Corps de rupture et de décomposition - Polynômes symétriques

Salim Rostam

9 janvier 2019

Références : Escofier et Gozard (Théorie de Galois), Gourdon (algèbre), RDO 1, Ulmer (Anneaux, corps, résultants)

Soit k un corps (commutatif). Rappel : l'anneau $k[X]$ est euclidien donc principal donc factoriel.

1 Racines d'un polynôme

Définition. Soit $P \in k[X]$ et $a \in k$. On dit que a est *racine* de P si $P(a) = 0$.

Proposition. *Un polynôme non nul de degré n possède au plus n racines.*

Démonstration. Si a est une racine de P alors on peut faire la division euclidienne de P par a et on trouve que $X - a$ divise P. □

Remarque. L'énoncé devient faux si k est non commutatif, ou si k n'est qu'un anneau (même commutatif).

1.1 Corps de rupture

Une *extension* de k est la donnée d'un corps K et d'un morphisme de corps $\phi : k \to K$. En particulier, le morphisme ϕ envoie 1_k sur 1_K, donc est non nul donc injectif.

Soit $P \in k[X]$ irréductible.

Définition. Un *corps de rupture* pour P est une extension de k dans laquelle P possède une racine, l'extension étant minimale pour cette propriété.

Autrement dit, si K/k est un corps de rupture pour P alors P possède une racine $\alpha \in K$ et $K = k(\alpha)$. Réciproquement, si une extension K/k possède une racine $\alpha \in K$ de P alors $k(\alpha)$ est un corps de rupture.

Proposition. *Il existe un unique corps de rupture pour P à k-isomorphisme près.*

Démonstration. Puisque P est irréductible, l'idéal (P) est maximal : si I est un idéal contenant strictement (P) alors I contient un polynôme Q non constant non multiple de P, mais alors P et Q sont premiers entre eux d'où $1 \in I$. On vérifie alors que $k[X]/(P)$ est un corps de rupture : on a bien un plongement $k \hookrightarrow k[X]/(P)$, la classe x de X est une racine de P et $k[X]/(P) = k(x)$.

Remarque. Si P est de degré n alors $\{1, x, \dots, x^{n-1}\}$ est une k-base de $k[X]/(P)$.

Montrons maintenant l'unicité ; soit L/k un corps de rupture et soit $\alpha \in L$ une racine de P. Le polynôme P étant irréductible sur k, c'est le polynôme minimal de α sur k. Ainsi, le noyau du morphisme f de k-algèbres $k[X] \to L$ envoyant X sur α (un tel morphisme existe, par exemple par la propriété universelle des anneaux de polynômes) est $\{Q \in k[X] : Q(\alpha) = 0\} = \{Q \in k[X] : P \mid Q\} = (P)$ donc f se factorise en un morphisme injectif de k-algèbres $\overline{f} : k[X]/(P) \to L$. Mais les deux algèbres sont des corps et $L = k(\alpha)$ par définition donc $\overline{f}$ est surjectif (on a $\alpha = \overline{f}(X)$) donc $\overline{f}$ est un isomorphisme. □

Si K est un corps de rupture pour P, le polynôme P n'est pas nécessairement scindé sur K. Par exemple, un corps de rupture pour $X^3 - 2 \in \mathbb{Q}[X]$ est $\mathbb{Q}(\sqrt[3]{2})$ mais ce dernier ne contient pas la racine $j\sqrt[3]{2}$.

Remarque. On peut également parler de corps de rupture pour un polynôme non irréductible, mais dans ce cas on perd l'unicité. En outre, la construction ne fonctionne plus : on doit y remplacer P par un facteur irréductible.

1.2 Corps de décomposition

Soit $P \in k[X]$ (pas nécessairement irréductible !).

Définition. Un *corps de décomposition* pour P est une extension de k dans laquelle P est scindé, minimale pour cette propriété.

Autrement dit, si K/k est un corps de décomposition pour P alors $K = k(\alpha_1, \ldots, \alpha_n)$ où les α_i sont les racines de P dans K. Réciproquement, si K/k est une extension contenant toutes les racines $\alpha_1, \ldots, \alpha_n \in K$ de P (i.e. P est un multiple scalaire de $\prod_{i=1}^{n}(X - \alpha_i)$) alors $k(\alpha_1, \ldots, \alpha_n)$ est un corps de décomposition.

