Sur les Résultants cycliques

Par Jean-Paul BÉZIVIN

Université de Caen, Département de Mathématiques et Mécanique, Laboratoire N.Oresme, Campus II, Boulevard du Maréchal Juin, BP 5186, 14032 Caen Cedex, France.

(Communicated by Heisuke HIRONAKA, M.J.A., Oct. 12, 2007)

Résumé: Let P be a non constant polynomial. For $n \geq 1$, the n-th cyclic resultant of P is the resultant of P and of $x^n - 1$. C.Hillar has proven a general result giving conditions on two polynomials to have the same set of non zero cyclic resultants. In this note, we give an alternative elementary proof of C.Hillar's theorem.

Key words: Cyclic resultant; recurring sequences; polynomials.

1. Introduction et résultats. Dans cette note, nous allons revenir sur un sujet introduit par D.Fried dans [1] qui est celui des résultants cycliques.

Soit K un corps commutatif de caractéristique nulle, que l'on peut supposer algébriquement clos, et $P(X) = a_0 \prod_{i=1}^{d}(X - \lambda_i)$ un polynôme non nul à coefficients dans K. On note $r_n(P)$ le résultant de P et de $X^n - 1$ pour $n \geq 1$:

$$r_n(P) = \mathrm{Res}(P, X^n - 1).$$

On appelle cette suite la suite des *résultants cycliques* de P.

On a immédiatement la formule $r_n(P) = a_0^n \prod_{i=1}^{d}(\lambda_i^n - 1)$. Dans toute la suite, on va supposer que les polynômes considérés n'ont pas de racines qui soient des racines de l'unité.

Le problème posé est de savoir dans quelle mesure la donnée des $r_n(P)$ pour $n \geq 1$ caractérise le polynôme P.

Dans [1], D.Fried donne une réponse partielle à cette question dans le cas de polynômes réciproques à coefficients réels.

Dans [2], C.Hillar reprend la question, et démontre le résultat général suivant :

Théorème 1.1 (C.Hillar)**.** *Soient f et g deux polynômes de $\mathbf{C}[x]$ n'ayant pas comme zéros de racines de l'unité. Alors f et g engendrent la même suite de résultants cycliques si et seulement si il existe $u, v \in \mathbf{C}[x]$ avec $u(0) \neq 0$, et des entiers naturels l_1, l_2 tels que* $\deg(u) \equiv l_2 - l_1 (\mathrm{mod}\ 2)$*, et*

$$f(x) = (-1)^{l_2 - l_1} x^{l_1} v(x) u(x^{-1}) x^{\deg(u)}$$
$$g(x) = x^{l_2} v(x) u(x)$$

On dira qu'un polynôme $P(x) = \prod_{i=1}^{d}(X - \lambda_i)$ est générique, si les λ_i ne sont pas des racines de l'unité, et si la condition suivante est satisfaite. Notons pour S partie de $\{1, \cdots, d\}$ par λ_S le produit $\prod_{i \in S} \lambda_i$, avec la convention que si S est vide, $\lambda_S = 1$.

On demande alors que pour S et T parties distinctes de $\{1, \cdots, d\}$, on ait $\lambda_S \neq \lambda_T$.

Dans le cas particulier où l'on suppose que les deux polynômes f et g sont unitaires et génériques, il résulte du théorème de C.Hillar que si $r_n(f) = r_n(g)$ pour tout $n \geq 1$, alors $f = g$.

Dans cet article, nous allons redémontrer le théorème de C.Hillar par des méthodes différentes que celles utilisées dans [1] et [2], et assez élémentaires.

Les propriétés des résultants cycliques interviennent dans différents domaines, comme par exemple dans le dénombrement des points périodiques des endomorphismes du tore. Nous renvoyons le lecteur à [3] pour d'autres renseignements et des références pour l'utilisation de ces résultats dans divers domaines.

