COLLOQUIUM MATHEMATICUM

VOL. LV 1988 FASC. 2

SUR LA COMPOSITION DES POLYNÔMES

PAR

PIERRE TORTRAT (MEUDON)

La première partie de l'article décrit tous les quadruplets (P_1, Q_1, P_2, Q_2) de polynômes à coefficients complexes tels que $P_1 \circ Q_2 = Q_1 \circ P_2$ (propositions 1 et 5). Ces résultats, dûs essentiellement à J. F. Ritt, se trouvent avec des démonstrations différentes dans [4], accompagnés d'une bibliographie détaillée.

Dans la deuxième partie, on associe algèbriquement à tout polynôme de degré $\geqslant 2$ une forme linéaire sur $C[X]$. Cette forme linéaire est par ailleurs la restriction à $C[X]$ de la mesure μ^* associée au polynôme dans [1] (μ^* est la mesure d'équilibre sur l'ensemble de Julia du polynôme). Les formes linéaires associées à deux polynômes P et Q dont les termes de plus haut degré ont pour coefficient 1 sont *égales* si et seulement si $P \circ Q = Q \circ P$. Le lien avec la commutation si l'on supprime cette hypothèse est l'objet de la proposition 8.

Le but de la deuxième partie est la proposition 11, qui décrit les couples de polynômes ayant même forme linéaire, généralisant ainsi certains résultats de [2] et [3].

Pour $P \in C[X]$ et m entier $\geqslant 1$, on note respectivement P^m et $P^{(m)}$ la puissance m-ième de P pour la multiplication des polynômes X et pour leur composition $\circ$.

Si $\deg P = 1$, on note P^{-1} le symétrique de P pour la loi $\circ$.

Pour $n \geqslant 2$, on note T_n le polynôme de Tchebycheff de degré n, c'est-à-dire le polynôme faisant commuter le diagramme

$$\begin{array}{ccc} & X^n & \\ \frac{1}{2}(X+1/X)\downarrow & \rightarrow & \downarrow\frac{1}{2}(X+1/X) \\ & T_n & \end{array}$$

PROPOSITION 1. *Soient k un corps algèbriquement clos, P_1, Q_1, P_2, Q_2 des éléments de degré > 0 de $k[X]$ tels que $P_1 \circ Q_2 = Q_1 \circ P_2$. On suppose que*

$\deg P_1 \circ Q_2$ est premier à la caractéristique de k si celle-ci est non nulle. Il existe alors R, P_3 et Q_3 dans $k[X]$ tels que

$$\deg R = \mathrm{PGCD}(\deg P_1, \deg Q_1), \quad P_1 = R \circ P_3, \quad Q_1 = R \circ Q_3,$$

et S, P_4 et Q_4 dans $k[X]$ tels que

$$\deg S = \mathrm{PGCD}(\deg P_2, \deg Q_2), \quad P_2 = P_4 \circ S, \quad Q_2 = Q_4 \circ S.$$

Démonstration. Soient

$$P = P_1 \circ Q_2, \quad n = \deg P, \quad p = \deg P_1, \quad q = \deg Q_1, \quad r = \mathrm{PGCD}(p, q),$$

$$s = \mathrm{PGCD}(n/p, n/q), \quad P = \sum_{i=0}^{n} a_i X^i, \quad P_1 = \sum_{i=0}^{p} b_i X^i, \quad Q_2 = \sum_{i=0}^{n/p} c_i X^i.$$

Soient Y transcendant sur k, K extension de $k(Y)$ engendrée par les racines $\alpha_0, \ldots, \alpha_{n-1}$ de $P - Y$. Soit v un prolongement à K de la valuation définie sur $k(Y)$ par

$$v\left(\frac{\sum_{i=0}^{l} d_i Y^i}{\sum_{i=0}^{m} e_i Y^i}\right) = m - l,$$

où $d_i \in k$, $e_i \in k$, $d_l \neq 0$, $e_m \neq 0$. Soient $\mathcal{O}$ l'anneau de valuation de K pour v, $\mathfrak{p}$ son idéal maximal. $\forall\, i$, $P(\alpha_i) = Y \notin \mathcal{O}$, donc $\alpha_i \notin \mathcal{O}$. On a

$$\left(\frac{\alpha_i}{\alpha_j}\right)^n \equiv 1 \pmod{\mathfrak{p}},$$

car

$$\left(\frac{\alpha_i}{\alpha_j}\right)^n = \frac{1 + \sum_{l=0}^{n-1} a_l/a_n \alpha_j^{n-l}}{1 + \sum_{l=0}^{n-1} a_l/a_n \alpha_i^{n-l}}$$

et $\sum_{l=0}^{n-1} a_l/a_n \alpha_i^{n-l}$, $\sum_{l=0}^{n-1} a_l/a_n \alpha_j^{n-l}$ appartiennent à $\mathfrak{p}$. Pour tout i

$$P - Y = (X - \alpha_i)\alpha_i^{n-1} \left| a_n \sum_{m=0}^{n-1} \left(\frac{X}{\alpha_i}\right)^m + \sum_{l=1}^{n-1} \frac{a_l}{\alpha_i^{n-l}} \sum_{m=0}^{l-1} \left(\frac{X}{\alpha_i}\right)^m \right|,$$

et si $x \in K$ est tel que

$$\frac{x}{\alpha_i} \equiv 1 \pmod{\mathfrak{p}}, \qquad a_n \sum_{m=0}^{n-1} \left(\frac{x}{\alpha_i}\right)^m \equiv n a_n \not\equiv 0 \pmod{\mathfrak{p}},$$

$$\sum_{l=1}^{n-1} \frac{a_l}{\alpha_i^{n-l}} \sum_{m=0}^{l-1} \left(\frac{x}{\alpha_i}\right)^m \in \mathfrak{p},$$

donc

$$a_n \sum_{m=0}^{n-1} \left(\frac{x}{\alpha_i}\right)^m + \sum_{l=1}^{n-1} \frac{a_l}{\alpha_i^{n-l}} \sum_{m=0}^{l-1} \left(\frac{x}{\alpha_i}\right)^m \not\equiv 0.$$

Par suite, $\forall j \neq i$,

$$\frac{\alpha_j}{\alpha_i} \not\equiv 1 \pmod{\mathfrak{p}}, \qquad \frac{\alpha_j}{\alpha_0} \not\equiv \frac{\alpha_i}{\alpha_0} \pmod{\mathfrak{p}}.$$

Ceci prouve que les classes dans le corps résiduel $\mathcal{O}/\mathfrak{p}$ des α_i/α_0 sont les racines n-ièmes de 1. Soit ζ une racine primitive n-ième de 1 dans $\mathcal{O}/\mathfrak{p}$. On peut supposer que les α_i ont été numérotés de telle sorte que la classe de α_i/α_0 dans $\mathcal{O}/\mathfrak{p}$ soit ζ^i. Comme $P = P_1 \circ Q_2$, $\forall i$ il existe n/p indices j tels que $Q_2(\alpha_i) = Q_2(\alpha_j)$; on a alors comme précédemment

$$\left(\frac{\alpha_i}{\alpha_j}\right)^{n/p} \equiv 1 \pmod{\mathfrak{p}}, \qquad \zeta^{(i-j)n/p} = 1, \qquad i \equiv j \pmod{p}.$$

On a donc l'équivalence

$$Q_2(\alpha_i) = Q_2(\alpha_j) \Leftrightarrow i \equiv j \pmod{p},$$

et de même

$$P_2(\alpha_i) = P_2(\alpha_j) \Leftrightarrow i \equiv j \pmod{q}.$$

Pour $0 \leqslant i \leqslant p-1$, soit

$$\beta_i = (-1)^{n/p} \prod_{j=0}^{n/p-1} \alpha_{i+pj}.$$

Les α_{i+pj} sont les racines de $Q_2 - Q_2(\alpha_i)$, donc

$$Q_2(\alpha_i) = c_0 - c_{n/p}\beta_i.$$

Les racines de $P_1 - Y$ sont donc les $c_0 - c_{n/p}\beta_i$.

$K/k(Y)$ est galoisienne. Soit $\sigma \in G(K/k(Y))$. L'automorphisme σ permute les α_i, ainsi que les β_i. Soit τ la permutation de $\{0, \ldots, p-1\}$ définie par $\sigma(\beta_i) = \beta_{\tau(i)}$. Pour $0 \leqslant i \leqslant p-1$, on a

$$\sigma(Q_2(\alpha_i)) = \sigma(c_0 - c_{n/p}\beta_i) = c_0 - c_{n/p}\beta_{\tau(i)} = Q_2(\alpha_{\tau(i)}).$$

Soient i et j dans $\{0, \ldots, p-1\}$. La congruence $i \equiv j \pmod r$ signifie qu'il existent l et m dans $\{0, \ldots, n-1\}$ tels que

$$i \equiv l \pmod p, \quad j \equiv m \pmod p, \quad l \equiv m \pmod q,$$

ce qui est équivalent à chacune des conditions suivantes:

$$\exists (l, m) \text{ tel que } Q_2(\alpha_i) = Q_2(\alpha_l),\ Q_2(\alpha_j) = Q_2(\alpha_m),\ P_2(\alpha_l) = P_2(\alpha_m)$$

$$\Leftrightarrow \exists (l, m) \text{ tel que } Q_2(\alpha_{\tau(i)}) = Q_2(\sigma(\alpha_l)),\ Q_2(\alpha_{\tau(j)}) = Q_2(\sigma(\alpha_m)),\ P_2(\sigma(\alpha_m)) = P_2(\sigma(\alpha_l))$$

$$\Leftrightarrow \exists (l, m) \text{ tel que } Q_2(\alpha_{\tau(i)}) = Q_2(\alpha_l),\ Q_2(\alpha_{\tau(j)}) = Q_2(\alpha_m),\ P_2(\alpha_l) = P_2(\alpha_m)$$

$$\Leftrightarrow \tau(i) \equiv \tau(j) \pmod r.$$

Pour $0 \leqslant j \leqslant r-1$, $1 \leqslant l \leqslant p/r$, soit $s_{j,l}$ la l-ième fonction symétrique élémentaire des β_{j+ri}, $i \in \{0, \ldots, p/r-1\}$. L'automorphisme τ permute les ensembles

$$\{j+ri:\ 0 \leqslant i \leqslant p/r-1\},$$

donc σ permute les $s_{j,l}$, $0 \leqslant j \leqslant r-1$. Par suite, pour $1 \leqslant m \leqslant r$, la m-ième fonction symétrique élémentaire $S_{l,m}$ des $s_{j,l}$ est invariante par σ. D'après l'arbitraire sur σ, on a donc $S_{l,m} \in k(Y)$.