Proposition. *Il existe un unique corps de décomposition pour P à k-isomorphisme près.*

Démonstration. Montrons d'abord l'existence, par récurrence sur le degré de P. Si P est constant ou de degré 1 c'est bon ; on suppose $\deg P \geq 2$. Soit K un corps de rupture d'un facteur irréductible de P et soit $\alpha_1 \in K$ une racine de P. Notons que $K = k(\alpha_1)$. Soit $Q \in K[X]$ tel que $P = (X - \alpha_1)Q$. Par hypothèse, le polynôme Q possède un corps de décomposition $L = K(\alpha_2, \ldots, \alpha_n)$, où $\alpha_2, \ldots, \alpha_n$ sont les racines de Q. Mais alors $L = k(\alpha_1)(\alpha_2, \ldots, \alpha_n) = k(\alpha_1, \ldots, \alpha_n)$ est bien un corps de décomposition pour P.

Montrons maintenant l'unicité. Encore une fois nous allons procéder par récurrence sur le degré de P. Si P est de degré 1 le résultat est clair car un corps de rupture est un corps de décomposition. On suppose maintenant $\deg P \geq 2$. Soit k' un corps isomorphe à k via θ et soit Q un facteur irréductible de P. Le plongement θ se prolonge de façon unique en un isomorphisme de corps $k[X]/(Q) \simeq k'[X]/(\theta(Q))$ fixant X (remarquons que $\theta(Q)$ est bien irréductible sur k' !). Soit maintenant K (resp. L) un corps de décomposition de $P \in k[X]$ sur k (resp. de $\theta(P) \in k'[X]$ sur k'). Soit α (resp. β) une racine de Q dans K (resp. de $\theta(Q)$ dans L) qui n'est pas dans k (resp. k'). Par la remarque précédente, on a $k(\alpha) \simeq k[X]/(Q) \simeq k'[X]/(\theta(Q)) \simeq k'(\beta)$. De plus, l'isomorphisme $\widehat{\theta} : k(\alpha) \xrightarrow{\sim} k'(\beta)$ prolonge θ et envoie α sur β. On a la situation suivante :

$$\begin{array}{ccc} K & & L \\ | & & | \\ k(\alpha) & \simeq & k'(\beta) \\ | & & | \\ k & \simeq & k' \end{array}$$

Finalement, écrivons $P = (X - \alpha)R$ et $\theta(P) = (X - \beta)S$ avec $R \in k(\alpha)[X]$ et $S \in k'(\beta)[X]$. Puisque $\widehat{\alpha} = \beta$ on a en fait $S = \widehat{\theta}(R)$. De plus, le corps K (resp. L) est un corps de décomposition

pour R (resp. S), car il est engendré sur $k(\alpha)$ (resp. $k'(\beta)$) par les racines de R (resp. S). Par hypothèse de récurrence, il existe donc un isomorphisme $K \simeq L$ qui prolonge $k(\alpha) \simeq k'(\beta)$ et qui prolonge donc $k \simeq k'$. On conclut en prenant $k = k'$ et $\theta = \mathrm{id}_k$. □

La construction implique que si K/k est un corps de décomposition pour P de degré n alors $[K : k] \leq n!$.

Application. Existence et unicité du corps fini à p^n éléments.

1.3 Clôture algébrique

Cette partie est hors programme mais bonne à savoir !

Définition. Un corps K est *algébriquement clos* si tout polynôme à coefficients dans K est scindé.

Définition. Une *clôture algébrique* de k est une extension à la fois algébrique sur k et algébriquement close.

Théorème (Steiniz)**.** *Il existe une unique clôture algébrique à k-isomorphisme près.*

On peut par exemple montrer ce théorème en utilisant le lemme de Zorn (Artin a donné une démonstration utilisant « plus simplement » l'existence d'un idéal maximal). Cependant, on a la version plus faible suivante.

