Construction de polynômes de $Q[X]$ (à racines réelles) dont le groupe de Galois sur $\mathbb{Q}$ est cyclique d'ordre 3 ou 4 ou 6 (à l'aide de fonctions homographiques d'ordre 3 ou 4 ou 6)

http://alain.pichereau.pages.perso-orange.fr
marc.pichereau@wanadoo.fr

1) Introduction

Cette méthode consiste à construire des polynômes vérifiant les hypothèses du théorème de Galois suivant (voir P12.5 de ma page sur Galois : alain.pichereau.pages.perso-orange.fr/equation7.pdf) :

soit P dans $\mathbb{Q}[X]$ irréductible, de degré $n \geq 2$ (rappel : étant irréductible, toutes les racines (dans $\mathbb{C}$) de P sont simples)

tel que ses n racines soient $r, f(r), f^{(2)}(r), \ldots, f^{(n-1)}(r)$

avec f fonction rationnelle et $f^{(2)} = f \circ f, f^{(3)} = f \circ f \circ f,$ etc,

alors le groupe de Galois (sur $\mathbb{Q}$) de P est cyclique d'ordre n,

c'est-à-dire isomorphe à $\mathbb{Z}/n\mathbb{Z}$, groupe que l'on peut noter C_n.

Exemple : $P(X) = X^4 - 10X^2 + 5$ a pour racines $\alpha = \sqrt{5 + 2\sqrt{5}}, -\alpha, \beta = \sqrt{5 - 2\sqrt{5}}, -\beta,$ soient $\alpha, f(\alpha), f^{(2)}(\alpha), f^{(3)}(\alpha)$ avec $f(X) = \frac{X^2 - 5}{2X},$ et comme P est irréductible (Eisenstein), $Gal(P) = C_4$.

Ce résultat se généralise : tous les polynômes $P_{s,t} = X^4 + 2s(t^2 + 1)X^2 + s^2(t^2 + 1),$ où s et t sont des rationnels tels que $P_{s,t}$ soit irréductible sur $\mathbb{Q}$ ont pour racines $r, f(r), f^{(2)}(r), f^{(3)}(r),$ avec f fonction rationnelle (je laisse le lecteur la déterminer), et donc ils ont tous C_4 comme groupe de Galois.

Dans la méthode exposée ci-dessous, on se limitera cependant à l'utilisation de fonctions rationnelles $f(X) = \frac{aX + b}{cX + d} \in \mathbb{Q}(X),$ avec $ad - bc \neq 0,$ qui sont d'ordre fini n.

Elles permettent d'obtenir des polynômes $\in \mathbb{Q}[X]$ de degré n ayant un groupe de Galois sur $\mathbb{Q}$ cyclique et d'ordre n.

Le cas $n = 2$ est sans intérêt car tout polynôme de degré 2 de $\mathbb{Q}[X]$ a un groupe de Galois cyclique, réduit à $\{id\}$ si le polynôme est réductible, et d'ordre 2 s'il est irréductible sur $\mathbb{Q}$.

On verra au 1.1) du II de l'annexe 1 la caractérisation des $f(X) = \frac{aX + b}{cX + d} \in \mathbb{R}(X)$ (il s'agit bien de $\mathbb{R}(X)$) avec $ad - bc \neq 0$ qui sont d'ordre $n \geq 3$ (cela implique $a + d \neq 0$) et au 2) du II de l'annexe 1 on verra que celles d'ordre 2 sont caractérisées par $a + d = 0$.

Malheureusement, cela ne signifie pas que $\forall n \geq 2,$ il existe $f(X) = \frac{aX + b}{cX + d} \in \mathbb{Q}(X),$ avec $ad - bc \neq 0$ qui soit d'ordre n : cela n'est vrai que si $n \in \{2; 3; 4; 6\}$ (voir le 5) du III de l'annexe 1).

2) Le résultat :

Note : on renverra, dans les annexes, à ce résultat par voir le 2)PP.

Soit $f(X) = \frac{aX+b}{cX+d} \in \mathbb{Q}(X)$ avec $ad-bc \neq 0$ et d'ordre $n = 3$ ou 4 ou 6 (voir le 5) du III de l'annexe 1) ; d'après la remarque 2 du 1.1) du II de l'annexe 1, pour tout $1 \leq i \leq n-1$, $f^{(i)}$ n'est pas un polynôme.

Alors

2.1) si r est algébrique sur $\mathbb{Q}$ de degré ≥ 3, alors $r, f(r), f^{(2)}(r), \ldots, f^{(n-1)}(r)$ sont définis et distincts.

Note : ce résultat ne sera pas utilisé ici.

2.2) soit $r \in \mathbb{C}$ tel que $f(r), f^{(2)}(r), \ldots, f^{(n-1)}(r)$ soient définis et avec $r \neq f(r)$, alors $r, f(r), f^{(2)}(r), \ldots, f^{(n-1)}(r)$ sont n nombres distincts.

Note : on verra en annexe 1 (remarque 3 du 1.1) du II) que r réel implique $r \neq f(r)$.

2.3) pour tout $1 \leq i \leq n-1$, $f^{(i)} = \frac{U_i}{V_i}$ avec U_i et V_i deux polynômes de $\mathbb{Q}[X]$ tels que $d^\circ U_i \leq 1$ (U_i peut être constant) et $d^\circ V_i = 1$ (car $f^{(i)}$ n'est pas un polynôme).

Bien sûr, U_i et V_i sont définies à une constante multiplicative près ; il peut être commode de les choisir à coefficients entiers.

On peut posera $f^{(0)} = id = \frac{U_0}{V_0}$ avec $U_0(X) = X$ et $V_0(X) = 1$.

2.3.1) Pour i et j distincts dans $\{1;2;\ldots;n-1\}$, V_i et V_j n'ont pas de racine commune, de même si U_i et U_j ont une racine, elle ne peut être commune.

2.3.2) Pour $i \in \{1;2;\ldots;n-1\}$, 0 racine de $V_i \Leftrightarrow U_{n-i}$ n'a pas de racine.

2.3.3) Si, pour $i \in \{1;2;\ldots;n-1\}$, U_i a une racine, c'est $f^{(n-i)}(0)$; voir exemple 2.

2.3.4) Si n est pair, $f^{(\frac{n}{2})}$ est d'ordre 2, et (voir annexe 1), $f^{(\frac{n}{2})}(X) = \frac{a'X+b'}{c'X-a'}$ avec $a' \neq 0$ ou $\frac{\lambda}{X}$ avec $\lambda \neq 0$

Si n est pair et 0 racine de $V_{\frac{n}{2}}$, alors $f^{(\frac{n}{2})}(X) = \frac{\lambda}{X}$ avec $\lambda \neq 0$

2.3.5) Pour i_0 dans $\{1;2;\ldots;n-1\}$, si $f^{(i_0)}(X) = \frac{U_{i_0}}{\xi X}$, alors pour i dans $\{1;2;\ldots;n-1\}$, $V_i = c_i U_{i-i_0}$ où c_i est une constante, $i-i_0$ étant pris modulo n dans $\{0;1;2;\ldots;n-1\}$. Donc U_{i-i_0} a une racine, celle de V_i, laquelle est donc, d'après le 2.3.3), $f^{(n-i+i_0)}(0)$.

Si $i = i_0$, on obtient $V_{i_0}(X) = \xi U_0(X) = \xi X$ (attendu, car $f^{(i_0)}(X) = \frac{U_{i_0}}{V_{i_0}}$) qui a bien pour racine $f^{(n-i_0+i_0)}(0) = id(0) = 0$.

On verra au 2.8) le cas particulier : $f^{(i_0)}(X) = \frac{\lambda}{X}$, qui n'est possible que si n est pair.

2.4) $X + f(X) + f^{(2)}(X) + \ldots + f^{(n-1)}(X) = \frac{N(X)}{D(X)}$ avec N et D deux polynômes unitaires de $\mathbb{Q}[X]$, N étant de degré n et D de degré $n-1$.

D est, à une constante multiplicative près, le produit des dénominateurs V_i des $f^{(i)}(X)$ pour $i = 1, 2, \ldots, n-1$; les racines de D sont donc rationnelles et "connues".

N et D n'ont pas de racine commune.

2.5) On pose, pour μ dans $\mathbb{Q}[X]$, $P_\mu = N + \mu D$: c'est un polynôme unitaire de degré n et on notera que les coefficients de P_μ sont tous des fonctions affines de μ.

P_μ a son terme constant indépendant de $\mu \Leftrightarrow D$ a son terme constant nul $\Leftrightarrow$ un V_i (i dans $\{1;2;\ldots;n-1\}$) a pour racine 0.

$P_\mu(f(X)) = \frac{N(f(X))}{N(X)}P_\mu(X) = \frac{D(f(X))}{D(X)}P_\mu(X)$ (ces égalités n'exigent pas l'irréductibilité de P_μ).

Soient $\theta_1, \theta_2, \ldots, \theta_{n-1}$ les racines distinctes de $V_1, V_2, \ldots, V_{n-1}$ rangées par ordre croissant (θ_i n'est donc pas forcément la racine de V_i) :

P_μ a n racines réelles distinctes de la forme $r, f(r), f^{(2)}(r), \ldots, f^{(n-1)}(r)$, chacun des n intervalles $]-\infty;\theta_1[,]\theta_1;\theta_2[,]\theta_2;\theta_3[, \ldots,]\theta_{n-2};\theta_{n-1}[,]\theta_{n-1};+\infty[$ contenant une et une seule racine de P_μ.

Si P_μ est irréductible sur $\mathbb{Q}$, son groupe de Galois est C_n.

Remarque 1 : on notera qu'ici $f^{(n)} = id$, alors que dans le théorème de Galois cité en introduction cela n'est pas exigé : voir d'ailleurs l'exemple cité dans cette introduction où $f^{(4)} \neq id$ (calculer $f^{(4)}(1)$ par exemple).
Je n'ai aucune régle pour caractériser les μ tels que P_μ soit irréductible ; bien sûr si P_μ est de degré 3, il sera irréductible si et seulement si il n'a aucune racine rationnelle.

Si P_μ a une racine rationnelle, alors toutes ses racines sont rationnelles et son groupe de Galois est le groupe réduit au neutre ; voir un cas de l'exemple 1 ci-dessous.

Remarque 2 : il est facile de trouver $\mu \in \mathbb{Q}$ tel que P_μ ait une racine rationnelle : il suffit de prendre $\mu = -\frac{N(r)}{D(r)}$ où r est un rationnel non racine de D (on a bien $\mu \in \mathbb{Q}$), puisque P_μ a alors r comme racine rationnelle.

P_μ peut être réductible sans avoir de racine rationnelle ; voir deux cas dans l'exemple 2 ci-dessous ($n = 4$) où le groupe de Galois est C_2.

Remarque 3 : on peut déterminer des approximations des plus grandes et plus petites racines de P_μ, pour $|\mu|$ infini.
Par exemple, si $P_\mu(X) = X^4 + \mu X^3 - 6X^2 - \mu X + 1$ (exemple 4 de l'annexe 2), alors $r_\mu = -\mu - \frac{5}{\mu} + \frac{21}{\mu^2}$ est une approximation de la plus grande racine de P_μ lorsque μ tend vers $-\infty$ et est une approximation de la plus petite racine de P_μ lorsque μ tend vers $+\infty$, les erreurs (absolues) étant en $O(\frac{1}{\mu^4})$: $r_{-50} = 50,099832$ alors que la plus grande racine de P_{-50} est $50,0998325\ldots$ soit une erreur d'environ 5×10^{-7}, alors que $\frac{1}{50^4} = 1.6 \times 10^{-7}$.

2.6) N n'a pas de terme en X^{n-1} et donc le coefficient de X^{n-1} dans P_μ est μ.

2.7) Posons $s_k(X)$ la somme des produits de k éléments distincts de $\{X; f(X); f^{(2)}(X); \ldots; f^{(n-1)}(X)\}$, pour $k \in \{1; 2; \ldots; n\}$.
On notera que pour $k \geq 1$, $s_k(f(X)) = s_k(X)$ car l'ensemble $\{X; f(X); f^{(2)}(X); \ldots; f^{(n-1)}(X)\}$ est invariant si on remplace X par $f(X)$ et donc pour tout $j \geq 1$, $s_k(f^{(j)}(X)) = s_k(X)$.
Le résultat vu au 2.4) et 2.5), à savoir, $s_1(X) = \frac{P_0(X)}{D(X)}$, se généralise à tout s_k pour $k \in \{2; 3; \ldots; n\}$.

Pour tout $k \in \{2; \ldots; n\}$,

2.7.1) Si le coefficient de X^{n-k} dans D est non nul, il existe un seul $\beta_k \in \mathbb{Q}$ tel que le coefficient de X^{n-k} dans P_{β_k} soit nul, et alors $\alpha_k \in \mathbb{Q}$ étant le coefficient de X^{n-k} de D, on a $s_k(X) = \alpha_k \frac{P_{\beta_k}(X)}{D(X)} = \alpha_k(s_1(X) + \beta_k)$, cad s_k est une fonction affine de s_1.
Note 1 : évidemment la formule ci-dessus est vraie pour $k = 1$ avec $\alpha_1 = 1$ et $\beta_1 = 0$.

Note 2 : on verra au 2.7.2) le cas où X^{n-k} n'apparaît pas dans D.

Cas particulier $k = n$: si le terme constant de D est non nul (cad $D(0) \neq 0$), il existe un seul $\beta_n \in \mathbb{Q}$ tel que le terme constant de P_{β_n} soit nul et alors $P_{\beta_n}(X) = \tau X \prod_{i=1}^{n-1} U_i(X)$, τ est une constante rationnelle égale à l'inverse du coefficient de tête de $\prod_{i=1}^{n-1} U_i$; donc pour tout $i \in \{1;2;\ldots;n-1\}$, $d^\circ U_i = 1$.
On peut le vérifier dans le cas de l'exemple 1 ci-dessous : $P_{\frac{9}{2}}(X) = \frac{1}{2} X U_1(X) U_2(X)$.