Les α_i sont entiers sur $k[Y]$, il en est donc de même des β_i et des $S_{l,m}$. L'anneau $k[Y]$ étant intégralement clos, $S_{l,m} \in k[Y]\ \forall (l, m)$. Nous avons

$$\forall i,\ v\left(\frac{\alpha_i}{\alpha_0}\right) = 0, \quad v(\alpha_i) = v(\alpha_0).$$

Ensuite

$$\prod_{i=0}^{n-1} \alpha_i = (-1)^n \frac{a_0 - Y}{a_n},$$

donc

$$nv(\alpha_0) = v\Big(\prod_{i=0}^{n-1} \alpha_i\Big) = -1$$

et

$$v(\beta_i) = v\Big((-1)^{n/p} \prod_{j=0}^{n/p-1} \alpha_{i+pj}\Big) = \frac{n}{p} v(\alpha_0) = -\frac{1}{p}.$$

$\forall (l, m) \neq (p/r, r)$, $S_{l,m}$ s'écrit comme polynôme à coefficients dans k de degré total $<p$ des β_i, donc

$$v(S_{l,m}) > pv(\beta_0) = -1.$$

Comme $S_{l,m} \in k[Y]$, $S_{l,m} \in k$. Ensuite on a

$$S_{p/r,r} = \prod_{i=0}^{p-1} \beta_i = (-1)^n \prod_{i=0}^{n-1} \alpha_i = \frac{a_0 - Y}{a_n}.$$

Pour $1 \leqslant l \leqslant p/r-1$, les $s_{j,l}$ sont racines d'un polynôme à coefficients dans k; k étant algèbriquement clos, cela implique $s_{j,l} \in k$.

$P-Y$ est irréductible sur $k(Y)$: en effet, le degré de α_0 sur $k(Y)$ est $\geqslant 1/|v(\alpha_0)| = n = \deg(P-Y)$. Par suite $G(K/k(Y))$ opère transitivement sur $\{\alpha_i : 0 \leqslant i \leqslant n-1\}$, donc aussi sur $\{\beta_i : 0 \leqslant i \leqslant p-1\}$ et sur $\{s_{j,l} : 0 \leqslant j \leqslant r-1\}$. Pour $l \leqslant p/r-1$, les $s_{j,l}$ étant invariant par $G(K/k(Y))$, $s_{j,l}$ est indépendant de j, on le notera s_l. Soient

$$P_3 = \left(\frac{X-c_0}{c_{n/p}}\right)^{p/r} + \sum_{l=1}^{p/r-1} s_l \left(\frac{X-c_0}{c_{n/p}}\right)^{p/r-l} \in k[X],$$

$$R = a_n\left(X^r + \sum_{m=1}^{r-1} S_{p/r,m} X^{r-m}\right) + a_0 \in k[X].$$

On a

$$\begin{aligned} P_1 &= b_p \prod_{i=0}^{p-1} (X - c_0 + c_{n/p}\beta_i) + Y \\ &= b_p c_{n/p}^p \prod_{j=0}^{r-1} \prod_{i=0}^{p/r-1} \left(\frac{X-c_0}{c_{n/p}} + \beta_{j+ri}\right) + Y \\ &= a_n \prod_{j=0}^{r-1} (P_3 + s_{j,p/r}) + Y = a_n\left(P_3^r + \sum_{m=1}^{r} S_{p/r,m} P_3^{r-m}\right) + Y = R \circ P_3. \end{aligned}$$

Comme $S_{p/r,m}$ est la m-ième fonction symétrique élémentaire des

$$s_{j,p/r} = \prod_{i=0}^{p/r-1} \beta_{j+ri} = (-1)^{n/r} \prod_{i=0}^{n/r-1} \alpha_{j+ri},$$

elle ne change pas quand on permute les rôles de P_1 et Q_1. Il existe donc $Q_3 \in k[X]$ tel que $Q_2 = R \circ Q_3$. Soit $Z = Q_2(\alpha_0)$. Les racines de $Q_2 - Z$ sont les α_{pi} ($i \in \{0, \ldots, n/p-1\}$), $P_1(Z) = Y$, $k(Y) \subset k(Z)$, $K/k(Z)$ est galoisienne. Soit $\sigma \in G(K/k(Z))$. Soit τ la permutation de $\{0, \ldots, n/p-1\}$ définie par $\sigma(\alpha_{pi}) = \alpha_{p\tau(i)}$. Soient i et j dans $\{0, \ldots, n/p-1\}$. Alors

$$\begin{aligned} i \equiv j \pmod{q/r} &\Leftrightarrow pi \equiv pj \pmod{pq/r} \Leftrightarrow pi \equiv pj \pmod{q} \Leftrightarrow P_2(\alpha_{pi}) = P_2(\alpha_{pj}) \\ &\Leftrightarrow \sigma(P_2(\alpha_{pi})) = \sigma(P_2(\alpha_{pj})) \Leftrightarrow P_2(\alpha_{p\tau(i)}) = P_2(\alpha_{p\tau(j)}) \\ &\Leftrightarrow \tau(i) \equiv \tau(j) \pmod{q/r}. \end{aligned}$$

Posons $s = nr/pq$. Pour $0 \leqslant j \leqslant q/r-1$, $1 \leqslant l \leqslant s$, soit $s'_{j,l}$ la l-ième fonction symétrique élémentaire des $\alpha_{p(j+qi/r)}$, $i \in \{0, \ldots, s-1\}$. Pour $1 \leqslant l \leqslant s$, $1 \leqslant m \leqslant q/r$, soit $S'_{l,m}$ la m-ième fonction symétrique élémentaire des $s'_{j,l}$, $j \in \{0, \ldots, q/r-1\}$.

La restriction de v à $k(Z)$ prend ses valeurs dans $v(Z)\mathbf{Z}$.

Comme précédemment, on montre que pour $0 \leqslant j \leqslant q/r-1$, $1 \leqslant l \leqslant s-1$, $s'_{j,l}$ appartient à k et est indépendant de j, on le note s'_l, et que pour $1 \leqslant m \leqslant q/r-1$, $S'_{s,m}$ appartient à k.

Soient

$$S = X^s + \sum_{l=1}^{s-1} (-1)^l s'_l X^{s-l} \in k[X],$$

$$Q_4 = c_{n/p}\Big(X^{q/r} + \sum_{m=1}^{q/r-1} (-1)^{sm} S'_{s,m} X^{q/r-m}\Big) + c_0 \in k[X].$$

On a

$$Q_2 = c_{n/p} \prod_{i=0}^{n/p-1} (X-\alpha_{pi}) + Z = c_{n/p} \prod_{j=0}^{q/r-1} \prod_{i=0}^{s-1} (X-\alpha_{p(j+qi/r)}) + Z$$

$$= c_{n/p} \prod_{j=0}^{q/r-1} \big(S+(-1)^s s'_{j,s}\big) + Z = c_{n/p}\Big(S^{q/r} + \sum_{m=1}^{q/r} (-1)^{sm} S'_{s,m} S^{q/r-m}\Big) + Z$$

$$= Q_4 \circ S - c_0 + c_{n/p}(-1)^{n/p} S'_{s,q/r} + Z$$

$$= Q_4 \circ S - c_0 + c_{n/p}(-1)^{n/p} \prod_{j=0}^{q/r-1} \prod_{i=0}^{s-1} \alpha_{p(j+qi/r)} + Z$$

$$= Q_4 \circ S - c_0 + c_{n/p} \prod_{k=0}^{n/p-1} (-\alpha_{pk}) + Z = Q_4 \circ S.$$

Comme $s'_l = s'_{0,l}$ est la l-ième fonction symétrique élémentaire des $\alpha_{ni/s}$, elle ne change pas quand on permute les rôles de P_2 et Q_2. Il existe donc $P_4 \in k[X]$ tel que $P_2 = P_4 \circ S$.

Remarque. Dans la proposition, on peut choisir P_3 de telle sorte que

$$P_3 \circ Q_4 = Q_3 \circ P_4.$$

Démonstration. On a

$$R \circ P_3 \circ Q_4 \circ S = R \circ Q_3 \circ P_4 \circ S,$$

donc

$$R \circ P_3 \circ Q_4 = R \circ Q_3 \circ P_4.$$

D'après la proposition appliquée aux polynômes R, $P_3 \circ Q_4$, $Q_3 \circ P_4$, il existe $T \in k[X]$ du premier degré tel que

$$T \circ P_3 \circ Q_4 = Q_3 \circ P_4.$$

On a

$$R \circ T \circ P_3 \circ Q_4 = R \circ Q_3 \circ P_4 = R \circ P_3 \circ Q_4,$$

donc

$$R \circ T \circ P_3 = R \circ P_3 = P_1.$$

Il suffit donc de remplacer P_3 par $T \circ P_3$ pour avoir la propriété demandée.