D'autre part, nous allons nous contenter de démontrer le résultat suivant :

Théorème 1.2. *Soit K un corps commutatif de caractéristique nulle. Soient $P(X) = a_0(X - \lambda_1) \ldots (X - \lambda_d)$ et $Q(X) = b_0(X - \mu_1) \ldots (X - \mu_{d'})$ deux polynômes à coefficients dans K, les racines λ_i étant dans K non nulles, ainsi que les μ_j; on suppose qu'aucune de ces racines n'est une racine de l'unité.*

1) On suppose que $\mathrm{Res}(P, X^n - 1) = \mathrm{Res}(Q, X^n - 1)$ *pour tout $n \geq 1$. Alors il existe deux*

2000 Mathematics Subject Classification. Primary 11B37, 11B83.

©2007 The Japan Academy

polynômes U et V, avec U de degré pair, tels que si on note U^* le polynôme réciproque de U, on a $P(X) = V(X)U^*(X)$ et $Q(X) = V(X)U(X)$.

2) *On suppose que* $\mathrm{Res}(P, X^n - 1) = -\mathrm{Res}(Q, X^n - 1)$ *pour tout $n \geq 1$. Alors il existe deux polynômes U et V, avec U de degré impair, tels que si on note U^* le polynôme réciproque de U, on a $P(X) = -V(X)U^*(X)$ et $Q(X) = V(X)U(X)$.*

En effet, on voit facilement que l'on peut supposer que les polynômes considérés n'ont pas de racines nulles, et que la partie 1) du résultat précédent est alors équivalente au théorème de C.Hillar ; d'autre part, le fait que si les conditions sur les polynômes sont satisfaites, alors on a l'égalité des suites de résultants cycliques est facile.

2. Un lemme préliminaire.

Lemme 2.1. *Soit K un corps commutatif de caractéristique nulle (que l'on peut supposer contenir $\mathbf{Q}$), et S une famille finie d'éléments non nuls de K, aucun n'étant une racine de l'unité. On note L le corps engendré sur $\mathbf{Q}$ par les éléments de S. Alors on peut toujours trouver un sous-corps M d'un des corps $\mathbf{C}$ ou $\mathbf{C}_p$, p premier, isomorphe à L tel que l'un des éléments de S ait une image dans M de module différente de* 1.

Démonstration. Comme L est un corps de type fini sur $\mathbf{Q}$, on peut le considérer comme sous-corps de $\mathbf{C}$. Supposons qu'il y ait un élément λ de S qui est trancendant sur $\mathbf{Q}$. Dans ce cas, on peut trouver une base de transcendance de L sur $\mathbf{Q}$ contenant λ, donc L sera de la forme $\mathbf{Q}(t_1, \ldots, t_m)[\alpha]$ avec α algébrique sur $\mathbf{Q}(t_1, \ldots, t_m)$, avec $t_1 = \lambda$. Notons $P(t_1, \ldots, t_m, X)$ le polynôme minimal de α sur $\mathbf{Q}(t_1, \ldots, t_m)$. Si l'on choisit un élément r_1 de $\mathbf{C}$ transcendant sur $\mathbf{Q}$ de module < 1, des éléments $r_2, \ldots, r_m$ tels que $r_1, \ldots, r_m$ soient algébriquement indépendants, et β une racine dans $\mathbf{C}$ de $P(r_1, \ldots, r_m)[X]$, on peut prendre $M = \mathbf{Q}(r_1, \ldots, r_m)[\beta]$.

Il reste à voir le cas où tous les éléments de S sont algébriques sur $\mathbf{Q}$. Considérons λ quelconque dans S. Si pour tous les plongements possibles de λ dans un des corps $\mathbf{C}_p$ on trouve un élément de module 1, alors λ est un entier algébrique sur $\mathbf{Z}$. Si de plus tous les conjugués de λ sont de module 1, un résultat bien connu de Kronecker dit que λ est une racine de l'unité, ce qui n'est pas, et termine la démonstration. □

3. Deux cas particuliers du théorème 1.2. Nous allons tout d'abord démontrer le résultat dans deux cas particuliers.

Dans le premier de ces deux cas, nous allons utiliser une idée introduite par K.Kedlaya [4; §8].