On en déduit aussi $D(0) = (-1)^{n+1} \dfrac{\text{coefficient de tête de} \prod_{i=1}^{n-1} U_i}{\text{coefficient de tête de} \prod_{i=1}^{n-1} V_i}$

2.7.2) Si le coefficient de X^{n-k} dans P_μ est une constante c indépendante de μ (cad X^{n-k} n'apparaît pas dans D mais peut apparaître dans N) alors $s_k(X) = (-1)^k c$.
Note : le résultat est bien vrai si $c = 0$ (cad X^{n-k} n'apparaît ni dans N, ni dans D) et on retrouve d'ailleurs ce que donnerait le 2.7.1), car alors pour tout $\beta_k \in \mathbb{Q}$, le coefficient de X^{n-k} dans P_{β_k} serait nul et en choisissant deux distincts, β_k et β'_k on aurait $s_k(X) = \alpha_k(s_1(X) + \beta_k) = \alpha'_k(s_1(X) + \beta'_k)$ et comme s_1 est une fraction rationnelle non constante nécessairement $\alpha_k = \alpha'_k$, puis $\alpha_k = 0$, soit $s_k(X) = 0$.
Cas particulier $k = n$: en fait le terme constant de P_μ ne peut être 0 pour tout $\mu \in \mathbb{Q}$ (car sinon $N(0) = D(0) = 0$ ce qui est impossible d'après le 2.4)), par contre le terme constant de P_μ peut être une constante $c \neq 0$ indépendante de μ : voir exemple 2 ci-dessous et le 2.8) donnant une condition suffisante pour qu'il en soit ainsi.
Dans ce cas, $X \prod_{i=1}^{n-1} f^{(i)}(X) = (-1)^n c$, cad $X \prod_{i=1}^{n-1} U_i(X) = (-1)^n c \prod_{i=1}^{n-1} V_i(X)$ et donc obligatoirement, un V_i a pour racine 0, un U_i est une constante, et les $n-2$ autres sont des V_i, donc sont de degré 1.

2.8) $f^{(i)}(X) = \frac{\lambda}{X}$ ($\lambda \neq 0$) n'est possible que si n est pair et si $i = \frac{n}{2}$.
On a vu au 3.3.4) que si n est pair, $f^{(\frac{n}{2})}$ est d'ordre 2 (rappel : f est d'ordre $n \geq 3$).
On verra au 1.2) de l'annexe 1, que si n est pair, $f^{(\frac{n}{2})}(X) = \frac{\lambda}{X}$ (λ constante) $\Leftrightarrow a = d$.
C'est le cas de $f(X) = \frac{X+1}{-X+1}$ qui est d'ordre 4 et $f^{(2)}(X) = \frac{-1}{X}$.
Note : $\lambda \neq 0$ car le $ad - bc$ de f est non nul, donc il en est de même pour ses itérés : voir annexe 1.
Si n est pair et si $f^{(\frac{n}{2})}(X) = \frac{\lambda}{X}$ alors $s_n(X) = X f(X) f^{(2)}(X) \ldots f^{(n-1)}(X) = \lambda^{\frac{n}{2}}$ et $P_\mu(0) = N(0) = \lambda^{\frac{n}{2}} \neq 0$.

Voici deux exemples, les calculs étant détaillés à l'annexe 2 dans laquelle on trouvera d'autres exemples.

Exemple 1 : $f(X) = -\frac{X+3}{X+2}$ est d'ordre $n = 3$ et $P_\mu(X) = X^3 + \mu X^2 + (3\mu - 9)X + 2\mu - 9$.
P_0 est irréductible ; ses racines sont $r \simeq -2,22668, f(r) \simeq 3,41147, f^{(2)}(r) \simeq -1,18479$.
On peut vérifier le 2.3.3) : $-3 = f^{(2)}(0)$ est racine de U_1, $-\frac{3}{2} = f(0)$ est racine de U_2.

-2 et -1 étant les racines des V_i, on vérifie le 5) :
$r \in]-\infty;-2[, f(r) \in]-2;-1[, f^{(2)}(r) \in]-1;+\infty[$.
$P_{\frac{9}{2}}(X) = X^3 + \frac{9}{2}X^2 + \frac{9}{2}X$ est réductible puisque factorisable par X :
$P_{\frac{9}{2}}(X) = X(X+3)(X+\frac{3}{2}) = \frac{1}{2}XU_1(X)U_2(X)$, ce qui correspond au cas particulier $k = n$ du 2.7.1)
Les racines de $P_{\frac{9}{2}}$ sont $0, f(0) = -\frac{3}{2}, f^{(2)}(0) = -3$, toutes rationnelles et donc le groupe de Galois de $P_{\frac{9}{2}}$ est le groupe réduit à l'élément neutre.

Exemple 2 : pour tout $m \in \mathbb{Q}^*$, $f(X) = m(1 - \frac{m}{2X})$ est d'ordre $n = 4$ et
$P_{\mu,m}(X) = X^4 + \mu X^3 - 3(\mu\frac{m}{2} + m^2)X^2 + (\mu\frac{m^2}{2} + 2m^3)X - \frac{m^4}{4}$.
On peut vérifier le 2.3.5) avec $i_0 = 1$, puisque $f(X) = \frac{U_1(X)}{\xi X}$ et on doit donc avoir $V_i = c_i U_{i-1}$: effectivement, $V_1 = 2U_0, V_2 = \frac{1}{m}U_1, V_3 = \frac{-2}{m}U_2$.
Je laisse le lecteur vérifier le cas particulier du 2.7.1), à savoir que $X\prod_{i=1}^{3} f^{(i)}(X) = -\frac{m^4}{4}$.

$P_{0,m}(X) = m^4((\frac{X}{m})^4 - 3(\frac{X}{m})^2 + 2(\frac{X}{m}) - \frac{1}{4}$ est irréductible (logiciel en posant $Y = \frac{X}{m}$)

cas $m = 1$:

$P_{\mu,1}(X) = X^4 + \mu X^3 - 3(\frac{\mu}{2} + 1)X^2 + (\frac{\mu}{2} + 2)X - \frac{1}{4}$ est irréductible sur $\mathbb{Q}$ si $\mu \in \{-10;-9;-8;\ldots;11;12\} - \{-2\}$ (logiciel)

$P_{-2,1}(X) = (X^2 - \frac{1}{2})(X^2 - 2X + \frac{1}{2})$ est réductible, et ses racines sont $r, f(r), f^{(2)}(r), f^{(3)}(r)$, avec, par exemple, $r = \frac{\sqrt{2}}{2}$, $f(X) = 1 - \frac{1}{2X}$ transformant une racine de l'un des facteurs en une racine de l'autre facteur :
$f(\frac{\sqrt{2}}{2}) = 1 - \frac{\sqrt{2}}{2}, f(1 - \frac{\sqrt{2}}{2}) = -\frac{\sqrt{2}}{2}, f(-\frac{\sqrt{2}}{2}) = 1 + \frac{\sqrt{2}}{2}$ et évidemment
$f(1 + \frac{\sqrt{2}}{2}) = f^{(4)}(\frac{\sqrt{2}}{2}) = \frac{\sqrt{2}}{2}$.
Le corps de décomposition de $P_{-2,1}$ est $\mathbb{Q}(\sqrt{10})$, extension de degré 2 de $\mathbb{Q}$ et donc le groupe de Galois de $P_{-2,1}$ est C_2.
On peut vérifier le 2.4), à savoir que $N(X) = X^4 - 3X^2 + 2X - \frac{1}{4}$ et $D(X) = X(X-1)(X-\frac{1}{2})$ n'ont aucune racine commune.

$P_{\mu,1}(f(X)) = -\frac{1}{X^4}P_{\mu,1}(X)$.

cas $m = 3$:

$P_{2,3}(X) = X^4 + 2X^3 - 36X^2 + 63X - \frac{81}{4} = \frac{1}{4}(2X^2 - 8X + 3)(2X^2 + 12X - 27)$ est réductible, et ses racines sont $r, f(r), f^{(2)}(r), f^{(3)}(r)$, avec, par exemple, $r = -3 + \frac{\sqrt{10}}{2}$, $f(X) = 3 - \frac{9}{2X}$ transformant une racine d'un des facteurs en une racine de l'autre facteur.
Le corps de décomposition de $P_{2,3}$ est $\mathbb{Q}(\sqrt{10})$, extension de degré 2 de $\mathbb{Q}$ et donc le groupe de Galois de $P_{1,3}$ est C_2.
Là aussi, comme pour $P_{-2,1}$, on vérifie que N et D n'ont pas de racine commune.

preuve :

2.1) D'après l'annexe 1, tous les $f^{(i)}$ sont de la forme $\frac{aX+b}{cX+d}$ avec $ad-bc \neq 0$ et $c \neq 0$ (puisqu'il ne s'agit pas de polynôme) ; donc $cX+d$ est un polynôme de degré 1 de $\mathbb{Q}[X]$, et ainsi, r étant algébrique de degré 3, il ne peut en être racine.
Si $r = f^{(i)}(r)$ pour $1 \leq i \leq n-1$, r est racine d'un polynôme$\in \mathbb{Q}[X]$ de degré 2 (puisque $f^{(i)} = \frac{d^\circ \leq 1}{d^\circ = 1}$, $f^{(i)}$ n'étant pas un polynôme), ce qui est contraire au fait que r est supposé algébrique de degré ≥ 3.
Si $f^{(i)}(r) = f^{(j)}(r)$ pour $1 \leq i < j \leq n-1$, en composant des deux côtés par $f^{(n-j)}$ on obtient $r = f^{(n-j+i)}(r)$ avec $1 \leq n-j+i \leq n-1$, ce qui est impossible d'après ce qui précéde.

2.2) Puisque $r \neq f(r)$, on a $f^{(k)}(r) \neq r$ pour $k = 1,2,\ldots,n-1$, sinon on aurait $f(r) = r$ d'après le lemme 3 de l'annexe 1.
Et si $f^{(j)}(r) = f^{(i)}(r)$ pour $1 \leq i < j \leq n-1$, en composant par $f^{(-i)}$, on obtient $f^{(j-i)}(r) = r$ avec $1 \leq j-i < n$, ce qui contredit la ligne précédente.
Donc $r, f(r), f^{(2)}(r), \ldots, f^{(n-1)}(r)$ sont distincts.

2.3)
2.3.1) Soient $i < j$ dans $\{1;2;..;n-1\}$ et supposons que V_i et V_j aient une racine commune : ils sont donc proportionnels.
Puisque $f(X) = \frac{aX+b}{cX+d}$, en considérant la matrice inversible $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, on a d'après les préliminaires de l'annexe 1, $f^{(i)}(X) = \frac{a_iX+b_i}{c_iX+d_i} = \frac{U_i(X)}{V_i(X)}$ avec $\begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} = A^i$; mais toujours d'après l'annexe 1, $A^i = u_iA + v_i$ et $A^j = u_jA + v_j$, donc il existe $\xi \neq 0$ tel que $(u_jc, u_jd+v_j) = \xi(u_ic, u_id+v_i)$, soit $u_jc = \xi u_ic$ et $u_jd + v_j = \xi(u_id+v_i)$.
Comme $bc \neq 0$ (remarque 2 du 1.1) du II de l'annexe 1), $u_j = \xi u_i$ et $v_j = \xi v_i$, soit $A^j = \xi A^i$ et A étant inversible, $A^{j-i} = \xi I$ avec $\xi \neq 0$, donc f est d'ordre $\leq j-i < n$, ce qui est contredit le fait que f est d'ordre n.
Donc V_i et V_j n'ont pas de racine commune.
Pour le cas U_i et U_j, il suffit de reprendre la preuve précédente, en considérant cette fois les premères lignes de A^i et A^j : $(u_ja + v_j, u_jb) = \xi(u_ia+v_i, u_ib)$ et cette fois on utilise le fait que $b \neq 0$ pour arriver à la même contradiction.

2.3.2) De $f^{(n-i)}(f^{(i)}(X)) = X$, on tire $\frac{U_{n-i}(\frac{U_i(X)}{V_i(X)})}{V_{n-i}(\frac{U_i(X)}{V_i(X)})} = X$, soit en posant $U_{n-i}(X) = pX+q$ et $V_{n-i}(X) = rX+s$, $pU_i(X) + qV_i(X) = X(rU_i(X) + sV_i(X))$.
D'où si $V_i(0) = 0$, on a $pU_i(0) = 0$ et comme $U_i(0) \neq 0$ (sinon $f^{(i)}$ est constant ce qui est exclu, $f^{(i)}$ n'étant pas un polynôme) et donc $p = 0$, donc U_{n-i} est constant $\neq 0$ (car $f^{(n-i)}$ ne peut être identiquement nul) et ainsi n'a pas de racine.
Si U_{n-i} n'a pas de racine, c'est une constante, donc $p = 0$ et $qV_i(0) = 0$ et aussi $(q-sX)V_i(X) = rXU_i(X)$. Comme $r \neq 0$ (puisque $f^{(n-i)}$ n'est pas un polynôme), $\frac{U_i(X)}{V_i(X)} = \frac{q-tX}{rX}$, donc $q \neq 0$ (sinon $f^{(i)}$ est constant) et ainsi $V_i(0) = 0$.