PROPOSITION 2. *Soient k un corps algébriquement clos de caractéristique 0, p et q deux entiers > 0 premiers entre eux, P_1, P_2 deux éléments de $k[X]$ de degré p, Q_1, Q_2 deux éléments de $k[X]$ de degré q tels que $P_1 \circ Q_2 = Q_1 \circ P_2$. Soient $a \in k$, $b \in k$ tels que $P_1(b) = a$, $c \in k$ tel que $Q_1(c) = a$, p' l'indice de ramification de P_1 en b, q' celui de Q_1 en c. Il existe exactement* PGCD(p', q') *éléments x de k tels que $Q_2(x) = b$, $P_2(x) = c$, et l'indice de ramification de $P_1 \circ Q_2$ en un tel x est* PPCM(p', q').

Démonstration. Soient Y transcendant sur k, Z une racine de $P_1 \circ Q_2 - Y$, $F = k(Z)$, $K = k(Q_2(Z))$, $L = k(P_2(Z))$; $P_1 \circ Q_2 - Y$ étant irréductible sur $k(Y)$, $[F: k(Y)] = pq$. De même, $Q_2(Z)$ étant une racine de $P_1 - Y$, $[K: k(Y)] = p$, et aussi

$$[L: k(Y)] = q.$$

p et q étant premiers entre eux, K et L sont linéairement disjoints sur $k(Y)$ et $F = KL$. Soient v la valuation de $k(Y)$ définie par

$$v\left((Y-a)^n \frac{P}{Q}\right) = n,$$

où P et Q sont deux éléments de $k[Y]$ tels que $P(a) \neq 0$, $Q(a) \neq 0$, v_K le prolongement de v à K défini par

$$v_K\left((Q_2(Z)-b)^n \frac{P}{Q}\right) = \frac{n}{p'},$$

P et Q dans $k[Q_2(Z)]$ avec $P(b) \neq 0$, $Q(b) \neq 0$, v_L défini de façon analogue. Les valuations de F prolongeant v_K et v_L sont les v_x, $x \in k$ tel que $Q_2(x) = b$ et $P_2(x) = c$, définies par

$$v_x\left((Z-x)^n \frac{P}{Q}\right) = \frac{n}{e_x},$$

P et Q dans $k[Z]$ tels que $P(x) \neq 0$, $Q(x) \neq 0$, et e_x désignant l'indice de ramification de $P_1 \circ Q_2$ en x. Supposons donné un tel x, et soient $\bar{F}$ le complété de F pour v_x, $\overline{k(Y)}$, $\bar{K}$ et $\bar{L}$ les adhérences de $k(Y)$, K et L dans $\bar{F}$. On a

$$[\bar{F}: \overline{k(Y)}] = e_x, \quad [\bar{K}: \overline{k(Y)}] = p', \quad [\bar{L}: \overline{k(Y)}] = q'.$$

$\bar{F}/\overline{k(Y)}$ est cyclique ([5], p. 76, prop. 8), $\bar{F} = \bar{K}\bar{L}$, donc $G(\bar{F}/\bar{K}) \cap G(\bar{F}/\bar{L})$ n'a

qu'un élément, l'intersection des sous-groupes d'indices p' et q' de $Z/e_x Z$ n'a qu'un élément, $e_x = \mathrm{PPCM}(p', q')$.

$\overline{k(Y)}$ étant le complété de $k(Y)$ pour v, soit A la clôture algébrique de $\overline{k(Y)}$. Il existe une valuation unique sur A dont la restriction à $\overline{k(Y)}$ soit v, on la notera encore v. L'indice de ramification d'un prolongement v' de v à une extension finie de $k(Y)$ est égal au nombre de plongements f de cette extension dans A au-dessus de $k(Y)$ tels que $v \circ f = v'$. L'ensemble $\mathscr{P}$ des plongements f de K dans A au-dessus de $k(Y)$ tels que $v \circ f = v_K$ a donc p' éléments, on définit de même l'ensemble $\mathscr{Q}$ à q' éléments. Si m désigne le nombre de valuations de F prolongeant v_K et v_L, $m\,\mathrm{PPCM}(p', q')$ est égal au nombre de plongements f de F dans A tels que $(f|_K, f|_L) \in \mathscr{P} \times \mathscr{Q}$. K et L étant linéairement disjoints sur $k(Y)$, $\forall (g, h) \in \mathscr{P} \times \mathscr{Q}$, il existe un plongement unique de $F = KL$ dans A dont les restrictions à K et L soient g et h. On a donc

$$m\,\mathrm{PPCM}(p', q') = \mathrm{Card}(\mathscr{P} \times \mathscr{Q}) = p'q', \qquad m = \mathrm{PGCD}(p', q').$$

PROPOSITION 3. *Soient k un corps algébriquement clos de caractéristique 0, p et q deux entiers $\geqslant 2$, premiers entre eux, avec $p < q$. Soient P_1, P_2 deux éléments de $k[X]$ de degré p, Q_1, Q_2 deux éléments de $k[X]$ de degré q tels que*

$$P_1 \circ Q_2 = Q_1 \circ P_2.$$

L'ensemble des images par P_1 des zéros de P_1' contient alors un ou deux points. S'il ne contient qu'un point x, en chacun des antécédents de x par Q_1 sauf un, l'indice de ramification de Q_1 est multiple de p. S'il contient deux points x et y, $\{x, y\}$ est également l'ensemble des images par Q_1 des zéros de Q_1'; si p est impair, les indices de ramification de P_1 en les antécédents de x par P_1 sont tous égaux à 2 sauf un qui est égal à 1, de même pour y; si p est pair, les indices de ramification de P_1 en les antécédents par P_1 d'un des points x ou y sont tous égaux à 2, tandis que pour l'autre point ils sont égaux à 2 sauf deux d'entre eux égaux à 1; on a la même chose pour Q_1.

Démonstration. Soit $\{x_1, \ldots, x_n\}$ la réunion des images par P_1 des zéros de P_1' et des images par Q_1 des zéros de Q_1'. L'ensemble $\{x_1, \ldots, x_n\}$ contient toutes les images par $P_1 \circ Q_2$ des zéros de $(P_1 \circ Q_2)'$. En effet, soient w un zéro de $(P_1 \circ Q_2)'$, p' l'indice de ramification de P_1 en $Q_2(w)$, q' l'indice de ramification de Q_1 en $P_2(w)$. D'après la proposition 2, l'indice de ramification de $P_1 \circ Q_2$ en w est $\mathrm{PPCM}(p', q')$. On a donc $\mathrm{PPCM}(p', q') > 1$, $p' > 1$ ou $q' > 1$. Dans le premier cas $P_1 \circ Q_2(w)$ est l'image par P_1 d'un zéro de P_1', tandis que dans le second $P_1 \circ Q_2(w) = Q_1 \circ P_2(w)$ est l'image par Q_1 d'un zéro de Q_1'.

Soient m un entier compris entre 1 et n, $y_1, \ldots, y_s$ les antécédents de x_m par P_1, p_i l'indice de ramification de P_1 en y_i, $z_1, \ldots, z_t$ les antécédents de x_m

par Q_1, q_i l'indice de ramification de Q_1 en z_i, $r_1, \ldots, r_u$ les indices de ramification de $P_1 \circ Q_2$ en les antécédents de x_m par $P_1 \circ Q_2$,

$$\pi_m = \sum (p_i - 1), \quad \varkappa_m = \sum (q_i - 1), \quad \varrho_m = \sum (r_i - 1).$$

On a

$$\sum p_i = p, \quad \sum q_i = q, \quad \pi_m = p - s, \quad \varkappa_m = q - t.$$

$\forall (i, j) \in \{1, \ldots, s\} \times \{1, \ldots, t\}$, x_m possède exactement $\mathrm{PGCD}(p_i, q_j)$ antécédents par $P_1 \circ Q_2$ ayant y_i pour image par Q_2 et z_j pour image par P_2, et l'indice de ramification de $P_1 \circ Q_2$ en un tel antécédent est $\mathrm{PPCM}(p_i, q_j)$. On a donc

$$\begin{aligned} \varrho_m &= \sum \mathrm{PGCD}(p_i, q_j)(\mathrm{PPCM}(p_i, q_j) - 1) \\ &= \sum p_i q_j - \mathrm{PGCD}(p_i, q_j) = pq - \sum \mathrm{PGCD}(p_i, q_j). \end{aligned}$$

$\forall (i, j)$, $\mathrm{PGCD}(p_i, q_j) \leqslant (p_i - 1)(q_j - 1) + 1$, donc

$$\sum \mathrm{PGCD}(p_i, q_j) \leqslant \pi_m \varkappa_m + st = pq - p\varkappa_m - q\pi_m + 2\pi_m \varkappa_m,$$

et

$$\varrho_m \geqslant p\varkappa_m + q\pi_m - 2\pi_m \varkappa_m.$$

Comme

$$\sum_{m=1}^{n} \pi_m = p - 1, \quad \sum_{m=1}^{n} \varkappa_m = q - 1, \quad \sum_{m=1}^{n} \varrho_m = pq - 1,$$

on a

$$pq - 1 \geqslant p(q-1) + q(p-1) - 2\sum \pi_m \varkappa_m,$$

$$\sum \pi_m \varkappa_m \geqslant \frac{(p-1)(q-1)}{2} = \frac{1}{2}\left(\sum \pi_m\right)\left(\sum \varkappa_m\right).$$

Ceci implique qu'il existe i tel que

$$\pi_i \geqslant \tfrac{1}{2} \sum \pi_m, \quad \varkappa_i \geqslant \tfrac{1}{2} \sum \varkappa_m.$$

On peut supposer que le numérotage a été fait de telle sorte que $i = 1$. Dorénavant, les lettres p_i, q_j désigneront les nombres associés à x_1. Soient

$$a = p - 1 - \pi_1 = \sum_{m>1} \pi_m, \quad b = q - 1 - \varkappa_1 = \sum_{m>1} \varkappa_m.$$

On a $0 \leqslant a \leqslant (p-1)/2$, $0 \leqslant b \leqslant (q-1)/2$.