Proposition. *Soit K/k une extension algébriquement close. Alors il existe une* unique *clôture algébrique de k dans K.*

Démonstration. **Existence** On considère l'ensemble L des éléments de K algébriques sur k. C'est un corps, et c'est même une extension algébrique de k. Si maintenant $P \in L[X]$ est non constant, toute racine dans K est algébrique sur L donc algébrique sur k (on peut écrire $P \in M[X]$ où M est l'extension finie de k engendrée par les coefficients de P, ainsi une racine de P engendre un corps de degré fini sur M donc de degré fini sur k) donc est dans L. Ainsi L est bien une clôture algébrique de k dans K.

Unicité Soit M une extension intermédiaire entre k et K, à la fois algébriquement close et algébrique sur k. Par définition de L on a $M \subseteq L$. Soit maintenant $x \in L$ et soit P son polynôme minimal sur k. Puisque L et M sont deux clôtures algébriques de k dans K, le polynôme P est scindé sur K et toutes ses racines sont dans L et dans M. Puisque x est une racine de P on en déduit que $x \in M$.

□

2 Polynômes symétriques

Le groupe symétrique $\mathfrak{S}_n$ agit sur $k[x_1, \ldots, x_n]$ par permutation des variables.

Exercice. L'action donnée par $(\sigma, x_i) \mapsto x_{\sigma(i)}$ est-elle une action à gauche ou une action à droite ?

Définition. Un polynôme $P \in k[x_1, \ldots, x_n]$ est dit *symétrique* s'il est un point fixe pour cette action. On note $\Lambda_n \coloneqq k[x_1, \ldots, x_n]^{\mathfrak{S}_n}$ la sous-algèbre fixée.

Un exemple de fonction symétrique est le *d-ième polynôme symétrique élémentaire*

$$\sigma_d(x_1, \ldots, x_n) \coloneqq \sum_{1 \leq i_1 < \cdots < i_d \leq n} x_{i_1} \cdots x_{i_d} \in \Lambda_n,$$

pour $d \in \{1, \dots, n\}$. C'est un polynôme (symétrique) homogène de degré (total) d. On a la « relation coefficients-racines » :

$$\prod_{d=1}^{n}(x - x_r) = x^n + \sum_{d=0}^{n-1}(-1)^{n-d}\sigma_{n-d}(x_1, \dots, x_n)x^d.$$

Théorème. *Tout polynôme symétrique s'écrit de façon unique sous la forme $Q(\sigma_1, \dots, \sigma_n)$ avec $Q \in k[y_1, \dots, y_n]$.*

Remarque. Le Théorème reste vrai si k est un anneau commutatif.

Il faut connaitre, bien sûr ce théorème, mais également une façon de trouver le polynôme Q ! Si P est un polynôme symétrique, on regarde le monôme de plus grand degré pour l'ordre lexicographique, de coefficient $\alpha \in k^\times$. Si ce degré est $a = (a_1, \dots, a_n)$, on considère alors $\widetilde{P} \coloneqq P - \alpha\sigma_1^{a_1-a_2} \cdots \sigma_{n-1}^{a_{n-1}-a_n}\sigma_n^{a_n}$. Le monôme de degré a a bien disparu dans $\widetilde{P}$, et comme il n'y a pas de monôme plus grand qui puisse apparaître on peut réappliquer la procédure à $\widetilde{P}$.

Une démonstration classique du théorème est, étant donnée un polynôme $P \in k[x_1, \dots, x_n]$ symétrique, considérer le polynôme symétrique $P(x_1, \dots, x_{n-1}, 0)$ et raisonner par récurrence (voir par exemple RDO 1). On va présenter ici une preuve moins constructive mais plus conceptuelle, que l'on peut trouver dans le livre de I. G. Macdonald « *Symmetric Functions and Hall Polynomials* ».

Rappelons qu'une *partition* d'un entier N est une suite finie $\lambda = (\lambda_1 \geq \cdots \geq \lambda_h > 0)$ décroissante (au sens large) d'entiers naturels non nuls de somme $N =: |\lambda|$. La *hauteur* de λ est l'entier $h =: h(\lambda)$. Si $\lambda = (\lambda_1, \dots, \lambda_h)$ est une partition de hauteur $h \leq n$, que l'on complète en un n-uplet en posant $\lambda_i \coloneqq 0$ pour $i \in \{h+1, \dots, n\}$, on définit

$$m_\lambda(x_1, \dots, x_n) \coloneqq \sum_{\alpha \in \mathfrak{S}_n \cdot \lambda} x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in \Lambda_n,$$

où $\mathfrak{S}_n \cdot \lambda$ désigne l'orbite de $(\lambda_1, \dots, \lambda_n)$ pour l'action de $\mathfrak{S}_n$ sur les n-uplets.