2.3.3) Si r est une racine de U_i, alors $V_i(r) \neq 0$ (sinon $f^{(i)}$ est constant), donc $f^{(i)}(r)$ est défini avec $f^{(i)}(r) = 0$.
D'après le 2.3.2) 0 n'est pas racine de V_{n-i}, donc $f^{(n-i)}(0)$ est défini, et $f^{(n-i)}(0) = f^{(n-i)}(f^{(i)}(r)) = f^{(n)}(r) = r$.

2.3.4) $f^{(\frac{n}{2})}$ est évidemment d'ordre 2 car $f^{(\frac{n}{2})} \circ f^{(\frac{n}{2})} = id$ et $f^{(\frac{n}{2})} \neq id$.

Si 0 est racine de $V_{\frac{n}{2}}$, d'après le 2.3.2) $U_{n-\frac{n}{2}} = U_{\frac{n}{2}}$ n'a pas de racine, donc est une constante et $f^{(\frac{n}{2})}(X) = \frac{U_{\frac{n}{2}}}{V_{\frac{n}{2}}} = \frac{\lambda}{X}$, avec $\lambda \neq 0$.

2.3.5) De $f^{(i_0)}(X) = \frac{U_{i_0}}{\xi X}$, on tire $f^{(i_0+j)} = f^{(i_0)} \circ f^{(j)} = \frac{U_{i_0}(\frac{U_j}{V_j})}{\xi \frac{U_j}{V_j}} = \frac{V_j U_{i_0}(\frac{U_j}{V_j})}{\xi U_j}$: le numérateur étant un polynôme de degré ≤ 1, d'après l'exercice 1 de l'annexe 1, $V_{i_0+j} = c_{i_0+j} U_j = c_{i_0+j} U_{i_0+j+n-i_0}$ (où c_{i_0+j} est une constante) car $U_{n+j} = U_j$ puisque $f^{(n+j)} = f^{(j)}$.
Ainsi $V_i = c_i U_{i+n-i_0} = c_i U_{i-i_0}$ en prenant l'indice modulo n dans $\{0;1;\ldots;n-1\}$ et c_i étant une constante.
Illustration pour l'exemple 2 où $n = 4, i_0 = 1$:
$f(X) = \frac{m(2X-m)}{2X}$, $f^{(2)}(X) = \frac{m(X-m)}{2X-m}$, $f^{(3)}(X) = \frac{m^2}{2(m-X)}$ et $V_1 = \frac{1}{2}U_0, V_2 = \frac{1}{m}U_1$, $V_3 = \frac{-2}{m}U_2$: on vérifie que V_2 a pour racine $f^{(n-i+i_0)}(0) = f^{(4-2+1)}(0) = f^{(3)}(0) = \frac{m}{2}$.
Voir une autre illustration à l'exemple 6 de l'annexe 2.

2.4) Pour tout $i \in \{1;2;\ldots;k-1\}$, $f^{(i)} = \frac{U_i}{V_i}$ avec U_i polynôme de degré ≤ 1 et V_i polynôme de degré 1 (car $f^{(i)}$ n'est pas un polynôme).

Donc $X + f(X) + f^{(2)}(X) + \ldots + f^{(n-1)}(X) = X + \frac{\sum_{j=1}^{n-1} U_j(X) \prod_{\substack{i \in \{1;2;\ldots;n-1\} \\ i \neq j}} V_i(X)}{\prod_{i=1}^{n-1} V_i(X)} = \frac{N_b(X)}{D_b(X)}$.

avec $D_b = \prod_{i=1}^{n-1} V_i$ de degré $n-1$ et $N_b(X) = XD_b(X) + \sum_{j=1}^{n-1} U_j(X) \prod_{i \neq j} V_i(X)$ de degré n, puisque XD_b est de degré n et $U_j(X) \prod_{i \neq j} V_i(X)$ est de degré $\leq 1 + n - 2 = n - 1$.

D_b et XD_b ayant évidemment le même coefficient de tête, D_b et N_b ont aussi le même coefficient de tête λ et donc on peut les rendre simultanément unitaires en les divisant par λ et ainsi $X + f(X) + f^{(2)}(X) + \ldots + f^{(n-1)}(X) = \frac{N(X)}{D(X)}$ avec $N = \frac{1}{\lambda}N_b$ et $D = \frac{1}{\lambda}D_b$ unitaires.

Montrons que N et D n'ont pas de racine commune.
Supposons que θ soit une racine commune à N et D, donc à N_b et à D_b.
θ est racine d'un V_i : pour simplifier un peu les écritures, supposons que θ est la racine de V_1.

Les racines des V_i étant distinctes, $\prod_{i\neq 1} V_i(\theta) \neq 0$ et si $j \neq 1$, $\prod_{i\neq j} V_i(\theta) = 0$, donc
$N_b(\theta) = \theta D_b(\theta) + U_1(\theta)\prod_{i\neq 1} V_i(\theta)$ et $U_1(\theta)\prod_{i\neq 1} V_i(\theta) = 0$.
Or $U_1(\theta) \neq \theta$, sinon, U_1 et V_1 sont proportionnels et f est un polynôme (constant), ce qui est exclu, d'où $\prod_{i\neq 1} V_i(\theta) = 0$, ce qui est en contradiction avec $\prod_{i\neq 1} V_i(\theta) \neq 0$.
Donc N et D n'ont pas de racine commune.

2.5) Cherchons un polynôme $P \in \mathbb{Q}[X]$, de degré $n \geq 3$, irréductible, unitaire et dont les racines sont $r, f(r), f^{(2)}(r), \ldots, f^{(n-1)}(r)$; évidemment P est le polynôme minimal de toutes ses racines, lesqelles sont donc algébriques sur $\mathbb{Q}$ de degré n ; à ce titre $D(f^{(i)}(r))$ est non nul pour $0 \leq i \leq n-1$, car $D \in \mathbb{Q}[X]$ et est de degré $n-1$.
On va exploiter le fait que la somme des racines de P est un rationnel (relations entre racines et coefficients), donc $\frac{N_b(r)}{D_b(r)}$ est un rationnel, donc $\frac{N(r)}{D(r)}$ est aussi un rationnel, disons $-\mu$ et ainsi r est racine de $N(X) + \mu D(X)$.
Le polynôme minimal de r étant P, P divise $N + \mu D$ et comme ces deux polynômes sont unitaires et de même degré, ils sont égaux.
Donc nécessairement le polynôme cherché P est $P_\mu = N + \mu D$ pour $\mu \in \mathbb{Q}$.
Réciproquement, pour tout $\mu \in \mathbb{Q}$, $P_\mu \in \mathbb{Q}[X]$, est unitaire et de degré n.
Mais est-il irréductible sur $\mathbb{Q}$? Ce n'est pas obligé, voir exemples 1 et 2 ci-dessus.
Mais, même si P_μ est réductible, on a $\frac{N(f(X))}{N(X)} = \frac{D(f(X))}{D(X)}$ et
$P_\mu(f(X)) = \frac{D(f(X))}{D(X)} P_\mu(X) = \frac{N(f(X))}{N(X)} P_\mu(X)$.
En effet dans la relation $X + f(X) + f^{(2)}(X) + \ldots + f^{(n-1)}(X) = \frac{N(X)}{D(X)}$, en remplacant X par $f(X)$, on obtient (puisque $f^{(n)} = id$) $\frac{N(f(X))}{D(f(X))} = \frac{N(X)}{D(X)} \Leftrightarrow \frac{N(f(X))}{N(X)} = \frac{D(f(X))}{D(X)}$.
Et de $\frac{P_\mu}{D} = \frac{N}{D} + \mu$, on déduit que $\frac{P_\mu(f(X))}{D(f(X))} = \frac{P_\mu(X)}{D(X)}$, soit $P_\mu(f(X)) = \frac{D(f(X))}{D(X)} P_\mu(X)$
(pour l'exemple 2, dans le cas $m = 1$, $\frac{D(f(X))}{D(X)} = -\frac{1}{X^4}$).

On va montrer maintenant que P_μ a n racines réelles distinctes de la forme $r, f(r), f^{(2)}(r), \ldots, f^{(n-1)}(r)$ et on va les localiser.
Pour cela on va revenir à $X + f(X) + f^{(2)}(X) + \ldots + f^{(n-1)}(X) = \frac{N(X)}{D(X)}$.
$f^{(i)}(X) = \frac{U_i(X)}{V_i(X)}$, U_i et V_i "correspondants" aux lignes de A^i (voir preuve du 2.3.1)) ;
comme $A^i = u_i A + v_i I = \begin{pmatrix} u_i a + v_i & u_i b \\ u_i c & u_i d + v_i \end{pmatrix}$, $f^{(i)}(X) = \frac{(u_i a + v_i)X + u_i b}{u_i c X + u_i d + v_i}$.
Rappelons, cf l'annexe 1, que pour $i \in \{1; 2; \ldots; n-1\}$, $u_i \neq 0$ (sinon f est d'ordre $\leq i < n$) et que $bc \neq 0$ (voir remarques 1 et 2 du 1.1) du II de l'annexe 1).
Et d'après l'identité $\frac{pX+q}{rX+s} = \frac{p}{r} - \frac{ps-qr}{r(rX+s)}$, $f^{(i)}(X) = \frac{u_i a + v_i}{u_i c} - \frac{1}{u_i c} \times \frac{\xi_i}{u_i c X + u_i d + v_i}$ où ξ_i n'est autre que le déterminant de A^i, soit $(ad - bc)^i = \delta^i$.
Ainsi $f^{(i)}(X) = \frac{u_i a + v_i}{u_i c} - \frac{\delta^i}{(u_i c)^2 (X - \tau_i)}$ avec $\tau_i = -\frac{u_i d + v_i}{u_i c}$ la racine de V_i. On notera

que puisque $\delta > 0$ (remarque 3 du 1.1) du II de l'annexe 1), pour tout i, $\frac{-\delta^i}{(u_i c)^2} < 0$.

On va pouvoir conclure à l'aide du résultat d'analyse suivant.

Soit g une fonction de la variable réelle x à valeurs dans $\mathbb{R}$ définie par $g(x) = x + h_0 - \sum_{j=1}^{n-1} \frac{h_j}{x-\theta_j}$, les h_j étant des constantes réelles positives et les θ_j tels que $\theta_j < \theta_{j+1}$.

g est évidemment continue sur chacun des n intervalles $]-\infty;\theta_1[,]\theta_1;\theta_2[,]\theta_2;\theta_3[,\ldots]\theta_{n-2};\theta_{n-1}[,]\theta_{n-1};+\infty[$ et, en considérant les limites aux bornes, on voit que l'image par g de chacun de ces intervalles est $\mathbb{R}$.

Et par ailleurs g est strictement croissante sur chacun de ces intervalles.

Donc, pour tout s donné réel, l'équation $g(x) = s$ a n solutions, chacun des intervalles ci-dessus contenant une et une seule de ces solutions.

On applique ce résultat à $\frac{N(x)}{D(x)} = x + \sum_{i=1}^{n-1} \frac{u_i a + v_i}{u_i c} - \sum_{j=1}^{n-1} \frac{\frac{\delta^{i_j}}{(u_{i_j} c)^2}}{x-\theta_j}$ avec $\theta_j = \tau_{i_j}$ et $\tau_{i_1} < \tau_{i_2} < \ldots < \tau_{i_{n-1}}$ (cad les θ_j sont les zéros τ_i des V_i ordonnés de façon croissante) :

$\forall \mu \in R$, l'équation $\frac{N(x)}{D(x)} = -\mu \Leftrightarrow P_\mu(x) = 0$ a exactement n solutions réelles, chacune étant dans un des n intervalles $]-\infty;\theta_1[,]\theta_1;\theta_2[,]\theta_2;\theta_3[,\ldots]\theta_{n-2};\theta_{n-1}[,]\theta_{n-1};+\infty[$.

Evidemment $\frac{N(x)}{D(x)} = -\mu \Rightarrow P_\mu(x) = 0$, mais la réciproque est vraie car $P_\mu(x) = 0 \Rightarrow D(x) \neq 0$ (sinon N et D ont une racine commune ce qui,d'après le 4), est exclu), donc $P_\mu(x) = 0 \Rightarrow \frac{N(x)}{D(x)} = -\mu$.

Ainsi P_μ a n racines réelles distinctes, chacune étant dans un des n intervalles $]-\infty;\theta_1[,]\theta_1;\theta_2[,]\theta_2;\theta_3[,\ldots]\theta_{n-2};\theta_{n-1}[,]\theta_{n-1};+\infty[$.

Montrons maintenant que les n racines réelles distinctes de P_μ sont de la forme $r, f(r), f^{(2)}(r), \ldots, f^{(n-1)}(r)$:

r étant une racine quelconque de P_μ, $D(r) \neq 0$ (voir plus haut), donc r n'est pas racine de V_1 et $f(r)$ est défini et cf plus haut $P_\mu(f(r)) = \frac{D(f(r))}{D(r)} P_\mu(r) = 0$ et $f(r)$ est racine de P_μ.

De même, $f(r)$ étant une racine quelconque de P_μ, $D(f(r)) \neq 0$, donc $f(r)$ n'est pas racine de V_1 et $f(f(r)) = f^{(2)}(r)$ est défini et $P_\mu(f^{(2)}(r)) = \frac{D(f^{(2)}(r))}{D(f(r))} P_\mu(f(r)) = 0$ et $f^{(2)}(r)$ est racine de P_μ.

Etc.

Comme $r \neq f(r)$ (sinon r n'est pas réel), le 2.2) nous donne que $r, f(r), f^{(2)}(r), \ldots, f^{(n-1)}(r)$ sont n nombres distincts donc sont les n racines de P_μ.

Dans le cas où P_μ est irréductible sur $\mathbb{Q}$, le résultat rappelé en introduction nous donne que le groupe de Galois de P_n est C_n.