Si $a = 0$,

$$pq - \sum \mathrm{PGCD}(p, q_j) + bp = \sum \varrho_m = pq - 1,$$

$$\sum_{j=1}^{b+1} \mathrm{PGCD}(p, q_j) = bp+1,$$

tous les q_j sauf un sont multiples de p.

Si $b = 0$, comme précédemment

$$p = \sum p_i \geqslant \mathrm{PGCD}(p_i, q) = aq+1 \geqslant ap+1, \qquad a = 0.$$

Supposons maintenant $a \neq 0$, ce qui implique $b \neq 0$. On a alors $p \geqslant 3$. $\forall (i, j)$, $\mathrm{PGCD}(p_i, q_j) \leqslant (p_i+q_j)/2$. Les p_i et les q_j ne sont pas tous égaux, car alors leur valeur commune serait ≥ 1, et p et q ne seraient pas premiers entre eux. $a+1$ et $b+1$ sont $\geqslant 2$, il existe donc au moins deux couples (i, j) tels que $p_i \neq q_j$, c'est-à-dire

$$\mathrm{PGCD}(p_i, q_j) \leqslant \frac{p_i+q_j-1}{2}.$$

On a donc

$$\sum \mathrm{PGCD}(p_i, q_i) \leqslant \frac{(b+1)p+(a+1)q-2}{2}.$$

Si on a l'égalité, il existe exactement deux couples (i, j) pour lesquels $p_i \neq q_j$, et pour ceux-là

$$\mathrm{PGCD}(p_i, q_j) = \frac{p_i+q_j-1}{2},$$

donc $\{p_i, q_j\} = \{1, 2\}$; l'une des familles $\{p_i\}$ et $\{q_j\}$ est donc $\{2, 2\}$, l'autre de la forme $\{2, \ldots, 2, 1\}$; on a donc $a = (p-1)/2$ ou $b = (q-1)/2$.

Si on a l'inégalité stricte

$$\sum \mathrm{PGCD}(p_i, q_j) < \frac{(b+1)p+(a+1)q-2}{2},$$

on a

$$\varrho_1 > pq - \frac{(b+1)p+(a+1)q-2}{2},$$

$$\sum_{m>1} \varrho_m \geqslant \sum_{m>1} p\varkappa_m + q\pi_m + 2\pi_m\varkappa_m$$

$$\geqslant p\sum_{m>1}\varkappa_m + q\sum_{m>1}\pi_m - 2\Big(\sum_{m>1}\pi_m\Big)\Big(\sum_{m>1}\varkappa_m\Big) = bp+aq-2ab,$$

$$pq-1 = \sum \varrho_m > pq - \frac{(b+1)p+(a+1)q-2}{2} + bp + aq - 2ab,$$

$$(p/4-a)(q/4-b) > (p/4-1)(q/4-1);$$

si $p=3$, on a $a=1=(p-1)/2$; si $p\neq 3$,

$$|p/4-a|\,|q/4-b|>(p/4-1)(q/4-1),$$

donc une au moins des inégalités

$$|p/4-a|>p/4-1 \quad \text{et} \quad |q/4-b|>q/4-1$$

est vérifiée, et comme $p/4-1\geqslant 0$, $q/4-1\geqslant 0$, on a $a\notin[1,(p-2)/2]$ ou $b\notin[1,(q-2)/2]$; comme de plus $a\in[1,(p-1)/2]$ et $b\in[1,(q-1)/2]$, une au moins des égalités $a=(p-1)/2$ et $b=(q-1)/2$ est vérifiée.

Dans tous les cas, une au moins des égalités $a=(p-1)/2$ et $b=(q-1)/2$ est vérifiée. Supposons par exemple que ce soit la première. On a

$$\pi_1=\tfrac{1}{2}\sum\pi_m \quad \text{et} \quad \sum\pi_m\varkappa_m\geqslant\tfrac{1}{2}\Big(\sum\pi_m\Big)\Big(\sum\varkappa_m\Big).$$

Ceci implique

$$n=2 \quad \text{et} \quad \sum\pi_m\varkappa_m=\tfrac{1}{2}\Big(\sum\pi_m\Big)\Big(\sum\varkappa_m\Big).$$

Il en résulte que $\mathrm{PGCD}(p_i,q_j)=(p_i-1)(q_j-1)+1\ \forall(i,j)$, donc les p_i et les q_j sont tous égaux à 1 ou 2. De même pour les p_i' et les q_j', en notant ainsi les nombres associés à x_2. Comme $\sum(p_i-1)+\sum(p_i'-1)=p-1$, l'ensemble des p_i et des p_i' compte $p-1$ éléments égaux à 2 et deux égaux à 1. De même pour l'ensemble des q_j et des q_j'.

PROPOSITION 4. *Soit $P\in C[X]$ de degré $n\geqslant 2$ tel que les zéros de P' soient simples et aient pour image par P 1 ou -1. On suppose de plus que 1 possède au moins un antécédent par P où P' ne s'annulle pas. Il existe alors $R\in C[X]$ du 1-er degré tel que $P=T_n\circ R$, où T_n est le polynôme de Tchebycheff de degré n.*

Démonstration. Soient

$$B=C-\{-1,1\}, \quad X=P^{-1}(B).$$

$P\colon X\to B$ est un revètement. $\pi_1(B,0)$ est le groupe libre engendré par la classe α du chemin

$$t\mapsto 1-e^{2\pi it}\colon [0,1]\to B$$

et la classe β du chemin

$$t\mapsto e^{2\pi it}-1.$$

$\pi_1(B,0)$ opère dans la fibre $P^{-1}(0)$. Soit h l'antihomomorphisme ainsi défini de $\pi_1(B,0)$ dans le groupe des permutations de $P^{-1}(0)$. Le groupe $P^{-1}(\infty)=\{\infty\}$, donc $(\alpha\beta)^n\in\operatorname{Ker}h$. Les indices de remification de P aux points de $P^{-1}(1)$ étant égaux à 1 ou 2, $\alpha^2\in\operatorname{Ker}h$. L'un au moins de ces indices étant égal à 1, il existe dans $P^{-1}(0)$ un point x invariant par $h(\alpha)$. De même $\beta^2\in\operatorname{Ker}h$. Soit H le sous-groupe normal de $\pi_1(B,0)$ engendré par $(\alpha\beta)^n$, α^2,

β^2. Le groupe $\pi_1(B, 0)/H$ est isomorphe au groupe dièdral D_n, donc $(\pi_1(B, 0): H) = 2n$. On a $H \subset \operatorname{Ker} h$. L'image de $\pi_1(X, x)$ dans $\pi_1(B, 0)$ est le stabilisateur de x pour l'action de $\pi_1(B, 0)$ dans $P^{-1}(0)$, elle contient donc H et α et comme $\pi_1(B, 0)$ opère transitivement, son indice dans $\pi_1(B, 0)$ est n. Cette image est donc le sous-groupe de $\pi_1(B, 0)$ engendré par H et α.

Les résultats précédents s'appliquent au polynôme T_n: si on lui associe X' et x' comme ci-dessus, $\pi_1(X, x)$ et $\pi_1(X', x')$ ont même image dans $\pi_1(B, 0)$. Par suite, il existe un homéomorphisme analytique $X \to X'$ faisant commuter le diagramme

$$\begin{array}{ccc} X & \to & X' \\ & {\scriptstyle p}\searrow \quad \swarrow{\scriptstyle T_n} & \\ & B & \end{array}.$$

Cet homéomorphisme se prolonge en une bijection analytique de C sur lui-même, c'est-à-dire un polynôme du 1-er degré R, tel que $P = T_n \circ R$.

PROPOSITION 5. *Soient p et q deux entiers $\geqslant 2$, premiers entre eux, avec $p < q$. Soient P_1, P_2 deux éléments de $C[X]$ de degré p, Q_1, Q_2 deux éléments de $C[X]$ de degré q tels que $P_1 \circ Q_2 = Q_1 \circ P_2$. Il existe alors quatre polynômes du 1-er degré R, S, U, V tels que ou bien*

$$P_1 = U \circ X^p \circ R, \quad Q_1 = U \circ X^n T^p \circ S,$$

$$P_2 = S^{-1} \circ X^p \circ V, \quad Q_2 = R^{-1} \circ X^n T(X^p) \circ V,$$

avec $n \in N$ et $T \in C[X]$, ou bien

$$P_1 = U \circ T_n \circ R, \quad Q_1 = U \circ T_q \circ S,$$

$$P_2 = S^{-1} \circ T_p \circ V, \quad Q_2 = R^{-1} \circ T_q \circ V.$$

Démonstration. D'après la proposition 3, l'ensemble des images par P_1 des zéros de P_1' est formé d'un ou deux points.