Remarque.
- Soit $d \in \{1, \dots, n\}$. Si (1^d) désigne la partition $(\underbrace{1, \dots, 1}_{d \text{ fois}})$ alors $m_{(1^d)}(x_1, \dots, x_n) = \sigma_d(x_1, \dots, x_n)$.
- Le polynôme m_λ est (symétrique) homogène de degré (total) $|\lambda|$.

Lemme. *La famille $\{m_\lambda\}_{h(\lambda) \leq n}$ est une k-base de Λ_n.*

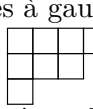
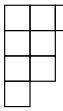
Démonstration. Tout d'abord, la famille est bien libre car la sous-famille constituée des termes dominants pour l'ordre lexicographique (les $x_1^{\lambda_1} \cdots x_n^{\lambda_n}$) est échelonnée. Si maintenant $P \in \Lambda_n$ est un polynôme symétrique, si $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ est un monôme de P avec coefficient $\alpha \in k^\times$ alors il existe une partition λ de hauteur au plus n telle que $\alpha \in \mathfrak{S}_n \cdot \lambda$ (on trie !). Exactement tous les termes de αm_λ apparaissent dans P, puisque P est symétrique, et $P - \alpha m_\lambda$ est un polynôme symétrique avec strictement moins de termes que P. On récurre. □

Si λ est une partition vérifiant $\lambda_1 \leq n$, on définit

$$\sigma_\lambda \coloneqq \sigma_{\lambda_1} \cdots \sigma_{\lambda_h} \in \Lambda_n.$$

C'est un polynôme (symétrique) homogène de degré (total) $|\lambda|$. On veut exprimer σ_λ sur la base des m_μ pour $h(\mu) \leq n$.

Définition. Soit $\lambda = (\lambda_1 \geq \dots)$ une partition. On définit la partition *conjuguée* λ' par $\lambda'_i \coloneqq \#\{j : \lambda_j \geq i\}$.

Graphiquement, on peut représenter λ par un *diagramme de Young*, c'est-à-dire, une série de boîtes justifiées à gauche représentant les parts de λ. Par exemple, la partition $\lambda \coloneqq (4,3,1)$ se représente par  : on a $\lambda_1 = 4$ cases sur la première ligne, $\lambda_2 = 3$ sur la deuxième et $\lambda_3 = 1$ sur la troisième. La partition conjuguée s'obtient en regardant le nombre de boîtes sur les colonnes (ou en renversant le diagramme par rapport à la diagonale), ici $\lambda' = (3,2,2,1)$ est  .

Remarque.
- On a $h(\lambda') = \lambda_1$. En particulier, la conjugaison réalise une bijection entre les partitions de première part n (resp. $\leq n$) et les partitions de hauteur n (resp. $\leq n$).
- On a $\lambda'' = \lambda$, en particulier $h(\lambda) = \lambda'_1$.

Proposition. *Soit λ une partition vérifiant $h(\lambda) \leq n$. Il existe des (uniques) scalaires $a_{\lambda,\mu} \in k$ tels que*

$$\sigma_{\lambda'}(x_1, \dots, x_n) = m_\lambda(x_1, \dots, x_n) + \sum_{\substack{h(\mu) \leq n \\ \mu < \lambda}} a_{\lambda,\mu} m_\mu(x_1, \dots, x_n).$$

Remarque. On a $\lambda'_1 = h(\lambda) \leq n$ donc $\sigma_{\lambda'}(x_1, \dots, x_n)$ est bien définie.

L'ordre dont il est question est l'ordre lexicographique. On a en fait un résultat plus fort puisque la proposition reste vraie avec l'ordre (partiel) $\lhd$ de *dominance* sur les partitions, plus fin que l'ordre lexicographique (autrement dit $\lambda \lhd \mu \implies \lambda < \mu$).