2.6) $N = P_0$ a n racines distinctes $r, f(r), f^{(2)}(r), \ldots, f^{(n-1)}(r)$, donc $D(r) \neq 0$ (sinon D et N ont une racine commune), et puisque $X + f(X) + f^{(2)}(X) + \ldots + f^{(n-1)}(X) = \frac{N(X)}{D(X)}$, on obtient $r + f(r) + f^{(2)}(r) + \ldots + f^{(n-1)}(r) = \frac{N(r)}{D(r)} = 0$,donc la somme des n racines de N est nulle et ainsi le coefficient de X^{n-1} dans N est nul.

D étant unitaire de degré $n-1$, le coefficient de X^{n-1} dans P_μ est toujours μ.

2.7.1) $s_k(X) = \sum_{\substack{i_1<i_2<\ldots<i_k \\ i_j\in\{0;1;..;n-1\}}} \frac{U_{i_1}U_{i_2}\ldots U_{i_k}}{V_{i_1}V_{i_2}\ldots V_{i_k}}$ puisque $f^{(i)}(X) = \frac{U_i(X)}{V_i(X)}$ avec $U_0(X) = X$,

$V_0(X) = 1$.

$D_b(X)s_k(X) = \sum_{\substack{i_1<i_2<\ldots<i_k \\ i_j\in\{0;1;..;n-1\}}} U_{i_1}U_{i_2}\ldots U_{i_k} \prod_{j\in\{0;1;\ldots;n-1\}-\{i_1;i_2;\ldots;i_k\}} V_j$ avec $D_b = \prod_{i=1}^{n-1} V_i = \prod_{i=0}^{n-1} V_i$.

$U_{i_1}U_{i_2}\ldots U_{i_k}$ est de degré $\le k$, chaque U_{i_j} étant de degré ≤ 1 ; par contre pour le produit des V_j, il y a deux cas à envisager : soit il y a un j qui prend la valeur 0 et le produit est de degré $n-k-1$ (car V_0 est le seul V_j à ne pas être de degré 1), sinon le produit des V_j est de degré $n-k$ et ainsi $D_b s_k$ est un polynôme de degré $\le n$.
Ce degré peut être n : c'est le cas de $D_b s_1$ puisque $Ds_1 = N$ et D_b est D à une constante multiplicative près ; on peut le retrouver à partir de la formule ci-dessus qui devient $D_b(X)s_1(X) = \sum_{\substack{i_1 \\ i_j\in\{0;1;..;n-1\}}} U_{i_1} \prod_{j\in\{0;1;\ldots;n-1\}-\{i_1\}} V_j$ et on remarque que si $i_1 = 0$,

$U_{i_1} \prod_{j\in\{0;1;\ldots;n-1\}-\{i_1\}} V_j = X \prod_{j\in\{1;\ldots;n-1\}} V_j$ est de degré n, et si $i_1 \neq 0$, $U_{i_1} \prod_{j\in\{0;1;\ldots;n-1\}-\{i_1\}} V_j$ est de degré $\le 1+n-2$, puisque dans le produit des V_j (il y en a $n-1$), l'un est $V_0 = 1$ qui est degré 0.
Cherchons les racines de ce polynôme $D_b s_k$.
Les n racines de P_{β_k} étant d'après le 5) de la forme $r, f(r), f^{(2)}(r), \ldots, f^{(n-1)}(r)$ distinctes, et le coefficient de X^{n-k} dans P_{β_k} étant (par définition de β_k) nul, la somme des produits k à k de ces racines est nulle, cad $s_k(r) = 0$.
Mais $s_k(f^{(i)}(X)) = s_k(X)$ donc $s_k(f^{(i)}(r)) = s_k(r) = 0$ pour $j = 0, 1, \ldots, n-1$.
On en déduit que le polynôme $D_b s_k$ a pour racines distinctes $r, f(r), f^{(2)}(r), \ldots, f^{(n-1)}(r)$, et comme il est de degré $\le n$, c'est qu'il est de degré n, et donc c'est, à une constante multiplicative près, P_{β_k}.

Mais D_b c'est D à une constante multiplicative près, donc $s_k(X) = \alpha_k \frac{P_{\beta_k}(X)}{D(X)}$ où α_k est une constante ; égalité qui s'écrit aussi $s_k(X) = \alpha_k \frac{N(X) + \beta_k D(X)}{D(X)}$ soit

$s_k(X) = \alpha_k(s_1(X) + \beta_k)$.

Passons maintenant à la détermination de la constante α_k.
Pour $k \in \{1; 2; \ldots; n-1\}$, on pose $t_k = \sum_{1\le i_1<i_2<\ldots<i_k\le n-1} f^{(i_1)}f^{(i_2)}\ldots f^{(i_k)}$ et $t_0(X) = 1$.

De façon immédiate on a
$\forall k \in \{1; 2; \ldots; n-1\}$ $s_k(X) = Xt_{k-1}(X) + t_k(X)$; par exemple $t_1 = \sum_{1\le i_1\le n-1} f^{(i_1)}$ et $t_0(X) = 1$

donnent $s_1(X) = Xt_0(X) + t_1(X)$

$\forall k \in \{1; 2; \ldots; n-1\}$ $t_k(X) = s_k(X) - Xs_{k-1}(X) + X^2 s_{k-2}(X) + \ldots + (-1)^k X^k = \sum_{j=0}^{k} (-1)^j X^j s_{k-j}(X)$

(récurrence immédiate, à partir de la relation précédente)
On vient de voir que Ds_k est un polynôme de degré n égal à $\alpha_k P_{\beta_k}$: donc α_k est le coefficient de tête de Ds_k.
Or $D(X)s_k(X) = D(X)Xt_{k-1}(X) + D(X)t_k(X)$ et comme

$D(X)t_k(X) = \sum_{1\le i_1<i_2<\ldots<i_k\le n-1} U_{i_1}(X)U_{i_2}(X)\ldots U_{i_k}(X) \prod_{j\in\{0;1;\ldots;n-1\}-\{i_1;i_2;\ldots;i_k\}} V_j$ est une somme de termes de degrés tous $\le k+n-1-k = n-1$, α_k est le coefficient de tête de $D(X)Xt_{k-1}(X)$, cad α_k est le coefficient de X^n dans $D(X)Xt_{k-1}(X)$.

Notons maintenant $N(X) = X^n + p_2X^{n-2} + p_3X^{n-3}\ldots$ ($p_0 = 1$ et $p_1 = 0$ d'après le 2.6)) et $D(X) = X^{n-1} + q_2X^{n-2} + \ldots$ ($q_1 = 1$).

On cherche à montrer que pour tout $k \in \{1;2;\ldots;n\}$, si $q_k \neq 0$, alors $\alpha_k = (-1)^{k+1}q_k$: pour cela on va procéder par récurrence, l'hypothèse de récurrence étant

pour $k \in \{1;2;\ldots;n-1\}$, on suppose que pour tout j tel que $1 \le j \le k$, si $q_j \neq 0$ alors $\alpha_j = (-1)^{j+1}q_j$ (cela est bien vrai si $k = 1$ car d'après la note 1 de l'énoncé $\alpha_1 = 1$ et donc $\alpha_1 = (-1)^{1+1}q_1$).

Il faut déduire de cette hypothèse de récurrence que si $q_{k+1} \neq 0$ alors $\alpha_{k+1} = (-1)^{k+2}q_{k+1}$.

q_{k+1} étant non nul, cf ci-dessus on sait que $s_{k+1}(X) = \alpha_{k+1}\frac{P_{\beta_{k+1}}(X)}{D(X)}$ avec α_{k+1} coefficient de X^n dans $D(X)Xt_k(X)$.

D'où α_{k+1} = coefficient de X^n dans $\sum_{j=0}^{k}(-1)^j D(X)X^{j+1}s_{k-j}(X)$ (avec $s_0(X) = 1$).

$\alpha_{k+1} = \sum_{j=0}^{k}\theta_j$ avec θ_j le coefficient de X^n dans $(-1)^j D(X)X^{j+1}s_{k-j}(X)$.

si $j = k$, $\theta_k = (-1)^k q_{k+1}$ puisque $s_0(X) = 1$ et par définition, q_{k+1} est le coefficient de $X^{n-(k+1)}$ dans D

si $j \neq k$ il y a deux cas à envisager selon que q_{k-j} (coeffcient de $X^{n-(k-j)}$ dans D) est nul ou pas, cela pour évaluer s_{k-j} :

si $q_{k-j} = 0$ (impossible si $k-j = 1$ car $q_1 = 1$)

alors, d'après le 2.7.2) (sera démontré plus loin),$s_{k-j}(X) = (-1)^{k-j}p_{k-j}$ et

$\theta_j = (-1)^j(-1)^{k-j}p_{k-j}\times$ par le coefficient de $X^{n-(j+1)}$ de D

$\theta_j = (-1)^k p_{k-j}q_{j+1}$

$\theta_j = (-1)^{k+1}(q_{k-j}p_{j+1} - p_{k-j}q_{j+1})$ car ici $q_{k-j} = 0$

si $q_{k-j} \neq 0$ (obligé si $k-j = 1$ car $q_1 = 1$)

alors d'après ci-dessus $s_{k-j} = \alpha_{k-j}\frac{P_{\beta_{k-j}}}{D}$ et l'hypothèse de récurrence donne $\alpha_{k-j} = (-1)^{k-j+1}q_{k-j}$

$(-1)^j D(X)X^{j+1}s_{k-j}(X) = (-1)^j\alpha_{k-j}X^{j+1}(N(X) + \beta_{k-j}D(X)$

$\theta_j = (-1)^j(-1)^{k-j+1}q_{k-j}(p_{j+1} + \beta_{k-j}q_{j+1})$

$\theta_j = (-1)^{k+1}(q_{k-j}p_{j+1} - p_{k-j}q_{j+1})$ car par définition de β_{k-j} on a $p_{k-j} + \beta_{k-j}q_{k-j} = 0$.

Donc dans les deux cas où $j \neq k$, les θ_j ont la même valeur $(-1)^{k+1}(q_{k-j}p_{j+1} - p_{k-j}q_{j+1})$.

On remarque aussi que si $j \in \{0;1;\ldots;k-1\}$ alors θ_j et θ_{k-1-j} sont opposés, donc, compte-tenu que $\alpha_{k+1} = \sum_{j=0}^{k-1}\theta_j + \theta_k$

si k est pair, $\theta_0 + \theta_{k-1} = 0, \theta_1 + \theta_{k-2} = 0, \ldots, \theta_{\frac{k}{2}-1} + \theta_{\frac{k}{2}} = 0$ et ainsi $\alpha_{k+1} = 0 + (-1)^k q_{k+1}$

si k est impair, dans le $\sum_{j=0}^{k-1}\theta_j$ il ne va rester que le terme central

$\theta_{\frac{k-1}{2}} = (-1)^{\frac{k+1}{2}}(q_{\frac{k+1}{2}}p_{\frac{k+1}{2}} - p_{\frac{k+1}{2}}q_{\frac{k+1}{2}}) = 0$

et on a encore $\alpha_{k+1} = 0 + (-1)^k q_{k+1}$.

Donc l'hypothèse de récurrence ci-dessus implique bien que SI $q_{k+} \neq 0$ alors $\alpha_{k+1} = (-1)^{k+2} q_{k+1}$, ce qui prouve le résultat annoncé sur ce coefficient α_k.

Le cas particulier $k = n$ (rappel $D(0) \neq 0$) donne $s_n(X) = \alpha_n \dfrac{P_{\beta_n}(X)}{D(X)}$ et comme $\lambda D = \prod_{i=1}^{n-1} V_i$ (λ constante) et $s_n(X) = X \prod_{i=1}^{n-1} f^{(i)}(X) = X \prod_{i=1}^{n-1} \dfrac{U_i(X)}{V_i(X)}$, on obtient $P_{\beta_n}(X) = \dfrac{1}{\lambda \alpha_n} X \prod_{i=1}^{n-1} U_i(X)$; et le degré de P_{β_n} étant n et $d^\circ U_i \leq 1$, c'est que pour tout $i \in \{1;2;\ldots;n-1\}$ $d^\circ U_i = 1$.

P_{β_n} étant unitaire, $\lambda \alpha_n$ est le coefficient de tête de $\prod_{i=1}^{n-1} U_i$.

Mais, puisque $\lambda =$ le coefficient de tête de $\prod_{i=1}^{n-1} V_i = \lambda D$ et que $\alpha_n = (-1)^{n+1} D(0)$ (voir le 2.7.1)), on a $D(0) = (-1)^{n+1} \dfrac{\text{coefficient de tête de } \prod_{i=1}^{n-1} U_i}{\text{coefficient de tête de } \prod_{i=1}^{n-1} V_i}$.

2.7.2) D'après le 2.5) les racines de P_μ sont $r, f(r), f^{(2)}(r), \ldots, f^{(n-1)}(r)$ et donc $s_k(r) = (-1)^k c$, puisque le coefficient de X^{n-k} dans P_μ est c.
Donc $s_k(r) = s_k(f(r)) = \ldots = s_k(f^{(n-1)}(r)) = (-1)^k c$.
Notons W_k le polynôme $D_b s_k$ qui est de degré $\leq n$ (voir preuve du 2.7.1)) : on a alors $D_b(f^{(i)}(r))(-1)^k c - W_k(f^{(i)}(r)) = 0$ pour $i = 0, 1, \ldots n-1$ et ainsi le polynôme $(-1)^k c D_b - W_k$ qui est de degré $\leq n$, a n racines distinctes $r, f(r), f^{(2)}(r), \ldots, f^{(n-1)}(r)$.
Considérons maintenant la racine θ de V_1 : θ est donc racine de D_b, donc de $(-1)^k c D_b - W_k$.
$\theta \notin \{r; f(r); f^{(2)}(r); \ldots; f^{(n-1)}(r)\}$ car si $\theta = f^{(i)}(r)$ pour $i \in \{0;1;\ldots;n-1\}$, $f^{(i)}(r)$ qui est une racine de P_μ est aussi racine de V_1, donc de D, donc de $N = P_\mu - D$, ce qui est impossible d'après le 4).
Donc le polynôme $(-1)^k c D_b - W_k$ qui est de degré $\leq n$, a $n+1$ racines distinctes $\theta, r, f(r), f^{(2)}(r), \ldots, f^{(n-1)}(r)$, c'est donc le polynôme nul et $D_b s_k = (-1)^k c D_b$, et comme D_b n'est pas le polynôme nul, c'est que $s_k = (-1)^k c$, cad $s_k(X) = (-1)^k c$.