Si l'ensemble des images par P_1 des zéros de P_1' est formé de deux points x et y, et si un des nombres p ou q est pair, par exemple p, un des points x ou y possède deux antécédents par P_1, où P_1' ne s'annule pas; supposons que ce soit x; q est alors impair, et x possède un antécédent par Q_1, où Q_1' ne s'annule pas. Si p et q sont impairs, x possède un antécédent par P_1, où P_1' ne s'annule pas, et un antécédent par Q_1, où Q_1' ne s'annule pas. Soit U le polynôme de 1-er degré tel que $U(1) = x$ et $U(-1) = y$. D'après la proposition 4, il existe des polynômes du 1-er degré R et S tels que

$$U^{-1} \circ P_1 = T_p \circ R, \quad U^{-1} \circ Q_1 = T_q \circ S.$$

On a $T_p \circ R \circ Q_2 = T_q \circ S \circ P_2$. Soient

$$B = C - \{-1, 1\}, \quad X = (T_p \circ R \circ Q_2)^{-1}(B), \quad X' = (T_p \circ T_q)^{-1}(B).$$

$\forall \xi \in X$, $T_p(R \circ Q_2(\xi)) = T_q(S \circ P_2(\xi))$, l'indice de ramification de T_p en

$R \circ Q_2(\xi)$ et celui de T_q en $S \circ P_2(\xi)$ sont égaux à 1, $T_p \circ T_q = T_q \circ T_p$, donc d'après la proposition 2 il existe $\xi' \in C$ unique tel que

$$T_q(\xi') = R \circ Q_2(\xi), \quad T_p(\xi') = S \circ P_2(\xi).$$

$T_p \circ T_q(\xi') = T_p \circ R \circ Q_2(\xi) \in B$, donc $\xi' \in X'$. Soit f: $X \to X'$ l'application $\xi \mapsto \xi'$. De même, $\forall \xi' \in X'$, il existe $\xi \in X$ unique tel que

$$R \circ Q_2(\xi) = T_q(\xi'), \quad S \circ P_2(\xi) = T_p(\xi'),$$

donc f est bijective.

Soient $\xi \in X$, W' une boule de centre $T_p \circ R \circ Q_2(\xi)$ incluse dans B, W un voisinage connexe de ξ tel que

$$T_p \circ R \circ Q_2(W) \subset W'.$$

$T_p \circ T_q$: $X' \to B$ est un revêtement. Soit g l'application continue de W' dans X' vérifiant

$$T_p \circ T_q \circ g = \mathrm{Id}_{W'} \quad \text{et} \quad g \circ T_p \circ R \circ Q_2(\xi) = f(\xi).$$

Sur W, on a

$$T_p \circ T_q \circ g \circ T_p \circ R \circ Q_2 = T_p \circ R \circ Q_2,$$

de plus

$$T_q \circ g \circ T_p \circ R \circ Q_2(\xi) = T_q \circ f(\xi) = R \circ Q_2(\xi),$$

donc

$$T_q \circ g \circ T_p \circ R \circ Q_2 = R \circ Q_2$$

sur W; de même

$$T_p \circ g \circ T_p \circ R \circ Q_2 = T_p \circ g \circ T_q \circ S \circ P_2 = S \circ P_2$$

sur W, donc f coïncide avec $g \circ T_p \circ R \circ Q_2$ sur W, f est donc analytique au voisinage de ξ.

f se prolonge en une bijection analytique de C sur lui-même, c'est-à-dire un polynôme du 1-er degré V, qui vérifie

$$T_q \circ V = R \circ Q_2, \quad T_p \circ V = S \circ P_2.$$

On a donc

$$P_2 = S^{-1} \circ T_p \circ V, \quad Q_2 = R^{-1} \circ T_q \circ V.$$

Si l'ensemble des images par P_1 des zéros de P_1' ne contient qu'un point x, soit U un polynôme du 1-er degré tel que $U(0) = x$. Vu que $U^{-1} \circ P_1$ est de la forme $(aX+b)^p$, on a, en posant $R = aX+b$,

$$P_1 = U \circ X^p \circ R.$$

D'après la proposition 3, les zéros de $U^{-1} \circ Q_1$ sont d'ordre multiple de p suaf un; $U^{-1} \circ Q_1$ est donc de la forme

$$(cX+d)^n \prod_i (X-a_i)^{pn_i};$$

en posant

$$S = cX+d, \qquad T = \prod_i \left(\frac{X-d}{c} - a_i\right)^{n_i},$$

on a

$$Q_1 = U \circ X^n T^p \circ S.$$

On a alors

$$X^p \circ R \circ Q_2 = X^n T^p \circ S \circ P_2.$$

On a aussi

$$X^p \circ X^n T(X^p) = X^n T^p \circ X^p.$$

Comme précédemment, on en déduit qu'il existe un polynôme du 1-er degré V tel que

$$P_2 = S^{-1} \circ X^p \circ V, \qquad Q_2 = R^{-1} \circ X^n T(X^p) \circ V.$$

Remarque. Si $p = 2$ et s'il existe trois polynômes du 1-er degré R, S, U tels que

$$P_1 = U \circ T_2 \circ R, \qquad Q_1 = U \circ T_q \circ S,$$

la même méthode montre qu'il existe un polynôme du 1-er degré V tel que

$$P_2 = S^{-1} \circ T_2 \circ V, \qquad Q_2 = R^{-1} \circ T_q \circ V.$$

Définition. Soient $P \in C[X]$ de degré $n \geqslant 2$, $Q \in C[X]$; $n^{-m} \sum_{P^{(m)}(\zeta)=z} Q(\zeta)$ est indépendant de l'entier naturel

$$m > \frac{\operatorname{Log} \deg Q}{\operatorname{Log} n}$$

et de $z \in C$. On le note $f_P(Q)$.

Démonstration. Soient

$$m > \frac{\operatorname{Log} \deg Q}{\operatorname{Log} n}, \qquad z \in C.$$

Alors $\deg(P^{(m)} - z) > \deg Q$, $\sum_{P^{(m)}(\zeta)=z} Q(\zeta)$ est une fonction symétrique des racines de $P^{(m)} - z$ de degré $< \deg(P^{(m)} - z)$, elle ne dépend donc pas du terme de degré 0 de $P^{(m)} - z$, ni donc de z.

De plus, $\forall l \in N$,

$$\frac{1}{n^{l+m}} \sum_{P^{(l+m)}(\zeta)=z} Q(\zeta) = \frac{1}{n^l} \sum_{P^{(l)}(z')=z} \frac{1}{n^m} \sum_{P^{(m)}(\zeta)=z'} Q(\zeta) = \frac{1}{n^m} \sum_{P^{(m)}(\zeta)=z} Q(\zeta).$$

f_P est une forme linéaire sur $C[X]$, et $f_P(1) = 1$.

DÉFINITION. Pour $P \in C[X]$ de degré $n \geqslant 1$, on note M_P l'opérateur sur $C[X]$ qui à Q associe $n^{-1} \sum_{P(Y)=X} Q(Y)$ et M'_P l'opérateur sur $C[X]^*$ transposé de M_P.

$\forall Q \in C[X]$, $M_P(Q \circ P) = Q$, M_P est donc surjectif et M'_P injectif.

Si P et Q sont deux éléments de $C[X]$ de degrés $\geqslant 1$, on a

$$M_{P \circ Q} = M_P M_Q, \qquad M'_{P \circ Q} = M'_Q M'_P.$$

Soient $P \in C[X]$ de degré $\geqslant 2$, $Q \in C[X]$; pour m assez grand, $M_{P^{(m)}} Q$ est constant égal à $f_P(Q)$; on a alors

$$f_P(Q) = M_{P^{(m)}} Q = M_{P^{(m-1)}} M_P Q = f_P(M_P Q) = M'_P f_P(Q),$$

donc $f_P = M'_P f_P$. Inversement, si $\varphi \in C[X]^*$ vérifie $\varphi = M'_P \varphi$ et $\varphi(1) = 1$, $\forall Q \in C[X]$, pour m assez grand on a

$$\varphi = M'^m_P \varphi = M'_{P^{(m)}} \varphi$$

et

$$\varphi(Q) = \varphi(M_{P^{(m)}} Q) = \varphi\big(f_P(Q)\big) = f_P(Q)\,\varphi(1) = f_P(Q),$$

donc $\varphi = f_P$. Par conséquent f_P est le seul élément de $C[X]^*$ invariant par M'_P et laissant 1 invariant.

Enfin, soient $U \in C[X]$ de degré $\geqslant 1$, P et Q dans $C[X]$ de degrés $\geqslant 2$ tels que $P \circ U = U \circ Q$. On a

$$M'_Q M'_U f_P = M'_{U \circ Q} f_P = M'_{P \circ U} f_P = M'_U M'_P f_P = M'_U f_P$$

et

$$M'_U f_P(1) = f_P(M_U 1) = f_P(1) = 1,$$

donc $f_Q = M'_U f_P$. En particulier, si $\deg U = 1$, on a $f_{U^{-1} \circ P \circ U} = M'_U f_P$.

DÉFINITION. Soit $\varphi \in C[X]^*$. On note $\mathscr{U}(\varphi)$ l'ensemble des $U \in C[X]$ de degré 1 tels que $M'_U \varphi = \varphi$. Cet ensemble $\mathscr{U}(\varphi)$ muni de 0 est évidemment un groupe.

PROPOSITION 6. *Soit $P \in C[X]$ de degré $\geqslant 2$. Les éléments Q de $C[X]$ tels que $\deg P = \deg Q$ et $f_P = f_Q$ sont les $U \circ P$, où $U \in \mathscr{U}(f_P)$.*

Démonstration. Si $U \in \mathscr{U}(f_P)$, on a

$$\deg P = \deg U \circ P, \qquad M'_{U \circ P} f_P = M'_P M'_U f_P = f_P,$$

donc $f_P = f_{U \circ P}$.

Réciproquement, soit $Q \in C[X]$ tel que $\deg P = \deg Q$ et $f_P = f_Q$. Pour $1 \leqslant k < \deg P$, $f_P(X^k)$ est la moyenne des puissances k-ièmes des racines de P, ainsi que de celles de Q. Les fonctions symétriques élémentaires de degré $< \deg P$ des racines de P sont donc les mêmes que pour Q, par suite $Q = U \circ P$, où $U \in C[X]$ est de degré 1,

$$M'_P M'_U f_P = M'_Q f_P = f_P = M'_P f_P,$$

et comme M'_P est injectif, $M'_U f_P = f_P$, $U \in \mathscr{U}(f_P)$.