Démonstration. L'unicité est claire par le Lemme. Pour l'existence, on va simplement regarder quels monômes apparaissent lorsque l'on développe $\sigma_{\lambda'}(x_1, \dots, x_n)$. Ce sont les

$$\left(x_{i_1^{(1)}} \cdots x_{i_{\lambda'_1}^{(1)}}\right) \cdots \left(x_{i_1^{(h)}} \cdots x_{i_{\lambda'_h}^{(h)}}\right),$$

où h est la hauteur de λ' et $1 \leq i_1^{(j)} < \cdots < i_{\lambda'_j}^{(j)} \leq n$ pour tout $j \in \{1, \dots, n\}$. Soit $\alpha \in \mathbb{N}^n$ tel que le monôme précédent s'écrive $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. On désire montrer que $\alpha \leq \lambda$ pour l'ordre lexicographique. Pour cela, remplissons le diagramme de Young de λ de la façon suivante : pour $j \in \{1, \dots, h(\lambda')\}$ (rappelons que $h(\lambda') = \lambda_1$), on remplit la colonne j de haut en bas par les $i_k^{(j)}$ pour k allant de 1 à λ'_j. Sur l'exemple précédent de la partition $\lambda = (4,3,1)$, cela donne

$i_1^{(1)}$	$i_1^{(2)}$	$i_1^{(3)}$	$i_1^{(4)}$
$i_2^{(1)}$	$i_2^{(2)}$	$i_2^{(3)}$	
$i_3^{(1)}$			

Comptons maintenant le nombre de 1 parmi les $i_k^{(j)}$. Par définition de α ils sont exactement α_1, de plus ils apparaissent nécessairement dans la première ligne du tableau (car les entiers sont strictement croissants suivant les colonnes par définition). Puisqu'il y a exactement λ_1 cases dans la première ligne du tableau, on en déduit qu'il y a au plus λ_1 fois l'entier 1 dans la première ligne et donc dans tout le tableau, d'où

$$\alpha_1 \leq \lambda_1.$$

Comptons maintenant le nombre de 1 et 2. Pour la même raison de stricte croissance que précédemment, ils ne peuvent apparaître que dans les deux premières lignes du tableau, qui contiennent exactement $\lambda_1 + \lambda_2$ cases. Mais on sait que les entiers 1 et 2 apparait exactement $\alpha_1\alpha_2$ fois, par définition de α (il y a α_1 fois 1 et α_2 fois 2). On a donc

$$\alpha_1 + \alpha_2 \leq \lambda_1 + \lambda_2.$$

On continue jusqu'à la dernière ligne du tableau, éventuellement vide (i.e. on a complété λ en une part nulle) pour laquelle on trouve

$$\alpha_1 + \cdots + \alpha_n \leq \lambda_1 + \cdots + \lambda_n.$$

Remarque. L'*ensemble* des inégalités précédentes définit exactement la relation de dominance $\alpha \trianglelefteq \lambda$. Cependant, on voit qu'elles impliquent bien $\alpha \leq \lambda$ pour l'ordre lexicographique.

Puisque $\sigma_{\lambda'}(x_1, \ldots, x_n)$ est symétrique, le monôme $x^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ y apparait si et seulement si $x^{\sigma\cdot\alpha}$ y apparait, pour chaque $\sigma \in \mathfrak{S}_n$. De plus, le raisonnement précédent assure que l'on a encore $\sigma \cdot \alpha \leq \lambda$. Finalement, si μ désigne le n-uplet α trié dans l'ordre décroissant alors μ est une partition et $\mu \leq \lambda$.

On obtient donc l'égalité proposée. On a bien $a_{\lambda,\lambda} = 1$ puisque le monôme x^λ, et donc m_λ, est atteint une unique fois : lorsque $i_k^{(j)} = k$ pour tout j, k (sur l'exemple, cela donne $\begin{array}{|c|c|c|}\hline 1&1&1\\\hline 2&2&2\\\hline 3\\\cline{1-1}\end{array}$).

□

Remarque. Les partitions de la forme (1^d) étant minimales pour $<$, on retrouve bien le résultat remarqué auparavant $\sigma_d(x_1, \ldots, x_n) = m_{(1^d)}(x_1, \ldots, x_n)$ (les partitions $(1^{d'})$ avec $d' < d$ n'apparaissent pas pour des raisons de degré total). En effet, la partition conjuguée de (1^d) est (d) (partition constituée d'une seule part, égale à d).