8) Supposons que pour $i \in \{1;2;\ldots;n-1\}$, $f^{(i)}(X) = \dfrac{\lambda}{X}$ avec $\lambda \neq 0$.
$f^{(i)}(f^{(i)}(X)) = X$, soit $f^{(2i)} = id$ et comme f est d'ordre n, c'est que $2i \geq n$.
Mais $X = f^{(i)}(f^{(n-i)}(X)) = \dfrac{\lambda}{f^{(n-i)}(X)}$ et $f^{(n-i)}(X) = \dfrac{\lambda}{X}$, donc $2(n-i) \geq n$, et on arrive à $2i \geq n \geq 2i$, soit nécessairement $n = 2i$.
Dans le cas n pair et où on a $f^{(\frac{n}{2})}(X) = \dfrac{\lambda}{X}$ (la cns pourqu'il en soit ainsi est $a = b$: voir 1.2) du II de l'annexe 1), alors
$f^{(\frac{n}{2}+1)}(X) = \dfrac{\lambda}{f(X)}, f^{(\frac{n}{2}+2)}(X) = \dfrac{\lambda}{f^{(2)}(X)}, \ldots, f^{(\frac{n}{2}+\frac{n}{2}-1)}(X) = \dfrac{\lambda}{f^{(\frac{n}{2}-1)}(X)}$ et donc, de part la définition même de $s_n(X)$, on a $s_n(X) = \lambda^{\frac{n}{2}}$; et d'après le 2.7.2) $s_n(X) = (-1)^n c = c$, où c est le terme constant de P_μ, soit $P_\mu(0) = \lambda^{\frac{n}{2}}$ qui est non nul, puisque $\lambda \neq 0$ (voir

énoncé). En outre puisque $V_{\frac{n}{2}}(0) = 0$, $D(0) = 0$ et $P_\mu(0) = N(0)$.

□

Annexe 1

Détermination des $f(X) = \frac{aX+b}{cX+d} \in \mathbb{R}(X)$ avec $ad-bc \neq 0$ d'ordre $2,3,4,5,6,7,8$ et détermination des $n \geq 2$ pour lesquels il existe $f(X) = \frac{aX+b}{cX+d} \in \mathbb{Q}(X)$ avec $ad-bc \neq 0$ d'ordre n.

I) Préliminaires.

Ici on ne considerera que l'ensemble E des fonctions rationnelles de la forme $f(X) = \frac{aX+b}{cX+d}$ avec a,b,c,d dans $\mathbb{R}$ et avec toujours $ad-bc \neq 0,$ ce qui implique que f est bien définie (c et d ne sont pas tous les deux nuls) et est non constante (sinon $\frac{aX+b}{cX+d} = k$ et $a = kc, b = kd$ et $ad-bc = 0$).

Réciproquement, si c et d ne sont pas tous les deux nuls et si f n'est pas constante, alors $ad-bc \neq 0$:

sinon $ad-bc = 0,$ et

soit $cd \neq 0$ et $\frac{a}{c} = \frac{b}{d} = k$ et $f(X) = k$

soit $c = 0, d \neq 0$ et alors $a = 0$ et $f(X) = \frac{b}{d}$

soit $c \neq 0, d = 0$ alors $b = 0$ et $f(X) = \frac{a}{c}$.

Voici quelques remarques qui serviront beaucoup.

Soit $f \in E$ avec $f(X) = \frac{aX+b}{cX+d}$:

alors $f(X) = X$ (cad $f = id$) $\Leftrightarrow b = c = 0$ et $a = d \neq 0 \Leftrightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \lambda I$ avec $\lambda \in \mathbb{R}^*$

Soit f et $g \in E$ avec $f(X) = \frac{aX+b}{cX+d}, g(x) = \frac{a'X+b'}{c'X+d'}$:

alors $g \circ f(X) = \frac{a''X+b''}{c''X+d''}$ avec $\begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$:

cette égalité matricielle implique (on passe au déterminant)

$(a''d''-b''c'') = (a'd' - b'c')(ad-bc) \neq 0$ et donc $g \circ f \in E$.

Tout $f \in E$ admet dans E une fonction réciproque définie par $f^{-1}(X) = \frac{dX-b}{-cX+a}$:

on a $f \circ f^{-1} = f^{-1} \circ f = id$ et $\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = (ad-bc)\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}$

$(E, \circ)$ est donc un groupe d'élément neutre id.

$f \in E$ est d'ordre $n \geq 1$ signifie que n est le plus petit entier ≥ 1 tel que $f^{(n)} = id$

donc $f \in E$ avec $f(X) = \frac{aX+b}{cX+d}$ est d'ordre $n \geq 1 \Leftrightarrow n$ est le plus petit entier ≥ 1 tel que $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^n = \lambda I$ avec $\lambda \in \mathbb{R}^*$.

On notera que la dernière relation matricielle implique $(ad-bc)^n = \lambda^2$.

Exercices préliminaires :

Exercice 1) Soient $f(X)=\frac{aX+b}{cX+d}$ et $g(X)=\frac{a'X+b'}{c'X+d'}$ deux éléments de E :
montrer que $f=g \Leftrightarrow$ il existe $\rho \in R^*$ tel que $(a',b',c',d')=\rho(a,b,c,d)$.

Exercice 2) On pose $f_1(X)=-\frac{1}{X}, f_2(X)=\frac{1-X}{1+X}, f_3(X)=\frac{X+1}{X-1}$
a) Déterminer l'ordre de chacune de ces fonctions rationnelles.
b) Montrer que $G_1=\{id;f_1;f_2;f_3\}$ est un sous-groupe commutatif de E.

Exercice 3) On pose
$f_1(X)=\frac{1}{X}, f_2(X)=1-X, f_3(X)=\frac{X}{X-1}, f_4(X)=\frac{1}{1-X}, f_5(X)=\frac{X-1}{X}$.
a) Déterminer l'ordre de chacune de ces fonctions rationnelles.
b) Montrer que $G_2=\{id;f_1;f_2;f_3;f_4;f_5\}$ est un sous-groupe non commutatif de E.

Remarque sur les exercices 2 et 3 : les sous-groupes finis de E sont connus : ce sont C_n, D_n pour tout $n \geq 1$ et A_4, S_4, S_5.

G_1 est le groupe de Klein qui peut être aussi vu comme le seul groupe diédral commutatif D_2.

G_2 est D_3 et ce groupe diédral est en relation avec la notion de bi-rapport .

En effet le bi-rapport (ou cross-ratio) de quatre points distincts A,B,C,D alignés du plan et pris dans cet ordre, noté (A,B,C,D) est

$\omega=\frac{\overline{AC}}{\overline{AD}} \div \frac{\overline{BC}}{\overline{BD}}$, et lorsqu'on permute ces quatre points (24 possibilités),

on n'obtient que les 6 bi-rapports suivants $\varpi, \frac{1}{\varpi}, 1-\varpi, \frac{1}{1-\varpi}, \frac{\varpi-1}{\varpi}, \frac{\varpi}{\varpi-1}$,

chaque bi-rapport étant obtenu par quatre permutations.

Par exemple, $(C,D,A,B)=\varpi$ et $(B,A,C,D)=(A,B,D,C)=\frac{1}{\varpi}$.

II) Détermination des $f \in E$ et d'ordre n avec $n \geq 2$.

Commencons par trois lemmes :

Lemme 1

A étant une matrice carrée quelconque à éléments réels,
si pour $p \geq 1$ $A^p=\lambda I$ avec $\lambda \in \mathbb{R}^*$, alors le plus entier $n \geq 1$ tel que $A^n=\mu I$ avec $\mu \in \mathbb{R}$ divise p.
Note : $\lambda \neq 0 \Rightarrow \det(A) \neq 0 \Rightarrow \mu \neq 0$.

Application à $f(X)=\frac{aX+b}{cX+d}$ avec $ad-bc \neq 0$: en prenant prendre $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, on voit tout de suite que si f est d'ordre $n \geq 1$ et si $f^{(p)}=id$, alors n divise p.
Ceci est bien entendu un résultat classique de la théorie des groupes.
preuve :
on considère la division euclidienne de p par n, $p=qn+r$ avec $0 \leq r < n$, ce qui donne $A^p=(A^n)^q A^r$ et $A^r=\frac{\lambda}{\mu^q} I$ avec $\frac{\lambda}{\mu^q} \neq 0$.
Si $r \neq 0$ on a $1 \leq r < n$ et on est en contradiction avec la définition de n : donc $r=0$ et n divise p.

Lemme 2

$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ étant une matrice quelconque 2×2 à éléments réels, $ad - bc$ pas forcément nul, on pose $s = a + d$ et $\delta = ad - bc$ (c'est le déterminant de A).

I désignera la matrice unité 2×2.

Les résultats ci-dessous sont alors faciles à vérifier :

$A^2 = sA - \delta I$

(c'est Caley -Hamliton dans le cas de la dimension 2 :l'égalité se vérifie sans difficulté).

On en tire facilement

$\forall n \geq 0,\ A^n = u_n A + v_n I$ avec $u_0 = 0, v_0 = 1$ $(A^0 = I)$ $u_1 = 1,\ v_1 = 0$ $(A^1 = A), u_2 = s, v_2 = -\delta$

et, $\forall n \geq 0,\ u_{n+1} = su_n + v_n$, $v_{n+1} = -\delta u_n$.

Par exemples

$A^3 = (s^2 - \delta)A - \delta sI$

$A^4 = (s^3 - 2\delta s)A - \delta(s^2 - \delta)I$

$A^5 = (s^4 - 3\delta s^2 + \delta^2)A - \delta(s^3 - 2\delta s)I$

$A^6 = (s^5 - 4\delta s^3 + 3s\delta^2)A - \delta(s^4 - 3\delta s^2 + \delta^2)I$

$A^7 = (s^6 - 5\delta s^4 + 6s^2\delta^2 - \delta^3)A - \delta(s^5 - 4\delta s^3 + +3s\delta^2)I$

On déduit de ces deux formules reliant u_n et v_n que

$\forall n \geq 0,\ u_{n+2} = su_{n+1} - \delta u_n$ et $v_{n+2} = sv_{n+1} - \delta v_n$

si $\delta = 0$: $\forall n \geq 0,\ u_{n+2} = su_{n+1}$ et comme $u_1 = 1$ on a, $\forall n \geq 2$, $u_n = s^{n-1}$.

si $\delta \neq 0$, explicitons u_n en utilisant la formule de Binet, l'équation caractéristique étant $x^2 - sx + \delta = 0$ dont le discriminant est $s^2 - 4\delta = (a - d)^2 + 4bc$.

si $\delta \neq 0$ et $4\delta = s^2$ l'équation caractéristique a une racine double $\frac{s}{2} \neq 0$:

donc pour $n \geq 0,\ u_n = c_1(\frac{s}{2})^n + c_2 n(\frac{s}{2})^n$ et comme $u_0 = 0, u_1 = 1,$ on a , $\forall n \geq 0$,

$u_n = n(\frac{s}{2})^{n-1}$.

Exemple.

On prend $A = aI$ avec $a \neq 0$: de $A^n = u_n A + v_n I$ on tire $a^n = au_n + v_n$.

Retrouvons le à partir de la formule ci-dessus : on a ici $s = 2a, \delta = a^2, 4\delta = s^2 \neq 0$ et ainsi $u_n = na^{n-1}$ et $v_n = -\delta u_{n-1} = -(n-1)a^n$, d'où $au_n + v_n = a^n$.

si $\delta \neq 0$ et $s^2 - 4\delta \neq 0$ l'équation caractéristique a deux racines distinctes et non nulles $r_1 = \frac{s + w}{2}$ et $r_2 = \frac{s - w}{2}$ où w est une racine 2ième de $s^2 - 4\delta$ (w est réel si et seulement si $s^2 - 4\delta > 0$),

donc pour $n \geq 0,\ u_n = c_1 r_1^n + c_2 r_2^n$ et comme $u_0 = 0, u_1 = 1,$ on a , $\forall n \geq 0$,

$u_n = \frac{1}{w}(r_1^n - r_2^n)$.

Si $s \neq 0,$ pour tout $n \geq 1,\ u_n = s^{n-1} R_n(\frac{\delta}{s^2})$ où R_n est un polynôme de $Z[X]$ de degré p si $n = 2p + 1$ ou $2(p + 1)$.

Ces polynômes R_n vérifient la relation de récurrence $R_{n+2}(X) = R_{n+1}(X) - XP_n(X)$ pour tout $n \geq 1$.

$R_1(X) = 1, R_2(X) = 1, R_3(X) = -X + 1, R_4(X) = -2X + 1, R_5(X) = X^2 - 3X + 1$

$R_6(X) = 3X^2 - 4X + 1, R_7(X) = -X^3 + 6X^2 - 5X + 1, R_8(X) = -4X^3 + 10X^2 - 6X + 1$

$R_9(X) = X^4 - 10X^3 + 15X^2 - 7X + 1, R_{10}(X) = 5X^4 - 20X^3 + 21X^2 - 8X + 1$
Le terme constant de P_n est toujours 1.