Proposition 7. *Soit $P \in C[X]$ de degré $\geqslant 2$. Soient*

$$\alpha = f_P(X), \quad U = X - \alpha, \quad \sum a_k X^k = U \circ P \circ U^{-1},$$

$$K = \{k \in N:\ a_k \neq 0\}, \quad k_0 = \operatorname{Inf} K,$$

$$d = \operatorname{PGCD}(k - k_0:\ k \in K).$$

Alors $\mathscr{U}(f_P)$ est l'ensemble des $U^{-1} \circ aX \circ U$, où a est une racine d-ième de 1 si $d \neq 0$ et $a \in C^*$ si $d = 0$.

Démonstration. Soit $V \in \mathscr{U}(f_P)$. On a $\deg P = \deg P \circ V$,

$$M'_{P \circ V} f_P = M'_V M'_P f_P = f_P,$$

donc $f_P = f_{P \circ V}$, et, d'après la proposition 6, $\exists W \in \mathscr{U}(f_P)$ tel que $P \circ V = W \circ P$. Il vient

$$V(\alpha) = f_P(V) = M'_V f_P(V) = f_P(M_V V) = f_P(X) = \alpha$$

et $W(\alpha) = \alpha$. Il existe donc a et a' dans C^* tels que

$$U \circ V \circ U^{-1} = aX, \quad U \circ W \circ U^{-1} = a' X.$$

Pour tout $k \in N$

$$\sum a_k a^k X^k = U \circ P \circ V \circ U^{-1} = U \circ W \circ P \circ U^{-1} = \sum a' a_k X^k, \quad a^k a_k = a' a_k,$$

ainsi que

$$a^k = a' \ \forall k \in K, \quad a^{k - k_0} = 1 \ \forall k \in K, \quad a^d = 1.$$

Réciproquement, soient $a \in C^*$ tel que

$$a^d = 1, \quad V = U^{-1} \circ aX \circ U.$$

On a $a_k a^k = a^{k_0} a_k$ $\forall k \in N$, donc

$$U \circ P \circ U^{-1} \circ aX = (aX)^{(k_0)} \circ U \circ P \circ U^{-1},$$

$$P \circ V = V^{(k_0)} \circ P,$$

et $\forall m \in N$

$$P^{(m)} \circ V = V^{\binom{m}{k_0}} \circ P^{(m)}.$$

$\forall Q \in C[X]$, pour m assez grand on a

$$M'_V f_P(Q) = f_P(M_V Q)$$
$$= M_{P(m)} M_V Q = M_{V(k_0^m)} M_{P(m)} Q = M_{V(k_0^m)} f_P(Q) = f_P(Q),$$

donc $M'_V f_P = f_P$, $V \in \mathscr{U}(f_P)$.

Remarque. Il résulte de la proposition 7 que d dépend seulement de f_P et non de P.

Proposition 8. *Soient P et Q deux éléments de $C[X]$ de degrés $\geqslant 2$. Si $P \circ Q = Q \circ P$, on a $f_P = f_Q$. Inversement, si $f_P = f_Q$, il existe $U \in \mathscr{U}(f_P)$ tel que*

$$P \circ Q = U \circ Q \circ P.$$

Démonstration. Supposons que $P \circ Q = Q \circ P$. Comme

$$P \circ (Q \circ P) = (P \circ Q) \circ P,$$

on a

$$f_{Q \circ P} = M'_P f_{P \circ Q} = M'_P f_{Q \circ P},$$

et $f_P = f_{Q \circ P}$. De même $f_Q = f_{Q \circ P}$, donc $f_P = f_Q$.

Inversement, si $f_P = f_Q$,

$$M'_{P \circ Q} f_P = M'_Q M'_P f_P = M'_Q f_P = f_P,$$

donc $f_{P \circ Q} = f_P$. De même, $f_{Q \circ P} = f_P$, donc

$$f_{P \circ Q} = f_{Q \circ P}.$$

Car $\deg P \circ Q = \deg Q \circ P$, donc d'après la proposition 6

$$\exists U \in \mathscr{U}(f_{P \circ Q}) = \mathscr{U}(f_P)$$

tel que $P \circ Q = U \circ Q \circ P$.

Définition. Si m et n sont deux entiers $\geqslant 2$, on a

$$X^m \circ X^n = X^n \circ X^m,$$

donc $f_{X^m} = f_{X^n}$, on note cette forme linéaire f, et

$$T_m \circ T_n = T_n \circ T_m,$$

donc $f_{T_m} = f_{T_n}$, on la note f'.

D'après la proposition 7 et l'égalité $T_2 = 2X^2 - 1$, on a

$$\mathscr{U}(f) = \{aX : a \in C^*\} \quad \text{et} \quad \mathscr{U}(f') = \{X, -X\}.$$

Soient n un entier $\geqslant 3$, U et V deux polynômes du 1-er degré tels que $T_n \circ U = V \circ T_n$. Les images par T_n des points de ramification de T_n sont 1 et

-1, par conséquent les images par $T_n \circ U$ des points de ramification de $T_n \circ U$ sont 1 et -1 et les images par $V \circ T_n$ des points de ramification de $V \circ T_n$ sont $V(1)$ et $V(-1)$. On a donc

$$\{1, -1\} = \{V(1), V(-1)\},$$

d'où $V = \pm X$. Puisque $V \in \mathscr{W}(f')$, on a

$$M'_U f' = M'_U M'_{T_n} f' = M'_{T_n} M'_V f' = f', \quad U \in \mathscr{W}(f'), \quad U = \pm X.$$

LEMME. *Soient p et q deux entiers $\geqslant 2$ premiers entre eux, $R \in C[X]$. On a*

$$(M_{X^p} R) \circ X^q = M_{X^p}(R \circ X^q), \quad (M_{T_p} R) \circ T_q = M_{T_p}(R \circ T_q).$$

Démonstration. Soit Y une racine du polynôme de la variable X_1 à coefficients dans $C(X)$: $T_p(X_1) - T_q(X)$. Soit

$$Z = T_q(X) = T_p(Y).$$

$T_q(X_1) - Z$ étant irréductible sur $C(Z)$,

$$[C(X): C(Z)] = q.$$

De même

$$[C(Y): C(Z)] = p.$$

p et q étant premiers entre eux, $C(X)$ et $C(Y)$ sont linéairement disjoints sur $C(Z)$, donc

$$[C(X, Y): C(X)] = p,$$

et $T_p(X_1) - T_q(X)$ est irréductible sur $C(X)$. Soit Y' une racine du polynôme de la variable X_1: $T_p(X_1) - X$. On a

$$T_p(T_q(Y')) = T_q(T_p(Y')) = T_q(X),$$

donc $T_q(Y')$ est racine de $T_p(X_1) - T_q(X)$. Les polynômes en X_1

$$\prod_{T_p(Y') = X} (X_1 - T_q(Y')) \quad \text{et} \quad T_p(X_1) - T_q(X)$$

ont même degré, ils ont au moins une racine en commun, leurs coefficients appartiennent à $C(X)$ et le second est irréductible sur $C(X)$, ils ont donc mêmes racines. Par suite, $\forall R \in C[X]$,

$$\frac{1}{p} \sum_{T_p(Y) = T_q(X)} R(Y) = \frac{1}{p} \sum_{T_p(Y') = X} R \circ T_q(Y'),$$

$$(M_{T_p} R) \circ T_q = M_{T_p}(R \circ T_q).$$

On démontre de même l'autre égalité.

PROPOSITION 9. *Soient P et Q deux éléments de $C[X]$ tels que*

$$2 \leqslant \deg P < \deg Q, \quad \deg P \nmid \deg Q \quad \text{et} \quad P \circ Q = Q \circ P.$$

Il existe un polynôme du 1-er degré U tel que

$$f_{U^{-1} \circ P \circ U} = f \text{ ou } f'.$$

Démonstration. D'après la proposition 1 et la remarque qui la suit, il existe des polynômes P_1, P_2, Q_1, Q_2, R_1, R_2 tels que

$$P = R_1 \circ P_1 = P_2 \circ R_2, \quad Q = R_1 \circ Q_1 = Q_2 \circ R_2, \quad P_1 \circ Q_2 = Q_1 \circ P_2,$$

$\deg P_1 = \deg P_2 = p$ et $\deg Q_1 = \deg Q_2 = q$ premiers entre eux. On a alors $1 < p < q$. On a

$$P_2 \circ R_2 \circ Q_2 \circ R_2 = Q_2 \circ R_2 \circ P_2 \circ R_2,$$

donc

$$P_2 \circ R_2 \circ Q_2 = Q_2 \circ R_2 \circ P_2,$$

$$R_2 \circ P_2 \circ R_2 \circ Q_2 = R_2 \circ Q_2 \circ R_2 \circ P_2;$$

il existe donc P_3, Q_3, R_3 tels que $\deg P_3 = p$, $\deg Q_3 = q$,

$$R_2 \circ P_2 = P_3 \circ R_3, \quad R_2 \circ Q_2 = Q_3 \circ R_3.$$

On définit ainsi des suites de polynômes (P_k), (Q_k), (R_k), $k \geqslant 1$, telles que $\deg P_k = p$, $\deg Q_k = q$,

$$P_k \circ R_k \circ Q_k = Q_k \circ R_k \circ P_k,$$

$$R_k \circ P_k = P_{k+1} \circ R_{k+1}, \quad R_k \circ Q_k = Q_{k+1} \circ R_{k+1}.$$

On a donc

$$P_k \circ Q_{k+1} \circ R_{k+1} = Q_k \circ P_{k+1} \circ R_{k+1},$$

$$P_k \circ Q_{k+1} = Q_k \circ P_{k+1}.$$

Soit l un entier tel que $p^l > q$. On a

$$Q_2 \circ P_3 \circ P_4 \circ \ldots \circ P_{2+l} = P_2 \circ P_3 \circ \ldots \circ P_{1+l} \circ Q_{2+l},$$

$$\deg Q_2 = \deg Q_{2+l} = q,$$

$$\deg P_2 \circ P_3 \circ \ldots \circ P_{1+l} = \deg P_3 \circ P_4 \circ \ldots \circ P_{2+l} = p^l,$$

q premier avec p^l. D'après la proposition 5, Q_2 est de la forme $U \circ X^q \circ V$ ou $U \circ T_q \circ V$, où U et V sont des polynômes du 1-er degré. Dans le second cas, $P_3 \circ P_4 \circ \ldots \circ P_{2+l}$ est de la forme $V^{-1} \circ T_{p^l} \circ W$, W du 1-er degré.

