bien sûr ! Pourquoi c'est particulièrement intéressant dans ce cas-là :

— On veut obtenir $u = s+n$. Ainsi, u s'écrit comme un zéro de P plus un élément nilpotent, donc un infinitésimal ! Si on était en analyse, on serait dans le cadre favorable où, en initialisant la méthode en u, on initialiserait pile dans un voisinage de s où la méthode converge.

— Puisque k est parfait, on a que P est scindé à racines simples dans un corps de décomposition étant donné qu'il est sans facteur carré. Ainsi, $P \wedge P' = 1$ (cf. développement sur Dirichlet faible !). En prenant une relation de Bézout :

$$UP + VP' = 1$$

On a alors :

$$V(s) \circ P'(s) = id_E.$$

Ainsi, $P'(s)$ est inversible ! Cela permettra d'assurer la convergence rapide de la méthode !

— La méthode n'aura pas de mal à s'initialiser : on a l'existence d'un entier $\alpha \in \mathbb{N}^*$ tel que :

$$\pi_u \mid P^\alpha.$$

Le α optimal serait $\max\limits_{1\leq i\leq r} \alpha_i$ mais si on n'a aucune information sur les multiplicités, $\alpha = \deg(\pi_u)$ convient de toute façon. Ainsi, étant donné que $P \wedge P' = 1$, on a également $P^\alpha \wedge P' = 1$, et donc en reprenant une relation de Bézout, comme pour le cas précédent, on obtiendra que :

$$P'(u) \in k[u]^\times.$$

Bref. Écrivons la méthode. Tous les calculs vont se passer dans $k[u]$. On posera alors la suite $(u_k)_{k\in\mathbb{N}} \in k[u]^{\mathbb{N}}$ de la façon suivante :

$$\begin{cases} u_0 &= u, \\ u_{k+1} &= u_k - P'(u_k)^{-1} \circ P(u_k), \quad \forall k \in \mathbb{N}. \end{cases}$$

Puisqu'on se trouve dans la k-algèbre commutative $(k[u], +, \cdot, \circ)$, on se fiche de l'ordre de composition. Remarquons également, que, puisque π_u divise P^α, $P(u)$ est nilpotent d'indice inférieur à α. Notons alors, comme en analyse, $\varepsilon := P(u)$ et, pour $m \in \mathbb{N}$, lorsque $v \in (\varepsilon^m)$ (v est dans l'idéal engendré par ε^m), $v = O(\varepsilon^m)$. Prouvons les trois faits suivants par récurrence :

1. u_n est bien définie,
2. $\forall k \in \mathbb{N}, \quad P(u_k) = O\left(\varepsilon^{2^k}\right)$,
3. $\forall k \in \mathbb{N}, \quad u_k - u = O(\varepsilon)$.

L'initialisation au rang $k = 0$ est évidente. Montrons que la propriété est héréditaire :

1. On a que $u_k - u = O(\varepsilon)$. Ainsi, on a :

$$P'(u_k) - P'(u) = O(\varepsilon).$$

   Ainsi, $P'(u_k)$ est la somme d'un élément de $k[u]^\times$ ($P'(u)$) et d'un élément nilpotent (tout élément dans l'idéal engendré par ε est nilpotent). Ainsi :

$$P'(u_k) \in k[u]^\times.$$

   Cela montre donc que u_{k+1} est bien définie.

2. Soit $Q \in k[X, Y]$ un polynôme tel que :

$$P(X + Y) = P(X) + YP'(X) + Y^2Q(X, Y).$$

   On peut montrer l'existence d'un tel polynôme via la formule de Taylor appliquée à P. On a alors :

$$\begin{aligned} P(u_{k+1}) &= P\left(u_k - P'(u_k)^{-1} \circ P(u_k)\right) \\ &= P(u_k) - P'(u_k)^{-1} \circ P(u_k) \circ P'(u_k) + \left(P'(u_k)^{-1} \circ P(u_k)\right)^2 \circ Q\left(u_k, -P'(u_k)^{-1} \circ P(u_k)\right) \\ &= O\left(P(u_k)^2\right) \\ &= O\left(\varepsilon^{2^{k+1}}\right) \end{aligned}$$

   par hypothèse de récurrence.