Cela s'obtient en faisant une récurrence à partir de $u_{n+2} = su_{n+1} - \delta u_n$ et $u_1 = 1,\ u_2 = 1$ (qui sont des polynômes de degré 0) :
$u_{n+2} = s(s^n R_{n+1}(\frac{\delta}{s^2})) - \delta s^{n-1} R_n(\frac{\delta}{s^2}) = s^{n+1}(R_{n+1}(\frac{\delta}{s^2}) - \frac{\delta}{s^2} R_n(\frac{\delta}{s^2}))$.

On verra au III de cette annexe que R_n a n racines réelles distinctes, toutes supérieures à $\frac{1}{4}$. Et on précisera dans quels cas R_n a des racines rationnelles et on précisera ces racines rationnelles.
On notera que si $s \neq 0,\ u_n = 0$ pour $n \geq 1$ alors obligatoirement $\delta \neq 0,$ puisque $\frac{\delta}{s^2}$ est racine de R_n de terme constant 1.

Moins immédiat : si $n \geq 3,\ s \neq 0,\ u_n = 0$ alors outre $\delta \neq 0$ on a $s^2 - 4\delta < 0$ et donc $\delta > 0$.
Note : u_0 est toujours nul, $u_1 = 1$ n'est jamais nul, de même que $u_2 = s$ puisqu'ici $s \neq 0$.
Exemple : $u_4 = s^3 - 2\delta s = 0 \Leftrightarrow s^2 = 2\delta$ (car $s \neq 0$) et $s^2 - 4\delta = -s^2 < 0$

En effet,
si $s^2 - 4\delta = 0,$ comme $\delta \neq 0,$ on aurait $u_n = n(\frac{s}{2})^{n-1} \neq 0$ ce qui est contraire à l'hypothèse
si $s^2 - 4\delta > 0,$ on aurait $u_n = \frac{1}{w}(r_1^n - r_2^n)$ avec r_1 et r_2 les racines de l'équation caractéristique (voir ci-dessus) réelles et distinctes. Donc $r_1^n = r_2^n$ n'est possible que si $r_1 = -r_2$ (et si n pair), mais $s \neq 0$ l'interdit ($s = r_1 + r_2$) et donc u_n ne peut être nul et on est encore en contradiction avec l'hypothèse.
Donc la seule possibilité est $s^2 - 4\delta < 0$.

Lemme 3
Soit $f \in E$ d'ordre $n \geq 3$:
il est évident que si $cr + d \neq 0$ et $r = f(r),$ alors $f^{(k)}(r) = r$ pour tout $k \geq 1$.
En fait on a aussi :
pour $1 \leq k < n,$ si $f^{(k)}(r)$ est défini et si $f^{(k)}(r) = r,$ alors $f(r)$ est défini et $r = f(r)$.

preuve

$f(X) = \frac{aX+b}{cX+d}$ et $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$: il est évident que $f(r) = r \Leftrightarrow cr + d \neq 0$ et
$A\begin{pmatrix} r \\ 1 \end{pmatrix} = (cr+d)\begin{pmatrix} r \\ 1 \end{pmatrix}$
$f^{(k)}(X) = \frac{a_k X + b_k}{c_k X + d_k}$ et $A^k = \begin{pmatrix} a_k & b_k \\ c_k & d_k \end{pmatrix}$.
Donc $f^{(k)}(r) = r \Leftrightarrow c_k r + d_k \neq 0$ et $A^k\begin{pmatrix} r \\ 1 \end{pmatrix} = (c_k r + d_k)\begin{pmatrix} r \\ 1 \end{pmatrix}$.
Mais $A^k = u_k A + v_k I,$ donc $u_k A\begin{pmatrix} r \\ 1 \end{pmatrix} = (c_k r + d_k - v_k)\begin{pmatrix} r \\ 1 \end{pmatrix}$, et comme $u_k \neq 0$ (sinon $A^k = v_k I$, avec $v_k \neq 0$ puisque $\delta \neq 0,$ et f serait d'ordre $\leq k < n$) on a

$A\begin{pmatrix} r \\ 1 \end{pmatrix} = \lambda\begin{pmatrix} r \\ 1 \end{pmatrix}$ avec $\lambda \neq 0$ (sinon A serait singulière ce qui est exclu puisque $\delta \neq 0$).
Donc $ar + b = \lambda r, cr + d = \lambda \neq 0,$ cad $f(r)$ est défini et $f(r) = r$.

1) Caractérisation générale des $f \in E$ avec $f(X) = \frac{aX+b}{cX+d}$ et $ad - bc \neq 0$ d'ordre $n \geq 3$

On notera dans tout ce qui suit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $s = a + d, \delta = ad - bc \neq 0$ et les suites u_n, v_nseront les suites définies au lemme 2 par $A^n = u_n A + v_n I$.

1.1) **Soit** $n \geq 3$.
$f \in E$ **est d'ordre** $n \geq 3 \Leftrightarrow f(X) = \frac{aX+b}{cX+d}, s \neq 0$ **et** $u_n = 0$ **et**,**SI** $n \geq 6$ **et** n **pas premier**, **pour tout** j **divisant** n **et** $3 \leq j \leq \frac{n}{2}$, $u_j \neq 0$ (cad $R_j(\frac{\delta}{s^2}) \neq 0$).

Remarque 1 :
Au cours de la preuve de cette caractérisation, on montre, SANS savoir que $\delta \neq 0,$ que si $s \neq 0$ et $u_n = 0$ alors $\delta \neq 0,$ et donc $f \in E$ et $f^{(n)} = id$.
On montre aussi que si $f \in E$ est d'ordre $n \geq 3,$ $\forall j \in \{1; 2; \ldots; n-1\}$ on a $u_j \neq 0$.
Remarque 2 :
Si $f \in E$ est d'ordre $n \geq 3,$ on a toujours $v_n \neq 0$ et $bc \neq 0$.
Donc si $f \in E$ et est d'ordre $\geq 3,$ ce n'est jamais un polynôme, mais, voir preuve ci-après du 1.1), c'est aussi vrai pour tout $f^{(j)}$ avec $2 \leq j \leq n-1$.
Remarque 3 :
$f \in E$ est d'ordre $n \geq 3,$ impliquant $s \neq 0$ et $u_n = 0$
d'après le lemme 2, $s^2 - 4\delta < 0,$ donc $\delta > \frac{s^2}{4} > 0$
d'après le lemme 2, $u_n = 0 \Leftrightarrow \frac{\delta}{s^2}$ est une racine de $P_{n,}$ racine qui est supérieure à $\frac{1}{4}$, d'après ce qui précéde ; en fait on verra au III de cette annexe que toutes les racines de R_n sont réelles et supérieures à $\frac{1}{4}$.
la condition $\frac{\delta}{s^2}$ est une racine r de $P_{n,}$ sera toujours donnée dans les exemples ci-après sous la forme bc en fonction de a et d : $bc = ad - r(a+d)^2$.
$cr + d \neq 0$ et $r = f(r) \Rightarrow r \notin \mathbb{R}$ (car $r = f(r) \Leftrightarrow cr^2 + (d-a)r - b = 0$ de discriminant $(a-d)^2 + 4bc = s^2 - 4\delta < 0$)

1.2)
Si n est pair, si $f \in E$ est d'ordre $n,$ alors $f^{(\frac{n}{2})}$ est d'ordre $2,$ et $f^{(\frac{n}{2})}(X) = \frac{\lambda}{X}$ (λ constante) $\Leftrightarrow a = d$.

1.3) Pour $n \geq 3,$ il existe $f(X) = \frac{aX+b}{cX+d} \in E \cap \mathbb{Q}(X)$ d'ordre $n \Leftrightarrow P_n$ a au moins une racine rationnelle.

Cf les exemples ci-dessous ceci est impossible si $n = 5$ ou 7 ou 8 : **au III de cette annexe on montrera qu'il existe** $f(X) = \frac{aX+b}{cX+d} \in E \cap \mathbb{Q}(X)$ **d'ordre** $n \geq 2 \Leftrightarrow n = 2$ **ou** $n = 3$ **ou** $n = 4$ **ou** $n = 6$.

2) Les $f \in E$ d'ordre 2 s'écrivent $f(X) = \frac{aX+b}{cX-a}$ avec $a^2 + bc \neq 0$

Exemples :

si $c = 0$, auquel cas $a \neq 0$ alors $f(X) = -X - \frac{b}{a}$: c'est un polynôme

si $a = 0$ alors $bc \neq 0$ et $f(X) = \frac{b}{cX}$, cad $f(X) = \frac{\lambda}{X}$ avec λ constante.

Bien sûr, pour ce cas la preuve ne fera pas appel au 1.1), puisque $n = 2 < 3$.

En prenant $a \in \mathbb{Q}$, on peut choisir b et c dans $\mathbb{Q}$ tels que $a^2 + bc \neq 0$
et alors $f \in E \cap \mathbb{Q}(X)$.

Les cas $n \in \{3;4;5;6;7;8\}$, eux, seront des applications immédiates de la caractérisation donnée au 1.1).

3) Les $f \in E$ d'ordre 3 s'écrivent $f(X) = \frac{aX+b}{cX+d}$ avec $a + d \neq 0$ et $bc = -(a^2 + d^2 + ad)$

Exemple : $f(X) = \frac{-X-3}{X+2}$.

En prenant a et d quelconques dans $\mathbb{Q}$, non opposés, on peut choisir b et c dans $\mathbb{Q}$ tels que $bc = -(a^2 + d^2 + ad)$ et alors $f \in E \cap \mathbb{Q}(X)$.

4) Les $f \in E$ d'ordre 4 s'écrivent $f(X) = \frac{aX+b}{cX+d}$
avec $a + d \neq 0$ et $2bc = -(a^2 + d^2)$.

En prenant a et d quelconques dans $\mathbb{Q}$, non opposés, on peut choisir b et c dans $\mathbb{Q}$ tels que $2bc = -(a^2 + d^2)$ et alors $f \in E \cap \mathbb{Q}(X)$.

Exemples : $f(X) = \frac{2mX - m^2}{2X}$ avec $m \in \mathbb{Q}^*$; $f(X) = \frac{X+1}{-X+1}$ ($\Rightarrow f^{(2)}(X) = \frac{-1}{X}$)

5) Les $f \in E$ d'ordre 5 s'écrivent $f(X) = \frac{aX+b}{cX+d}$
avec $a + d \neq 0$ et $bc = ad - \frac{3 \pm \sqrt{5}}{2}(a+d)^2$.
On notera qu'ici, a, b, c, d ne peuvent pas être tous rationnels et donc, il n'existe pas $f \in E \cap \mathbb{Q}(X)$ qui soit d'ordre 5.

6) Les $f \in E$ d'ordre 6 s'écrivent $f(X) = \frac{aX+b}{cX+d}$
avec $a + d \neq 0$ et $3bc = -(a^2 + d^2 - ad)$

Exemple : $f(X) = \frac{3X-1}{3X+3}$
les itérés de f sont $\frac{X-1}{3X+1}, \frac{-1}{3X}, -\frac{X+1}{3X-1}, -\frac{3X+1}{3X-3}, X$.

En prenant a et d quelconques dans $\mathbb{Q}$, non opposés, on peut choisir b et c dans $\mathbb{Q}$ tels que $3bc = -(a^2 + d^2 - ad)$ et alors $f \in E \cap \mathbb{Q}(X)$.

7) Les $f \in E$ d'ordre 7 s'écrivent $f(X) = \frac{aX+b}{cX+d}$
avec $a + d \neq 0$ et $bc = ad - r_i(a+d)^2$ où r_i est une des trois racines (toutes réelles, aucune rationnelle) de $X^3 - 6X^2 + 5X - 1$. Ces racines peuvent être explicitées à l'aide de radicaux (Cardan), mais bon...on verra mieux au III.
On notera qu'ici, a, b, c, d ne peuvent pas être tous rationnels et donc, il n'existe pas

$f \in E \cap \mathbb{Q}(X)$ qui soit d'ordre 7.

8) Les $f \in E$ d'ordre 8 s'écrivent $f(X) = \frac{aX+b}{cX+d}$
avec $a+d \neq 0$ et $bc = ad - (1 \pm \frac{\sqrt{2}}{2})(a+d)^2$.
On notera qu'ici, a, b, c, d ne peuvent pas être tous rationnels et donc, il n'existe pas $f \in E \cap \mathbb{Q}(X)$ qui soit d'ordre 8.
Exemple : $f(X) = \frac{X+(3+2\sqrt{2})}{-X+1}$
$f^{(4)}(X) = \frac{-(3+2\sqrt{2})}{X}, f^{(8)}(X) = X$
Remarque : en prenant $A = \begin{pmatrix} 1 & 3+2\sqrt{2} \\ -1 & 1 \end{pmatrix}$:
$A^4 = \begin{pmatrix} 0 & -40\sqrt{2}-56 \\ 8\sqrt{2}+8 & 0 \end{pmatrix}^2, A^8 = \begin{pmatrix} -768\sqrt{2}-1088 & 0 \\ 0 & -768\sqrt{2}-1088 \end{pmatrix}$
Bien sûr, on vérifie que, $\frac{-40\sqrt{2}-56}{8\sqrt{2}+8} = -(3+2\sqrt{2})$

preuves :

1.1) Montrons que $f \in E$ est d'ordre $n \geq 3 \Rightarrow s \neq 0$ et $u_n = 0$ et, SI $n \geq 6$ et n pas premier, pour tout j divisant n et $3 \leq j \leq \frac{n}{2}$, $u_j \neq 0$.