Par la Proposition, la famille $(\sigma_{\lambda'})_{h(\lambda)\leq n} = (\sigma_\lambda)_{\lambda_1 \leq n}$ s'exprime via une matrice triangulaire inversible en fonction de la famille $(m_\lambda)_{h(\lambda)\leq n}$, où l'on a pris soin de ranger les partitions dans l'ordre lexicographique. Par le Lemme, la famille $(\sigma_\lambda)_{\lambda_1\leq n}$ est donc également une k-base de Λ_n. On en déduit donc le Théorème. En effet, si $P \in \Lambda_n$ est un polynôme symétrique alors il s'écrit $P = \sum_{\lambda_1\leq n} p_\lambda \sigma_\lambda$ qui est bien de la forme voulue. Réciproquement, soit $P = Q(\sigma_1, \ldots, \sigma_n)$ avec $Q(y) = \sum_{\alpha\in\mathbb{N}^n} q_\alpha y^\alpha$. On veut écrire

$$P = Q(\sigma_1, \ldots, \sigma_n) = \sum_{\alpha\in\mathbb{N}^n} q_\alpha \sigma_1^{\alpha_1} \cdots \sigma_n^{\alpha_n},$$

en fonction des σ_λ. On va faire un changement de variable : soit $\phi : \{\lambda\}_{\lambda_1\leq n} \to \mathbb{N}^n$ l'application qui à une partition λ vérifiant $\lambda_1 \leq n$ associe le vecteur $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ des multiplicités : l'entier i apparait exactement α_i fois dans λ (remarquons que la hauteur de λ devient la somme des composantes de α). L'application ϕ est bijective, d'inverse l'application qui à $\alpha \in \mathbb{N}^n$ associe la partition où chaque $i \in \{1, \ldots, n\}$ apparait exactement α_i fois. Remarquons que si $\alpha = \phi(\lambda)$ avec λ de hauteur h alors

$$\sigma_1^{\alpha_1} \cdots \sigma_n^{\alpha_n} = \sigma_{\lambda_1} \ldots \sigma_{\lambda_h} = \sigma_\lambda.$$

Ainsi, on obtient

$$P = Q(\sigma_1, \ldots, \sigma_n) = \sum_{\alpha\in\mathbb{N}^n} q_\alpha \sigma_1^{\alpha_1} \cdots \sigma_n^{\alpha_n} = \sum_{\lambda_1\leq n} q_{\phi(\lambda)} \sigma_\lambda,$$

donc les $q_{\phi(\lambda)}$ sont uniquement déterminés par P donc Q est entièrement déterminé par P.

Application (Oraux X-ENS, algèbre 1)**.** Théorème de Kronecker : si $P \in \mathbb{Z}[X]$ est unitaire dont les racines complexes z vérifient $|z| \leq 1$. Alors les racines non nulles de P sont des racines de l'unité.

On suppose que $X \nmid P$. À l'aide de la relation coefficients-racines, on montre qu'il n'y a qu'un nombre fini de tels polynômes P. Ensuite, si $P = \prod_{i=1}^{n}(X - \alpha_k)$, pour chaque $m \in \mathbb{N}^*$ on définit $P_m \coloneqq \prod_{i=1}^{n}(X - \alpha_k^m)$. Puisque P est à coefficients dans $\mathbb{Z}$, on a $\sigma_d(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$ pour tout d. Pour chaque $m \in \mathbb{N}^*$, le polynôme $\sigma_d(x_1^m, \ldots, x_n^m) \in \mathbb{Z}[x_1, \ldots, x_n]$ est symétrique donc s'exprime comme un polynôme *à coefficients entiers* en les $\sigma_e(x_1, \ldots, x_n)$, pour $e \in \{1, \ldots, n\}$. On en déduit que $\sigma_d(\alpha_1^m, \ldots, \alpha_n^m)$ est un entier et donc que P_m est à coefficients entiers pour tout m. On conclut.

Remarque. Il y a d'autres façons d'obtenir $P_m \in \mathbb{Z}[X]$. Par exemple en utilisant le résultant, ou alors les puissances de la matrice compagnon associée à P (sans doute la plus simple).