Si Q_2 est de la forme $U \circ X^q \circ V$, d'après la proposition 5, l'égalité

$P_1 \circ Q_2 = Q_1 \circ P_2$ implique que (P_2, Q_2) est de la forme

$$(V_1^{-1} \circ X^p \circ W_1, S_1^{-1} \circ X^n T(X^p) \circ W_1)$$

et l'égalité $P_2 \circ Q_3 = Q_2 \circ P_3$ implique que (P_2, Q_2) est de la forme

$$(U_2 \circ X^p \circ S_2, U_2 \circ X^{\bar{n}} \tilde{T}^p \circ V_2),$$

car sinon les indices de ramification de Q_2 seraient $\leqslant 2$, contradiction. La moyenne des racines de $X^n T(X^p)$ est 0, donc la moyenne des racines de $S_1^{-1} \circ X^n T(X^p) \circ W_1$ est $W_1^{-1}(0)$, c'est la moyenne des racines de $Q_2 = U \circ X^q \circ V$, donc

$$W_1^{-1}(0) = V^{-1}(0).$$

$X^{\bar{n}} \tilde{T}^p$ a au moins une racine multiple, donc $Q_2 - U_2(0)$ en a, $U(0) = U_2(0)$. Puisque

$$V_1^{-1} \circ X^p \circ W_1 = U_2 \circ X^p \circ S_2,$$

il vient $V_1^{-1}(0) = U_2(0)$. On a donc

$$W_1 \circ V^{-1}(0) = 0, \qquad U^{-1} \circ V_1^{-1}(0) = 0,$$

donc $\exists a \in C^*$ tel que

$$U^{-1} \circ V_1^{-1} \circ X^p \circ W_1 \circ V^{-1} = aX^p, \qquad P_2 = U \circ aX^p \circ V.$$

Si Q_2 est de la forme $U \circ T_q \circ V$, supposons d'abord $p \geqslant 3$. D'après la proposition 5, l'égalité $P_2 \circ Q_3 = Q_2 \circ P_3$ implique que (P_2, Q_2) est de la forme

$$(U_2 \circ T_p \circ S_2, U_2 \circ T_q \circ V_2),$$

car sinon Q_2 serait de la forme $U_2 \circ X^n T^p \circ V_2$ et aurait un indice de ramification $\geqslant 3$, contradiction. L'égalité $P_1 \circ Q_2 = Q_1 \circ P_2$ implique que (P_2, Q_2) est de la forme

$$(V_1^{-1} \circ T_p \circ W_1, S_1^{-1} \circ T_q \circ W_1),$$

car sinon P_2 aurait un indice de ramification $\geqslant 3$, contradiction. L'égalité

$$S_1^{-1} \circ T_q \circ W_1 = U \circ T_q \circ V$$

entraîne $W_1 = \pm V$. Comme

$$U_2 \circ T_q \circ V_2 = U \circ T_q \circ V,$$

on a $U_2 = U \circ \pm X$. Ensuite

$$V_1^{-1} \circ T_p \circ W_1 = U_2 \circ T_p \circ S_2,$$

donc $V_1^{-1} = U_2 \circ \pm X$. On a donc

$$P_2 = V_1^{-1} \circ T_p \circ W_1 = U \circ \pm T_p \circ V.$$

Supposons maintenant $p = 2$. D'après la proposition 5, l'égalité $P_2 \circ Q_3 = Q_2 \circ P_3$ implique que (P_2, Q_2) est de la forme

$$(U_2 \circ X^2 \circ S_2,\ U_2 \circ X^n \circ T^2 \circ V_2).$$

Le polynôme $Q_2 - U_2(0)$ a au moins une racine multiple, donc $U_2(0) = U(\pm 1)$. Par conséquent, il existe S_3 tel que

$$P_2 = U \circ \pm T_2 \circ S_3.$$

De l'égalité

$$T_2 \circ S_3 \circ Q_3 = \pm T_q \circ V \circ P_3 = T_q \circ \pm V \circ P_3$$

on déduit d'après la remarque suivant la proposition 5 que (P_3, Q_3) est de la forme $(V^{-1} \circ \pm T_2 \circ W_3,\ S_3^{-1} \circ T_q \circ W_3)$. On a

$$Q_3 \circ P_4 \circ \ldots \circ P_{3+l} = P_3 \circ \ldots \circ P_{2+l} \circ Q_{3+l},$$

donc d'après la proposition 5, il existe U_4, V_4, S_4 tels que

$$Q_3 = U_4 \circ T_q \circ V_4, \qquad P_3 \circ \ldots \circ P_{2+l} = U_4 \circ T_{2l} \circ S_4.$$

$S_3^{-1} \circ T_q \circ W_3 = U_4 \circ T_q \circ V_4$, donc $S_3^{-1} = U_4 \circ \pm X$. L'égalité

$$U_4 \circ T_{2l} \circ S_4 = V^{-1} \circ T_{2l} \circ W$$

entraîne $U_4 = V^{-1} \circ \pm X$. On a donc

$$S_3^{-1} = V^{-1} \circ \pm X, \qquad S_3 = \pm V, \qquad P_2 = U \circ \pm T_2 \circ V.$$

Dans tous les cas, (P_2, Q_2) est donc égal à

$$(U \circ aX^p \circ V,\ U \circ X^q \circ V) \quad \text{ou} \quad (U \circ \pm T_p \circ V,\ U \circ T_q \circ V).$$

Posons $R = V \circ R_2 \circ U$. Dans le premier cas on a

$$\begin{aligned} aX^p \circ R \circ X^q &= U^{-1} \circ P_2 \circ R_2 \circ Q_2 \circ V^{-1} \\ &= U^{-1} \circ Q_2 \circ R_2 \circ P_2 \circ V^{-1} = X^q \circ R \circ aX^p \end{aligned}$$

et

$$U^{-1} \circ P \circ U = U^{-1} \circ P_2 \circ R_2 \circ U = aX^p \circ R.$$

Dans le second cas on a

$$\sigma T_p \circ R \circ T_q = T_q \circ R \circ \sigma T_p \quad \text{et} \quad U^{-1} \circ P \circ U = \sigma T_p \circ R$$

avec $\sigma = \pm 1$. Si q est pair et $\sigma = -1$, on a

$$\begin{aligned} T_p \circ -R \circ T_q &= -T_p \circ R \circ T_q \circ -X \\ &= T_q \circ R \circ -T_p \circ -X = T_q \circ -R \circ T_p \end{aligned}$$

et

$$U^{-1} \circ P \circ U = T_p \circ -R;$$

en remplaçant dans ce cas R par $-R$, on peut supposer qu'on a toujours $\sigma T_q = T_q \circ \sigma X$, et donc

$$\sigma T_p \circ T_q = T_q \circ \sigma T_p.$$

Soient $S \in C[X]$ et n un entier tel que $\deg S < p^n$.
Dans le premier cas, soient b une racine q^{n-1}-ième de a, et

$$c = b^{(q^n - p^n)/(q-p)}.$$

On a

$$(aX^p \circ R)^{(n)} \circ X^{q^n} = (X^q \circ R)^{(n)} \circ cX^{p^n} \quad \text{et} \quad M_{(aX^p \circ R)^{(n)}} M_{X^{q^n}} = M_{(X^q \circ R)^{(n)} \circ cX} M_{X^{p^n}}.$$

p^n et q^n étant premiers entre eux, on a d'après le lemme

$$M_{X^{p^n}}(S \circ X^{q^n}) = (M_{X^{p^n}} S) \circ X^{q^n}.$$

On a donc

$$\begin{aligned} f_{aX^p \circ R}(S) &= M_{(aX^p \circ R)^{(n)}} S = M_{(aX^p \circ R)^{(n)}} M_{X^{q^n}}(S \circ X^{q^n}) \\ &= M_{(X^q \circ R)^{(n)} \circ cX} M_{X^{p^n}}(S \circ X^{q^n}) = M_{(X^q \circ R)^{(n)} \circ cX}((M_{X^{p^n}} S) \circ X^{q^n}) \\ &= f_{X^p}(S), \end{aligned}$$

$$f_{U^{-1} P U} = f_{aX^p R} = f_{X^p} = f.$$

Dans le second cas, on a

$$(\sigma T_p \circ R)^{(n)} \circ T_q^{(n)} = (T_q \circ R)^{(n)} \circ (\sigma T_p)^{(n)} = (T_{q \circ R})^{(n)} \circ \pm T_p^{(n)}$$

et

$$M_{(\sigma T_p \circ R)^{(n)}} M_{T_q^{(n)}} = M_{(T_q \circ R)^{(n)} \circ \pm X} M_{T_p^{(n)}}.$$

D'après le lemme,

$$M_{T_{p^n}}(S \circ T_{q^n}) = (M_{T_{p^n}} S) \circ T_{q^n}, \qquad M_{T_p^{(n)}}(S \circ T_q^{(n)}) = (M_{T_p^{(n)}} S) \circ T_q^{(n)}.$$

On a donc

$$\begin{aligned} f_{\sigma T_p \circ R}(S) &= M_{(\sigma T_p R)^{(n)}} M_{T_q^{(n)}}(S \circ T_q^{(n)}) = M_{(T_q \circ R)^{(n)} \circ \pm X} M_{T_p^{(n)}}(S \circ T_q^{(n)}) \\ &= M_{(T_q R)^{(n)} \cdot X}((M_{T_p^{(n)}} S) \circ T_q^{(n)}) = f_{T_p}(S), \end{aligned}$$

$$f_{U^{-1} \circ P \circ U} = f_{\sigma T_p \circ R} = f_{T_p} = f'.$$

PROPOSITION 10. *Soient P et Q deux éléments de $C[X]$ tels que*

$$2 \leqslant \deg P \leqslant \deg Q \quad \text{et} \quad f_P = f_Q.$$

Alors ou bien $\deg P \mid \deg Q$, *ou bien il existe un polynôme du 1-er degré U tel que f_P soit égal à $M'_U f$ ou $M'_U f'$.*

Démonstration. Supposons que $\deg P \nmid \deg Q$ et que f_P n'est pas de la forme $M'_U f$, U polynôme du 1-er degré.