Proposition 3.1. *On note K le corps $\mathbf{C}$ ou l'un des corps $\mathbf{C}_p$, p premier, munis de leur valeur absolue usuelle, que nous notons $|.|$. Soient $P(X) = (X - \lambda_1) \ldots (X - \lambda_d)$ et $Q(X) = (X - \mu_1) \ldots (X - \mu_{d'})$ deux polynômes à coefficients dans K, les racines λ_i étant non nulles, ainsi que les μ_j ; on suppose que toutes ces quantités sont de modules < 1.*

On suppose que $\prod_{i=1}^{d}(1 - \lambda_i^n) = \prod_{j=1}^{d'}(1 - \mu_j^n)$ *pour tout $n \geq 1$. Alors on a $P = Q$.*

Démonstration. Que ce soit dans $\mathbf{C}$ ou $\mathbf{C}_p$, la fonction $\log(1 + x)$ est définie, analytique et vérifie l'équation fonctionnelle usuelle dans un disque $B(0, r) = \{x; |x| < r\}$. Posons

$$a_n = -\frac{1}{n} \log\left(\prod_{i=1}^{d}(1 - \lambda_i^n)\right) = \sum_{k \geq 1} \sum_{i=1}^{d} \frac{\lambda_i^{nk}}{nk}.$$

Si on pose $b_n = \sum_{i=1}^{d} \frac{\lambda_i^n}{n}$, on a obtenu que $a_n = \sum_{k \geq 1} b_{nk}$ pour tout n assez grand. Par inversion de Moebius, toutes les séries considérées étant absolument convergentes, on a $b_n = \sum_{k \geq 1} \mu(k) a_{nk}$ pour tout $n \geq 1$. On fait de même pour le polynôme Q; on a $a_n = -\frac{1}{n} \log(\prod_{i=1}^{d'}(1 - \mu_i^n))$, d'où en notant $c_n = \sum_{j=1}^{d'} \frac{\mu_j^n}{n}$, on obtient que $c_n = \sum_{k \geq 1} \mu(k) a_{nk} = b_n$. Comme $\alpha_n = nb_n = \sum_{i=1}^{d} \lambda_i^n$ et $\beta_n = nc_n = \sum_{j=1}^{d'} \mu_j^n$ sont des suites récurrentes linéaires (et que les λ_i et μ_j sont non nuls), l'égalité $\alpha_n = \beta_n$ vraie si n est assez grand est en fait vraie pour tout n ; pour $n = 0$, on obtient que $d = d'$. Ces égalités impliquent alors par les formules de Newton que $P = Q$. □

Nous passons au second cas particulier :

Proposition 3.2. *On note K le corps $\mathbf{C}$ ou l'un des corps $\mathbf{C}_p$, p premier, munis de leur valeur absolue usuelle, que nous notons $|.|$. Soient $P(X) = a_0(X - \lambda_1) \ldots (X - \lambda_d)$ et $Q(X) = b_0(X - \mu_1) \ldots (X - \mu_{d'})$ deux polynômes à coefficients et racines dans K, les racines λ_i étant non nulles, ainsi que les μ_j ; on suppose qu'aucune de ces racines n'est de module* 1.

1) *On suppose que* $\mathrm{Res}(P, X^n - 1) = \mathrm{Res}(Q, X^n - 1)$ *pour tout $n \geq 1$. Alors il existe deux*

polynômes U et V, avec U de degré pair, tels que si on note U^* le polynôme réciproque de U, on a $P(X) = V(X)U^*(X)$ et $Q(X) = V(X)U(X)$.

2) *On suppose que* $\mathrm{Res}(P, X^n - 1) = -\mathrm{Res}(Q, X^n - 1)$ *pour tout $n \geq 1$. Alors il existe deux polynômes U et V, avec U de degré impair, tels que si on note U^* le polynôme réciproque de U, on a $P(X) = -V(X)U^*(X)$ et $Q(X) = V(X)U(X)$.*

Démonstration. On note de manière générale E_1 l'ensemble des indices i tels que $|\lambda_i| < 1$, E_2 l'ensemble des indices i tels que $|\lambda_i| = 1$, E_3 l'ensemble des indices i tels que $|\lambda_i| > 1$, et de même F_1 l'ensemble des indices j tels que $|\mu_j| < 1$, F_2 l'ensemble des indices j tels que $|\mu_j| = 1$, F_3 l'ensemble des indices j tels que $|\mu_j| > 1$. Certains de ces ensembles peuvent être vides. Pour des produits fait sur un ensemble d'indice vide, nous utilisons la convention qu'il est égal à 1. Dans notre énoncé, les ensembles E_2 et F_2 sont vides.