Puisque $f \in E$, $\delta \neq 0$.
Et $f^{(n)} = id$ donne $A^n = \lambda_n I$ avec $\lambda_n \neq 0$ ($\delta^n = \lambda_n^2$), d'où $\lambda_n I = u_n A + v_n I$.
Si $u_n \neq 0$, on a $A = \mu I$ avec $\mu \neq 0$ (car $\delta \neq 0$) et f est d'ordre $1 \neq n \geq 3$, donc contradiction.
Ainsi $u_n = 0$.
Et $s \neq 0$, car sinon $A^2 = -\delta I$ et f est d'ordre ≤ 2, ce qui est encore en contradiction avec $n \geq 3$.
Et, pour tout $j \in \{1; 2; \ldots; n-1\}$, $u_j \neq 0$, sinon $A^j = u_j A + v_j I = v_j I$ et f serait d'ordre $\leq j < n$.

On montre maintenant la réciproque.
$u_n = 0$ donne $A^n = v_n I$ et ainsi f est d'ordre $p \leq n$ avec p divisant n (cf lemme 1).
Si $v_n = 0$, alors $\delta = 0$ ($\delta^n = v_n^2$), et donc (voir cas particuliers du lemme 2) $u_n = s^{n-1}$ pour $n \geq 2$, d'où $s = 0$ ce qui est en contradiction avec l'hypothèse $s \neq 0$.
Ainsi $v_n \neq 0$, donc $\delta \neq 0$ et f est bien dans E et $f^{(n)} = id$.
f ne peut être d'ordre 1, car cela implique $A = \lambda_1 I$ avec $\lambda_1 \neq 0$ et alors $a = d = \lambda_1$ et $b = c = 0$, donc $s^2 = (2a)^2 = 4\delta \neq 0$, donc (voir cas particuliers du lemme 2) $u_n = n(\frac{s}{2})^{n-1}$ et comme $u_n = 0$, on obtient $s = 0$ encore en contradiction avec l'hypothèse $s \neq 0$.
f ne peut être d'ordre 2, car alors $A^2 = \lambda_2 I$, donc $u_2 A = (\lambda_2 - v_2) I$ et comme $u_2 = s \neq 0$, on a $A = \mu I$ (donc $\mu \neq 0$ car $\delta \neq 0$) et f est d'ordre 1, ce qui vient d'être exclu.
Donc f est d'ordre $p \geq 3 : 3 \leq p \leq n$ et p divise n.
si n est premier, alors $p = n$

si $n = 4$, comme 3 ne divise pas 4, c'est que $p = 4 = n$
si $n \geq 6$ et n n'est pas premier : on a $n = qp$ avec $q \geq 1$, mais si $q \geq 2$, alors $3 \leq p \leq \frac{n}{2}$ et donc, par hypothèse, u_p n'est pas nul, donc f n'est pas d'ordre p (sinon dans ce cas u_p serait nul, d'après la preuve du sens direct) et contradiction avec la définition de p. Donc $q = 1$ et $p = n$.
Donc dans tous les cas on a f d'ordre $p = n$.

Prouvons la remarque 2 de l'énoncé : si $f \in E$ est d'ordre $n \geq 3$, on a toujours $v_n \neq 0$ et $bc \neq 0$.
$v_n \neq 0$ est évident puisque $A^n = v_n I$ et $\delta \neq 0$ (en fait cela a été déjà été vu dans la preuve de la caractérisation).
Pour $bc \neq 0$ c'est un peu moins évident.
Supposons $bc = 0$, donc A va être triangulaire et en prenant par exemple $c = 0$ on a $A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$
Donc $A^n = \begin{pmatrix} a^n & \theta_n \\ 0 & d^n \end{pmatrix}$ et comme $A^n = v_n I$ avec $v_n \neq 0$, c'est que $a = d \neq 0$ ou $a = -d \neq 0$ (selon la parité de n) ; mais $s = a + d \neq 0$, donc la seule possibilité est $a = d$, donc $\theta_n = na^{n-1}b = 0$, d'où $b = 0$ et $A = aI$, avec $a \neq 0$, et f est d'ordre 1, ce qui est contraire à f d'ordre $n \geq 3$.
bc étant différent de 0, on a $c \neq 0$ et f n'est pas un polynôme, mais cela est aussi vrai pour tout $f^{(j)}$ avec $2 \leq j \leq n-1$:
si $f^{(j)}$ est un polynôme alors $A^j = u_j A + v_j I$ a son terme $(2,1)$ nul, donc $u_j c = 0$, soit $u_j = 0$
et alors $A^j = v_j I$, donc $v_j = 0$ (sinon $f^{(j)} = id$ et contradiction avec f d'ordre n, puisque $j < n$)
et on arrive ainsi à $A^j = 0$, ce qui est impossible car $ad - bc \neq 0$.

1.2) Si n est pair, $f^{(\frac{n}{2})}$ est évidemment d'ordre 2 car $f^{(\frac{n}{2})} \circ f^{(\frac{n}{2})} = f^{(n)} = id$ **et** $f^{(\frac{n}{2})} \neq id$ puisque f est d'ordre $n > \frac{n}{2}$.
$f^{(\frac{n}{2})}$ étant d'ordre 2, on verra au 2) ci-dessous que $f^{(\frac{n}{2})}(X) = \frac{a'X + b'}{c'X + d'}$ avec $a'^2 + b'c' \neq 0$; donc si $a' \neq 0$, $f^{(\frac{n}{2})}(X) \neq \frac{\lambda}{X}$.
Montrons que $f^{(\frac{n}{2})}(X) = \frac{\lambda}{X} \Leftrightarrow a = d$; on notera $n' = \frac{n}{2}$.
$f^{(n')}(X) = \frac{\lambda}{X} \Leftrightarrow A^{n'} = \begin{pmatrix} 0 & \times \\ \times & 0 \end{pmatrix}$ avec $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $f(X) = \frac{aX + b}{cX + d}$.
$\Leftrightarrow u_{n'} A + v_{n'} I = \begin{pmatrix} 0 & \times \\ \times & 0 \end{pmatrix}$
$\Leftrightarrow u_{n'} a + v_{n'} = 0$ et $u_{n'} d + v_{n'} = 0$
$\Leftrightarrow a = d$ et $u_{n'} a + v_{n'} = 0$ (car si $a \neq d$, par différence on voit qu'il faut $u_{n'} = 0$ et alors $A^{n'} = v_{n'} I$, avec $v_{n'} \neq 0$ car $\delta \neq 0$, donc $f^{(n')} = id$, ce qui contredit que f est d'ordre $n > n'$).

Mais il se trouve que $a = d$ et f d'ordre $n \geq 3$ impliquent $u_{n'}a + v_{n'} = 0$.
En effet, puisque f est d'ordre $n \geq 3$, d'après le 1.1) on a $s \neq 0$ et $u_n = 0$; or d'après le lemme 2, $u_n = \frac{1}{w}(r_1^n - r_2^n)$ avec r_1, r_2 non nuls (car $\delta \neq 0$) et d'après la remarque 3 de l'énoncé du 1.1), $s^2 - 4\delta < 0$, donc r_1 et r_2 sont distincts, et non réels.
Ainsi $r_1^n = r_2^n$, d'où $\frac{r_1}{r_2} = e^{\frac{2ik\pi}{n}}$ (racine n –ième de 1) et $(\frac{r_1}{r_2})^{n'} = e^{ik\pi} = \pm 1$.
Comme $(\frac{r_1}{r_2})^{n'} = 1$ entraîne $u_{n'} = \frac{1}{w}(r_1^{n'} - r_2^{n'}) = 0$, soit $A^{n'} = v_{n'}I$, avec $v_{n'} \neq 0$, donc $f^{(n')} = id$, ce qui contredit que f est d'ordre $n > n'$, la seule possibilité est $r_1^{n'} = -r_2^{n'}$, d'où $u_{n'} = \frac{2r_1^{n'}}{w}$ et $v_{n'} = -\delta u_{n'-1}$ (voir lemme 2).
De $v_{n'} = \frac{-\delta}{w}(r_1^{n'-1} - r_2^{n'-1})$ et $-r_2^{n'-1} = \frac{r_1^{n'}}{r_2}$ on tire $v_{n'} = \frac{-\delta r_1^{n'}}{w}(\frac{1}{r_1} + \frac{1}{r_2}) = -\frac{sr_1^{n'}}{w}$ (car $r_1 + r_2 = s$ et $r_1 r_2 = \delta$) et ainsi $u_{n'}a + v_{n'} = \frac{r_1^{n'}}{w}(2a - s) = 0$, puisque $s = a + d$ et par hypothèse $a = d$.
Donc, f étant d'ordre $n \geq 3$, $f^{(n')}(X) = \frac{\lambda}{X} \Leftrightarrow a = d$ et $u_{n'}a + v_{n'} = 0 \Leftrightarrow a = d$.
Une vérification dans le cas $n = 6$: $u_3 = s^2 - \delta, v_3 = -\delta s$, donc $u_3 a + v_3 = a(s^2 - \delta) - \delta s$, mais d'après le 6) ci-dessous, $\frac{\delta}{s^2} = \frac{1}{3}$, ce qui donne $u_3 a + v_3 = \frac{2as^2}{3} - \frac{s^3}{3}$, qui est bien nul si $a = d$ car alors $s = a + d = 2a$.

1.3) D'après le 1.1), $f \in E$ sera d'ordre $n \geq 3$ implique $s \neq 0$ et $u_n = 0$, donc $\frac{\delta}{s^2}$ est racine de R_n. Si on impose que f soit dans $\mathbb{Q}(X)$, alors a, b, c, d sont tous rationnels et $\frac{\delta}{s^2}$ est une racine rationnelle de R_n.
Réciproquement si $\frac{\delta}{s^2}$ est une racine rationnelle r de R_n, $bc = ad - r(a + d)^2$ et en choisissant a, d, non opposés, dans $\mathbb{Q}$, on peut choisir b et c rationnels tels que $bc = ad - r(a + d)^2$ et alors $f \in E \cap \mathbb{Q}(X)$.

2) Le 1.1) n'étant vrai que pour $n \geq 3$, on fait ici un raisonnement particulier en utilisant $A^2 = sA - \delta I$.
Si $f \in E$ est d'ordre 2, alors $A^2 = \lambda I$ avec $\lambda \neq 0$ (puisque $(ad - bc)^2 = \lambda^2$ et $ad - bc \neq 0$) et $(a + d)A = (ad - bc)I + \lambda I$.
Nécessairement $a + d = 0$ sinon $A = \mu I$ avec $\mu \neq 0$ et A n'est pas d'ordre 2 ; par ailleurs $a + d = 0$ implique $a^2 + bc \neq 0$.
Réciproquement, si $a + d = 0$ et $a^2 + bc \neq 0$, $A^2 = (a^2 + bc)I$ et $A \neq \lambda I$ (sinon $A = \lambda I$, donc $\lambda \neq 0$, et alors $a = d = \lambda$, $a + d = 2\lambda$ et on a une contradiction avec $a + d = 0$) et ainsi f est bien d'ordre 2.

On peut bien sûr faire autrement : $f^{(2)} = id \Rightarrow f^{-1} = f$ et en utilisant les préliminaires cela implique l'existence de ρ tel que $d = \rho a, -b = \rho b, -c = \rho c, a = \rho d$, et donc f d'ordre 2 implique que $d(1 - \rho^2) = b(1 + \rho) = c(1 + \rho) = 0$; donc $\rho = -1$ ou 1 (sinon $d = b = c = 0$, contraire à $ad - bc \neq 0$) : si $\rho = 1$ alors $b = c = 0$ et $a = d \neq 0$ et $f = id$ n'est pas d'ordre 2, si $\rho = -1$, alors $d = -a$ et la seule possibilité est $f(X) = \frac{aX + b}{cX - a}$ avec $a^2 + bc \neq 0$, possibilité qui est bien d'ordre 2.

3) $f \in E$ est d'ordre 3 équivaut à $s \neq 0$ et $u_3 = s^2(1 - \frac{\delta}{s^2}) = 0$.

Et $u_3 = 0 \Leftrightarrow \frac{\delta}{s^2} = 1 \Leftrightarrow ad - bc = (a+d)^2 \Leftrightarrow bc = -(a^2 + d^2 + ad)$

4) $f \in E$ est d'ordre 4 équivaut à $s \neq 0$ et $u_4 = s^3(1 - 2\frac{\delta}{s^2}) = 0$.

Et $u_4 = 0 \Leftrightarrow \frac{\delta}{s^2} = \frac{1}{2} \Leftrightarrow 2(ad - bc) = (a+d)^2 \Leftrightarrow 2bc = -(a^2 + d^2)$

5) $f \in E$ est d'ordre 5 équivaut à $s \neq 0$ et $u_5 = s^4(1 - 3\frac{\delta}{s^2} + (\frac{\delta}{s^2})^2) = 0$.

Les racines de $R_5(X) = 1 - 3X + X^2$ étant $\frac{3 \pm \sqrt{5}}{2}$, $u_5 = 0 \Leftrightarrow bc = ad - \frac{3 \pm \sqrt{5}}{2}(a+d)^2$

6) $f \in E$ est d'ordre 6 équivaut à $s \neq 0$ et $u_6 = s^5(1 - 4\frac{\delta}{s^2} + 3(\frac{\delta}{s^2})^2) = 0$ et $u_3 \neq 0$ (car 3 est le seul j divisant 6 et $3 \leq j \leq \frac{6}{2}$: voir 1.1)).

Les racines de $R_6(X) = 1 - 4X + 3X^2$ sont 1 et $\frac{1}{3}$, donc $\frac{\delta}{s^2} = 1$ ou $\frac{\delta}{s^2} = \frac{1}{3}$.