Soient $\alpha = f_P(X)$, $U = X - \alpha$, et d défini comme dans la proposition 7. Alors $d \neq 0$, car sinon $U \circ P \circ U^{-1}$ serait un monôme, d'où

$$M'_{U^{-1}} f_P = f_{U \circ P \circ U^{-1}} = f, \quad f_P = M'_U f.$$

$U \circ P \circ U^{-1}$ est de la forme $X^n T(X^d)$, où $T \in C[X]$ est tel que $T(0) \neq 0$, donc en posant $P_1 = X^n T^d$, on a le diagramme commutatif

$$\begin{array}{ccc} & \xrightarrow{U \circ P \circ U^{-1}} & \\ x^d \downarrow & \longrightarrow & \downarrow x^d \\ & P_1 & \end{array}$$

On a de même un polynôme Q_1 faisant commuter le diagramme

$$\begin{array}{ccc} & \xrightarrow{U \circ Q \circ U^{-1}} & \\ x^d \downarrow & \longrightarrow & \downarrow x^d \\ & Q_1 & \end{array}$$

Comme $f_P = f_Q$, il existe d'après les propositions 8 et 7 une racine d-ième de l'unité a telle que

$$P \circ Q = U^{-1} \circ aX \circ U \circ Q \circ P.$$

Si $d = 1$, on a $P \circ Q = Q \circ P$, et la proposition 10 résulte immédiatement de la proposition 9. On suppose maintenant $d > 1$. On a

$$U \circ P \circ U^{-1} \circ U \circ Q \circ U^{-1} = aU \circ Q \circ U^{-1} \circ U \circ P \circ U^{-1},$$

donc

$$P_1 \circ Q_1 = Q_1 \circ P_1.$$

$\deg P_1 = \deg P$, $\deg Q_1 = \deg Q$, $\deg P_1 \nmid \deg Q_1$, donc d'après la proposition 9 il existe un polynôme du 1-er degré V tel que

$$f_{V \circ P_1 \circ V^{-1}} = f \text{ ou } f'.$$

Soit $p = \deg P$.

Si

$$f_{V \circ P_1 \circ V^{-1}} = f, \quad f_{V \circ P_1 \circ V^{-1}} = f_{X^p},$$

donc, d'après la proposition 6, $\exists b \in C^*$ tel que

$$V \circ P_1 \circ V^{-1} = bX^p, \quad X^n T^d = P_1 = V^{-1} \circ bX^p \circ V,$$

$X^n T^d$ a au moins une racine multiple donc $V^{-1} \circ bX^p \circ V$ aussi, $V(0) = 0$, $X^n T^d$ est de la forme cX^p, donc T est constant et $U \circ P \circ U^{-1} = X^n T(X^d)$ est un monôme, on a vu que c'est impossible.

On a donc

$$f_{V \circ P_1 \circ V^{-1}} = f' = f_{T_p}, \quad V \circ P_1 \circ V^{-1} = \pm T_p, \quad X^n T^d = P_1 = V^{-1} \circ \pm T_p \circ V.$$

Les indices de ramification de $V^{-1} \circ \pm T_p \circ V$ étant égaux à 2, ceci montre que $d = 2$, et $X^n T^d$ ayant au moins une racine multiple, $V(0) = 1$ ou -1. En remplaçant éventuellement V par $-V$, on peut supposer que $V(0) = -1$. Il existe alors $\beta \in C^*$ tel que

$$V = 2\beta^2 X - 1.$$

$X^2 \circ U \circ P \circ U^{-1} = V^{-1} \circ \pm T_p \circ V \circ X^2$, donc

$$V \circ X^2 \circ U \circ P \circ U^{-1} = \pm T_p \circ V \circ X^2.$$

On a $V \circ X^2 = 2(\beta X)^2 - 1 = T_2 \circ \beta X$, donc

$$T_2 \circ \beta X \circ U \circ P \circ U^{-1} = \pm T_p \circ T_2 \circ \beta X,$$

$$T_2 \circ \beta U \circ P \circ (\beta U)^{-1} = \pm T_p \circ T_2.$$

On en déduit que

$$M'_{(\beta U)^{-1}} f_P = f_{\beta U \circ P \circ (\beta U)^{-1}} = M'_{T_2} f_{\pm T_p} = f', \quad f_P = M'_{\beta U} f'.$$

PROPOSITION 11. *Deux éléments P et Q de $C[X]$ de degrés $\geqslant 2$ vérifient $f_P = f_Q$ si et seulement si*

ou bien il existe $U \in C[X]$ de degré 1, m et n entiers $\geqslant 2$, a et b dans C^* tels que

$$P = U^{-1} \circ aX^m \circ U, \quad Q = U^{-1} \circ bX^n \circ U;$$

ou bien il existe $U \in C[X]$ de degré 1, m et n entiers $\geqslant 2$, a et b dans $\{-1, 1\}$ tels que

$$P = U^{-1} \circ aT_m \circ U, \quad Q = U^{-1} \circ bT_n \circ U;$$

ou bien il existe $R \in C[X]$ de degré $\geqslant 2$, $U \in \mathcal{U}(f_R)$, $V \in \mathcal{U}(f_R)$, m et n entiers $\geqslant 1$ tels que

$$P = U \circ R^{(m)}, \quad Q = V \circ R^{(n)}.$$

Démonstration. La suffisance est évidente.

Réciproquement, soient P et Q tels que $f_P = f_Q$.

S'il existe U tel que $f_P = M'_U f$, soient m et n les degrés de P et Q. On a $f_{U \circ P \circ U^{-1}} = f_{X^m}$, donc $\exists a \in C^*$ tel que

$$U \circ P \circ U^{-1} = aX^m, \quad P = U^{-1} \circ aX^m \circ U.$$

De même, Q est de la forme $U^{-1} \circ bX^n \circ U$.

S'il existe U tel que $f_P = M'_U f'$, on montre de façon analogue qu'il existe a et b dans $\{-1, 1\}$ tels que

$$P = U^{-1} \circ aT_m \circ U, \quad Q = U^{-1} \circ bT_n \circ U.$$

Sinon, d'après la proposition 10, un des nombres $\deg P$ et $\deg Q$ divise l'autre. Supposons, par exemple, $\deg P \mid \deg Q$. L'égalité $f_P = f_Q$ implique qu'il existe U_1 tel que

$$P \circ Q = U_1 \circ Q \circ P,$$

et d'après la proposition 1 il existe S, P_1, Q_1 tels que

$$P = P_1 \circ S, \quad Q = Q_1 \circ S, \quad \deg S = \mathrm{PGCD}(\deg P, \deg Q) = \deg P,$$

donc

$$\deg P_1 = 1 \quad \text{et} \quad Q = Q_1 \circ P_1^{-1} \circ P = R_1 \circ P.$$

Puisque $f_P = f_Q$, on a

$$M'_P f_P = f_P = M'_Q f_P = M'_P M'_{R_1} f_P, \quad f_P = M'_{R_1} f_P.$$

Si $\deg R_1 \neq 1$, $f_{R_1} = f_P$, elle n'est pas de la forme $M'_U f$ ou $M'_U f'$, on applique donc le même procédé aux polynômes P et R_1, ce qui permet de définir un nouveau couple de polynômes (R_2, S_2). On définit ainsi une suite finie (R_k, S_k) de couples de polynômes ayant les propriétés suivantes: $(R_0, S_0) = (P, Q)$, R_k et S_k s'écrivent comme composés de R_{k+1} et S_{k+1}, $f_{R_{k+1}} = f_{S_{k+1}} = f_{R_k}$, $\deg R_{k+1} + \deg S_{k+1} < \deg R_k + \deg S_k$. La suite s'arrête quand le degré d'un des polynômes R_k ou S_k est égal à 1, disons $\deg S_l = 1$, et posons $R = R_l$. Alors P et Q s'écrivent comme composés de polynômes égaux à R_l ou S_l, donc il existe deux entiers m et $n \geqslant 1$ tels que

$$\deg P = (\deg R)^m, \quad \deg Q = (\deg R)^n.$$

$f_P = f_R = f_{R^{(m)}}$, $\deg P = \deg R^{(m)}$, donc, d'après la proposition 6, $\exists U \in \mathscr{U}(f_R)$ tel que $P = U \circ R^{(m)}$. De même, $\exists V \in \mathscr{U}(f_R)$ tel que $Q = V \circ R^{(n)}$.

TRAVAUX CITÉS

[1] H. Brolin, *Invariant sets under iteration of rational functions*, Ark. Mat. 6 (1965), pp. 103–144.

[2] G. Julia, *Mémoire sur la permutabilité des fractions rationnelles*, Ann. Sci. École Normale Sup. 39 (1922), pp. 131–215.

[3] J. F. Ritt, *Permutable rational functions*, Trans. Amer. Math. Soc. 24 (1923), pp. 399–448.

[4] A. Schinzel, *Selected topics on polynomials*, Ann Arbor 1982.

[5] J. P. Serre, *Corps locaux*, Paris 1962.

Reçu par la Rédaction le 29. 5. 1985