On a $r_n(P) = a_0^n \prod_{i=1}^{d}(\lambda_i^n - 1)$ qui est égal à $(-1)^{e_1}(a_0\theta_1)^n A_n C_n$, avec $\theta_1 = \prod_{i\in E_3} \lambda_i$, $A_n = \prod_{i\in E_1}(1 - \lambda_i^n)$, et $C_n = \prod_{i\in E_3}(1 - \lambda_i^{-n})$, et e_1 est le cardinal de E_1.

De même, $r_n(Q) = b_0^n \prod_{j=1}^{d'}(\mu_j^n - 1)$ s'écrit $(-1)^{f_1}(b_0\theta_2)^n A_n^* C_n^*$, avec $\theta_2 = \prod_{i\in F_3} \mu_i$, $A_n^* = \prod_{i\in F_1}(1 - \mu_i^n)$, et $C_n^* = \prod_{i\in F_3}(1 - \mu_i^{-n})$, et f_1 est le cardinal de F_1.

On note que par les hypothèses faites, les suites A_n, A_n^*, C_n, C_n^* ont toutes pour limite 1 si $n \to +\infty$.

D'autre part, on a $r_n(P) = (-1)^{\varepsilon} r_n(Q)$ pour tout n, où $\varepsilon = 0$ ou 1 suivant que l'on se trouve dans le premier cas ou dans le second. On peut donc écrire en notant $\theta = \dfrac{a_0\theta_1}{b_0\theta_2}$ que

$$\theta^n = (-1)^{-e_1+f_1+\varepsilon} \frac{A_n^* C_n^*}{A_n C_n}.$$

Il en résulte que θ^n admet comme limite $(-1)^{-e_1+f_1+\varepsilon}$ si n tend vers l'infini, et donc $\theta = 1$, $a_0\theta_1 = b_0\theta_2$, et e_1 est de même parité que $f_1 + \varepsilon$. On a $A_n C_n = A_n^* C_n^*$ pour tout $n \geq 1$. Par la proposition 3.1 les polynômes $\prod_{i\in E_1}(X - \lambda_i) \prod_{i\in E_3}(X - \lambda_i^{-1})$ et $\prod_{i\in F_1}(X - \mu_i) \prod_{i\in F_3}(X - \mu_i^{-1})$ sont égaux. On peut en réindexant les λ_i et les μ_j, trouver une partie E et une partie F partition de l'ensemble d'indices tels que $\lambda_i = \mu_i$ si $i \in E$ et $\lambda_i = \mu_i^{-1}$ si $i \in F$.

Posons $V(X) = b_0 \prod_{i\in E}(X - \mu_i)$, $U(X) = \prod_{i\in F}(X - \mu_i)$, de sorte que $U(X)V(X) = Q(X)$. Le polynôme réciproque $U^*(X)$ de $U(X)$ est égal à $\dfrac{(-1)^f}{\prod_{i\in F}\lambda_i} \prod_{i\in F}(X - \lambda_i)$, où f est le cardinal de F. On peut réécrire les relations de départ, qui donnent après simplification par $\prod_{i\in E}(\lambda_i^n - 1)$ que la quantité

$$a_0^n \prod_{i\in F}(\lambda_i^n - 1) = (-1)^{\varepsilon} b_0^n \prod_{i\in F}(\mu_i^n - 1)$$

est égale à

$$b_0^n (-1)^{f+\varepsilon} \left(\prod_{i\in F} \lambda_i^{-1}\right)^n \prod_{i\in F}(\lambda_i^n - 1)$$

et on trouve que $a_0^n = b_0^n (-1)^{f+\varepsilon} (\prod_{i\in F} \lambda_i^{-1})^n$ pour tout $n \geq 1$, donc pour tout n. On en déduit que $f + \varepsilon$ est pair, et que $a_0 = b_0 (-1)^{f+\varepsilon} (\prod_{i\in F} \lambda_i^{-1})$. On a alors que

$$\begin{aligned} U^*(X)V(X) &= \frac{b_0(-1)^{f+\varepsilon}}{\prod_{i\in F}\lambda_i} \prod_{i\in E\cup F}(X - \lambda_i) \\ &= (-1)^{\varepsilon} P(X) \end{aligned}$$

et comme le degré de U est le nombre f, ce degré est pair si $\varepsilon = 0$, et impair si $\varepsilon = 1$. □