3. On a tout simplement :

$$u_{k+1} - u = \underbrace{u_k - u}_{=O(\varepsilon)} + \underbrace{P(u_k) \circ P'(u_k)^{-1}}_{=O\left(\varepsilon^{2^k}\right)} = O(\varepsilon).$$

Ces 3 propriétés sont donc vraies pour tout $k \in \mathbb{N}^*$. De ce fait, en notant $N = \lceil \log_2(\alpha) \rceil$, on a :

$$\varepsilon^{2^N} = 0.$$

En particulier, $P(u_N) = 0$ et donc $u_{N+1} = u_N$ et la suite (u_k) stationne donc à partir du rang N. En notant $s := u_N$, on a que $s \in k[u]$ et que $P(s) = 0$. s est donc annulé par un polynôme sans facteur carré (P). s est donc semi-simple et son polynôme minimal π_s divise P, donc divise π_u. En notant $n = u - s = u - u_N$, la propriété 3 nous dit que :

$$n = O(\varepsilon).$$

Ainsi, n est nilpotent, et on a également $n \in k[u]$ donc n commute avec s. Enfin, par définition, $u = s + n$. Cela termine donc la démonstration ! □

Tout cela est très bien, mais pour avoir une méthode complètement effective de calcul de la décomposition de Dunford/Jordan-Chevalley, il faut avoir une méthode effective du calcul du radical d'un polynôme ! Pas de soucis, ça existe ! En caractéristique 0, c'est le plus facile : lorsque $P \in k[X]$, le quotient :

$$\frac{P}{P \wedge P'}$$

donne directement le radical de P, et le pgcd peut-être calculé effectivement avec l'algorithme d'Euclide. En caractéristique $p > 0$, ça se corse un peu ! Mais l'algorithme rad suivant :

```
def rad(P):
    if deg(P) == 0:
        return 1
    else:
```

```
if deriv(P) == 0:
    S = P**(1/p)
    R = rad(S)
else:
    U = pgcd(P,deriv(P))
    V = P/U
    W = pgcd(U,V**(deg(P)-1))
    R = V*rad(U/W)
return R
```

permet de calculer effectivement le radical du polynôme P. Remarquez qu'on aura besoin de calculer une puissance $\frac{1}{p}$-ième, c'est-à-dire l'inverse du Frobenius. Si on est dans un corps fini de cardinal p^d, alors on a que cet inverse est simplement l'itérée $(d-1)$-uple du Frobenius. Dans les autres cas, je ne sais pas s'il exsite un calcul effectif de cette puissance $\frac{1}{p}$-ième. Montrons que cet algorithme retourne bien le radical d'un polynôme P. Si $\deg(P) = 0$, 1 convient. Si $P' = 0$, alors la prodécure fait baisser le degré d'un facteur p, et donc le degré décroît strictement. Si $P' \neq 0$, écrivons P comme produit de facteurs irréductibles :

$$P = \prod_{i=1}^{r} Q_i^{\alpha_i}.$$

Notons alors :

$$E = \prod_{i, p \nmid \alpha_i} Q_i^{\alpha_i}$$

et :

$$F = \prod_{i, p \mid \alpha_i} Q_i^{\alpha_i}$$

de sorte que $P = EF$ et E est non constant car $P' \neq 0$. Puisque $F' = 0$ (tous les exposants sont multiples de P). Ainsi :

$$P' = E'F,$$

de sorte que :

$$P \wedge P' = (E \wedge E')F$$

avec :

$$E \wedge E' = \prod_{i, p \nmid \alpha_i} Q_i^{\alpha_i - 1}.$$

En effet, ce calcul s'effectue comme en caractéristique 0 puisque tous les exposants sont non-nuls modulo p : si $E = Q^\alpha G$ avec Q irréductible et G premier avec Q, on a :

$$E' = Q^{\alpha-1}(\alpha Q' + QG')$$

et donc :

$$Q^{\alpha-1} \mid E'$$

mais :

$$Q^\alpha \nmid E'$$

car $\alpha \not\equiv 0\ [p]$ et $Q' \wedge Q = 1$ car k est parfait et Q est irréductible. À partir de là, on a :

$$U = P \wedge P' = \prod_{i, p \nmid \alpha_i} Q_i^{\alpha_i - 1} \prod_{i, p \mid \alpha_i} Q_i^{\alpha_i}$$

et donc :

$$V = \frac{P}{P \wedge P'} = \frac{E}{E \wedge E'} = \prod_{i, p \nmid \alpha_i} Q_i.$$

C'est un premier pas, mais il manque les facteurs Q_i tels que $p \mid \alpha_i$! C'est là qu'on remarque que, en notant $n := \deg(P)$, on a :

$$V^{n-1} = \prod_{i, p \nmid \alpha_i} Q_i^{n-1}.$$

Et donc, puisque $\alpha_i \leq n$ pour tout i :

$$W = U \wedge V^{n-1} = \prod_{i, p \nmid \alpha_i} Q_i^{\alpha_i - 1}$$

de sorte que :

$$\frac{U}{W} = \prod_{i, p \mid \alpha_i} Q_i^{\alpha_i}$$

et donc :

$$\mathrm{rad}(P) = V \times \mathrm{rad}\left(\frac{U}{W}\right).$$

Étant donné que $\deg\left(\frac{U}{W}\right) < \deg(P)$ l'algorithme termine et la relation des radicaux juste au-dessus permet de montrer qu'en fin d'algorithme, $F = 1$ et donc $R = V = \mathrm{rad}(P)$.