4. Démonstration du théorème 1.2. Nous allons procéder par récurrence sur $m = d + d'$; il est clair que le résultat est valide pour les petites valeurs de m.

D'après le lemme 2.1, on peut supposer, quitte à se placer dans le corps $\mathbf{C}$ ou un corps $\mathbf{C}_p$ convenable, que λ_1 est de module différent de 1. Si tous les λ_i et tous les μ_j sont de module différents de 1, le résultat découle de la proposition 3.2. Nous pouvons donc supposer qu'il existe soit un des λ_i de module 1, soit un des μ_j de module 1.

On a $r_n(P) = a_0^n \prod_{i=1}^{d}(\lambda_i^n - 1)$ qui est égal à $(-1)^{e_1}(a_0\theta_1)^n A_n B_n C_n$, avec $\theta_1 = \prod_{i\in E_3} \lambda_i$, $A_n = \prod_{i\in E_1}(1 - \lambda_i^n)$, $B_n = \prod_{i\in E_2}(\lambda_i^n - 1)$ et $C_n = \prod_{i\in E_3}(1 - \lambda_i^{-n})$, et e_1 est le cardinal de E_1.

De même, $r_n(Q) = b_0^n \prod_{j=1}^{d'}(\mu_j^n - 1)$ s'écrit $(-1)^{f_1}(b_0\theta_2)^n A_n^* B_n^* C_n^*$, avec $\theta_2 = \prod_{i\in F_3} \mu_i$, $A_n^* =$

$\prod_{i\in F_1}(1-\mu_i^n)$, $B_n^*=\prod_{i\in F_2}(\mu_i^n-1)$ et $C_n^*=\prod_{i\in F_3}(1-\mu_i^{-n})$, et f_1 est le cardinal de F_1.

Posons $\theta=\dfrac{a_0\theta_1}{b_0\theta_2}$, $w_n=\dfrac{A_n^*C_n^*}{A_nC_n}$. La suite w_n converge vers 1, et on a $w_n-1=t_n=O(\rho^n)$, avec $0<\rho<1$. Les suites B_n et B_n^* sont majorées en module par un nombre M indépendant de n.

Soit encore ε égal à 0 ou 1 selon que l'on se trouve dans le premier cas de figure ou dans le second.

On a $\theta^nB_n=(-1)^{-e_1+f_1+\varepsilon}w_nB_n^*$. Supposons que $|\theta|>1$. Alors il existe une constante $M_1>0$ telle que on a $|B_n|\le\dfrac{M_1}{|\theta|^n}$ pour tout n, et on en déduit que la série entière $R(x)=\sum_{n\ge1}B_nx^n$ a un rayon de convergence $\ge|\theta|>1$. Mais B_n est une somme finie $\sum a_kb_k^n$, où les b_k sont des produits finis de $\lambda_i, i\in E_2$, donc sont de module 1. Par suite R est une fraction rationnelle dont les seuls pôles possibles, qui sont parmi les b_k^{-1}, sont de module 1. Donc R n'a aucun pôle, c'est un polynôme, ce qui est absurde car B_n n'est jamais nul. Le raisonnement symétrique montre que l'on ne peut avoir $|\theta|<1$, donc on a $|\theta|=1$.

Posons $D_n=\theta^nB_n-(-1)^{-e_1+f_1+\varepsilon}B_n^*=(-1)^{-e_1+f_1+\varepsilon}B_n^*t_n$. Par ce qui précède, la fraction rationnelle $S(x)=\sum_{n\ge1}D_nx^n$ n'a pour pôles possibles que des nombres de module 1, et d'autre part il existe une constante $M_2>0$ telle que $|D_n|\le M_2\rho^n$ pour tout n, donc S a un rayon de convergence >1 ; c'est donc un polynôme, donc D_n est nulle pour n assez grand, et comme c'est une suite récurrente linéaire, elle est nulle pour tout n.

On a donc que $\theta^nB_n-(-1)^{-e_1+f_1+\varepsilon}B_n^*=0$ pour tout n, et aussi que $A_n^*C_n^*=A_nC_n$ pour tout n.

On remarque que E_2 et F_2 sont tous les deux non vides. En effet, si par exemple E_2 est vide, et donc $B_n=1$ pour $n\ge1$, on sait que F_2 est non vide. Soit $j_0\in F_2$; il existe une suite n_k strictement croissante d'entiers telle que $\mu_{j_0}^{n_k}$ converge vers 1 (que l'on soit dans le cas de $\mathbf{C}$ ou de $\mathbf{C}_p$), ce qui donne que $B_{n_k}^*$ converge vers 0, donc aussi θ^{n_k}, ce qui est absurde car θ est de module 1. Donc ici, on aura E_2 et F_2 non vides, et $E_1\cup E_3$ également.

On réécrit les relations obtenues sous la forme

$$a_0^n\theta_1^n\prod_{i\in E_2}(\lambda_i^n-1)=(-1)^{-e_1+f_1+\varepsilon}b_0^n\theta_2^n\prod_{i\in F_2}(\mu_i^n-1)$$

et

$$(-1)^{-e_1+f_1}\theta_1^{-n}\prod_{i\in E_1\cup E_3}(\lambda_i^n-1)=\theta_2^{-n}\prod_{i\in F_1\cup F_3}(\mu_i^n-1).$$

Du fait que $e_1+e_3\ge1$ et $e_2\ge1$, on peut alors utiliser pour ces deux situations l'hypothèse de récurrence, pour les polynômes $P_1(X)=a_0\theta_1\prod_{i\in E_2}(X-\lambda_i)$ et $Q_1(X)=b_0\theta_2\prod_{i\in F_2}(X-\mu_i)$ d'une part, avec ε_1 égal à $-e_1+f_1+\varepsilon$, puisque l'on a $r_n(P_1)=(-1)^{\varepsilon_1}r_n(Q_1)$, et les polynômes $P_2(X)=\theta_1^{-1}\prod_{i\in E_1\cup E_3}(X-\lambda_i)$ et $Q_2(X)=\theta_2^{-1}\prod_{i\in F_1\cup F_3}(X-\mu_i)$ d'autre part, avec ε_2 égal à $-e_1+f_1$, puisque l'on a $r_n(P_2)=(-1)^{\varepsilon_2}r_n(Q_2)$.

Il existe donc des polynômes U_1,V_1,U_2,V_2, avec les degrés de U_1 et U_2 de même parité que ε_1 et ε_2, tels que $P_1=(-1)^{\varepsilon_1}U_1^*V_1$, $Q_1=U_1V_1$, et $P_2=(-1)^{\varepsilon_2}U_2^*V_2$, $Q_2=U_2V_2$. On en conclut que $P=P_1P_2$ et $Q=Q_1Q_2$ s'écrivent sous la forme $P=(-1)^{\varepsilon_1+\varepsilon_2}U^*V$ et $Q=UV$, avec $U=U_1U_2$, $V=V_1V_2$. Le nombre $\varepsilon_1+\varepsilon_2$ est congru à ε modulo 2, et le degré de U est de même parité que ε, et ceci termine la démonstration.

Références

[1] D. Fried, Cyclic resultants of reciprocal polynomials, in *Holomorphic dynamics* (*Mexico,* 1986), 124–128, Lecture Notes in Math., 1345, Springer, Berlin.

[2] C. J. Hillar, Cyclic resultants, J. Symbolic Comput. **39** (2005), no. 6, 653–669.

[3] C. Hillar, L. Levine, Polynomial recurrences and cyclic resultants, Proc Amer Math Soc, **135**, (2007), 1607–1618.

[4] K. S. Kedlaya, Quantum computation of zeta functions of curves, Comput. Complexity **15** (2006), no. 1, 1–19.