Mais pour chacune de ces possibilités il faut voir si $u_3 \neq 0$, cad si $R_3(\frac{\delta}{s^2}) \neq 0$; or $R_3(X) = -X + 1$, donc $\frac{\delta}{s^2} = 1$ est à exclure et la seule possibilité est $\frac{\delta}{s^2} = \frac{1}{3}$.

Donc $f \in E$ est d'ordre 6 équivaut à $s \neq 0$ et $3\delta = s^2$, soit $3bc = -(a^2 + d^2 - ad)$.

7) $f \in E$ est d'ordre 7 équivaut à $s \neq 0$ et $u_7 = s^6(1 - 5\frac{\delta}{s^2} + 6(\frac{\delta}{s^2})^2 - (\frac{\delta}{s^2})^3) = 0$ (puisque 7 est premier).

Donc $u_7 = 0 \Leftrightarrow \frac{\delta}{s^2}$ est racine de $R_7(X) = 1 - 5X + 6X^2 - X^3$, et en notant r_i les trois racines de R_7 (elles sont réelles, non rationnelles : si $\frac{p}{q}$ est une racine rationnelle avec p et q premiers entre eux, on voit tout de suite que p doit diviser q et q diviser p, donc $\frac{p}{q} = \pm 1$, valeurs qui ne sont pas racines),

et $u_7 = 0 \Leftrightarrow \frac{ad - bc}{(a+d)^2} = r_1$ ou r_2 ou r_3.

8) $f \in E$ est d'ordre 8 équivaut à $s \neq 0$ et $u_8 = 0$ et $u_4 \neq 0$ (car 4 est le seul j divisant 4 et $3 \leq j \leq \frac{8}{2}$: voir 1.1)).

$u_8 = s^7 R_8(\frac{\delta}{s^2})$ et $R_8 = R_7 - XR_6$ soit $R_8(X) = -4X^3 + 10X^2 - 6X + 1$, lequel a pour racines $\frac{1}{2}$ et $1 \pm \frac{\sqrt{2}}{2}$.

A noter que R_8, de degré 3, a une racine rationnelle, ce qui n'est pas le cas de R_7.

Ainsi $\frac{\delta}{s^2} = \frac{1}{2}$ ou $1 + \frac{\sqrt{2}}{2}$ ou $1 - \frac{\sqrt{2}}{2}$.

Mais, pour chacune de ces possibilités il faut voir si $u_4 \neq 0$, cad si $R_4(\frac{\delta}{s^2}) \neq 0$; or $R_4(X) = -2X + 1$ et $\frac{\delta}{s^2} = \frac{1}{2}$ est à exclure et fiinalement il n'y a que $\frac{\delta}{s^2} = 1 \pm \frac{\sqrt{2}}{2}$ qui convient pour que f soit d'ordre 8.

□

III) Détermination des $f \in E \cap \mathbb{Q}(X)$ d'ordre n avec $n \geq 2$.

Cette détermination va se faire en explicitant les racines des polynômes R_n définis au

lemme 2 du II) : $A^n = u_n A + v_n I$ et $u_n = s^{n-1} R_n(\frac{\delta}{s^2})$.

Il sera alors facile d'en déduire (voir le 4) ci-dessous) que
pour seulement $n = 2$ ou 3 ou 4 ou 6, il existe de $f \in E \cap \mathbb{Q}(X)$ d'ordre n.

1) Cf le lemme 2 du II) on a
$R_1(X) = R_2(X) = 1$ et $\forall n \geq 1,\ R_{n+2}(X) = R_{n+1}(X) - XR_n(X)$. (voir toujours le lemme 2, pour les dix premières valeurs de R_n).

Mais rien n'empêche de poser $R_0(X) = 0$ et alors $\boxed{\forall n \geq 0,\ R_{n+2}(X) = R_{n+1}(X) - XR_n(X).}$

En fait cette suite est du type $\forall n \geq 0, S_{n+2} = AS_{n+1} + BS_n$ avec $A = 1$ et $B = -X$: c'est une suite de Fibonacci généralisée.
Dans mon papier AB-8fibo-monsite.pdf, ces suites sont étudiées dans leur généralité avec A, B, S_0, S_1 quelconques.

2) $\boxed{\forall n \geq 1,\ R_n(X) = \frac{1}{2^{n-1}} \sum_{0 \leq k \leq \frac{n-1}{2}} C_n^{2k+1}(1-4X)^k}$

preuve :
on applique Binet à la suite $\forall n \geq 0, U_{n+2} = U_{n+1} - cU_n$ avec $U_0 = 0, U_1 = 1$ et c constante réelle distincte de $\frac{1}{4}$ et de 0.
L'équation caractéristique de cette suite est $r^2 - r + c = 0$ de discriminant $1 - 4c$ et donc elle a deux racines distinctes r_1 et r_2 non nulles et il existe deux constantes λ et μ telles que $\forall n \geq 0$ on a $U_n = \lambda r_1^n + \mu r_2^n$: $U_0 = 0$ et $U_1 = 1$ donnent λ et μ :
$U_n = \frac{1}{w}((\frac{1+w}{2})^n - (\frac{1-w}{2})^n)$ avec w une racine 2 –ième de $1 - 4c$ (qui peut être imaginaire)
En développant on obtient, pour $n \geq 1,\ U_n = \frac{1}{2^{n-1}} \sum_{0 \leq k \leq \frac{n-1}{2}} C_n^{2k+1}(1-4c)^k$.

Posons, $T_0(X) = 0$ et pour $n \geq 1,\ T_n(X) = \frac{1}{2^{n-1}} \sum_{0 \leq k \leq \frac{n-1}{2}} C_n^{2k+1}(1-4X)^k$, donc $T_n \in \mathbb{Q}[X]$,

$T_1(X) = C_1^0(1-4X)^0 = 1$.
Puisque par définition de T_n, $\forall n \geq 0,\ T_n(c) = U_n$,
on a $\forall n \geq 0,\ T_{n+2}(c) - T_{n+1}(c) + cT_n(c) = 0$.
Mais cela est vrai pour tout c distinct de 0 et $\frac{1}{4}$, donc $\forall n \geq 0,\ T_{n+2}(X) - T_{n+1}(X) + XT_n(X)$ est le polynôme nul ; donc les polynômes R_n et T_n vérifient la même relation de récurrence avec les mêmes conditions initiales en $n = 0$ et $n = 1$: ils sont donc égaux.

3) $\boxed{\forall n \geq 1,\ R_n(X) = \sum_{0 \leq k \leq \frac{n-1}{2}} (-1)^k C_{n-1-k}^k X^k}$

Par exemple, $R_1(X) = R_2(X) = (-1)^0 C_{0 \text{ ou } 1}^0 X^0 = 1$,
$R_3(X) = (-1)^0 C_2^0 X^0 + (-1)^1 C_{2-1}^1 X^1 = 1 - X$ et
$R_{10}(X) = (-1)^0 C_9^0 X^0 + (-1)^1 C_8^1 X^1 + (-1)^2 C_7^2 X^2 + (-1)^3 C_6^3 X^3 + (-1)^4 C_5^4 X^4$
$= 1 - 8X + 21X^2 - 20X^3 + 5X^4$.

Conséquences immédiates :

$\forall n \geq 1$ $d°R_n = \frac{n-1}{2}$ si n est impair, le coefficient de tête étant $(-1)^{\frac{n-1}{2}}$

$\forall n \geq 1$ $d°R_n = \frac{n}{2} - 1 < \frac{n-1}{2}$ si n est pair, le coefficient de tête étant $(-1)^{\frac{n}{2}-1}\frac{n}{2}$

$\forall n \geq 1$ le terme constant de R_n est 1 (ceci peut se faire via la relation de récurrence, car $R_1(0) = R_2(0) = 1$)

$\forall n \geq 2$ le coefficient de X dans R_n est $-(n-2)$ (ceci peut se faire aussi via la relation de récurrence, car si c_n est le coefficient de X dans R_n, $c_{n+2} = c_{n+1} - 1$, $\forall n \geq 1$)

preuve :

voir AB-8fibo-monsite.pdf.

4) Pour $n \geq 3$, pour $k = 1, 2 \ldots, d°R_n$, les racines de R_n sont

$$\boxed{r_{k,n} = \frac{1}{4}(1 + \tan^2(\frac{k\pi}{n})) = \frac{1}{4\cos^2(\frac{k\pi}{n})}}$$

Toutes ces racines sont donc $> \frac{1}{4}$.

Si R_n a une racine rationnelle, cette racine rationnelle $\in \{\frac{1}{3}; \frac{1}{2}; 1\}$:

1 est racine de $R_n \Leftrightarrow 3$ divise n

$\frac{1}{2}$ est racine de $R_n \Leftrightarrow 4$ divise n

$\frac{1}{3}$ est racine de $R_n \Leftrightarrow 6$ divise n

preuve :

R_0 étant le polynôme nul et $R_1(X) = R_2(X) = 1$ n'ayant pas de racine, on s'intéresse aux racines de R_n que pour $n \geq 3$.

D'après la preuve du 2) ci-dessus, pour tout $x \neq 0$ et $x \neq \frac{1}{4}$, pour tout $n \geq 1$,

$R_n(x) = \frac{1}{w}((\frac{1+w}{2})^n - (\frac{1-w}{2})^n)$ avec w une racine 2 –ième de $1 - 4x$.

Comme 0 et $\frac{1}{4}$ ne sont pas racines de R_n (car $\forall n \geq 1$, $R_n(0) = 1$ et $R_n(\frac{1}{4}) = \frac{n}{2^{n-1}}$),

x est racine de $R_n \Leftrightarrow (1+w)^n = (1-w)^n \Leftrightarrow (\frac{1+w}{1-w})^n = 1$, car $x \neq 0 \Rightarrow w \neq 1$

x est racine de $R_n \Leftrightarrow \frac{1+w}{1-w} = \xi$ avec ξ racine n –ième de 1

Mais $\frac{1+w}{1-w} \neq -1$ et $\frac{1+w}{1-w} \neq 1$ car $x \neq \frac{1}{4}$,

et ainsi x est racine de $R_n \Leftrightarrow \frac{1+w}{1-w} = \xi$ avec ξ racine n –ième de 1, distincte de -1 et 1,

x est racine de $R_n \Leftrightarrow w = \frac{\xi - 1}{\xi + 1}$ avec ξ racine n –ième de 1, distincte de -1 et 1,

ce qui implique $1 - 4x = (\frac{\xi - 1}{\xi + 1})^2$.

Posons $\theta_{k,n} = \frac{k\pi}{n}$ et $\xi_{k,n} = e^{2i\theta_{k,n}}$ pour $1 \leq k \leq n-1$ et $k \neq \frac{n}{2}$, donc $\theta_{k,n} \in]0; \pi[- \{\frac{\pi}{2}\}$.

Les formules trigonométriques $\cos 2u - 1 = -2\sin^2 u$ et $\cos 2u + 1 = 2\cos^2 u$ donnent

$$\frac{\xi_{k,n} - 1}{\xi_{k,n} + 1} = \frac{-2\sin^2\theta_{k,n} + 2i\sin\theta_{k,n}\cos\theta_{k,n}}{2\cos^2\theta_{k,n} + 2i\sin\theta_{k,n}\cos\theta_{k,n}} = i\tan\theta_{k,n}.$$

Donc si x est racine de R_n, nécessairement $1 - 4x = -\tan^2\theta_{k,n}$ et les racines de R_n ne peuvent être que $r_{k,n} = \frac{1}{4}(1 + \tan^2\theta_{k,n})$ pour pour $1 \leq k \leq n-1$ et $k \neq \frac{n}{2}$.

Réciproquement, une racine n –ième de $1 - 4r_{k,n} = -\tan^2\theta_{k,n}$ étant $i\tan\theta_{k,n}$,

$R_n(r_{k,n}) = \frac{1}{i\tan\theta_{k,n}}(\frac{1+i\tan\theta_{k,n}}{2})^n - (\frac{1-i\tan\theta_{k,n}}{2})^n)$, et en utilisant Moivre, on obtient $R_n(r_{k,n}) = 2i\sin(n\theta_{k,n}) = 0$.

Donc les racines de R_n sont les $r_{k,n} = \frac{1}{4}(1+\tan^2\theta_{k,n})$ pour pour $1 \le k \le n-1$ et $k \ne \frac{n}{2}$.

Reste à voir lesquelles sont distinctes.

De $\tan(\pi - \frac{k\pi}{n}) = \tan\frac{(n-k)\pi}{n} = -\tan\frac{k\pi}{n}$, on déduit que $r_{n-k,n} = r_{k,n}$, d'où

si n est impair, $r_{1,2}, r_{2,n}, \ldots, r_{\frac{n-1}{2},n}$ sont distintes car

$0 < \theta_{1,n} < \theta_{2,n} < \ldots < \theta_{\frac{n-1}{2},n} < \frac{\pi}{2}$ et $r_{\frac{n-1}{2},n}, \ldots, r_{n-1,n}$ sont les mêmes que les précédentes et on obtient $\frac{n-1}{2}$ racines pour R_n : ce sont toutes ses racines, son degré étant $\frac{n-1}{2}$

si n est pair, $r_{1,2}, r_{2,n}, \ldots, r_{\frac{n}{2}-1,n}$ sont distinctes car $0 < \theta_{1,n} < \theta_{2,n} < \ldots < \theta_{\frac{n}{2}-1,n} < \frac{\pi}{2}$ et $r_{\frac{n}{2}+1,n}, \ldots, r_{n-1,n}$ sont les mêmes que les précédentes (k étant $\ne \frac{n}{2}$ il n'y a pas à considérer $r_{\frac{n}{2},n}$) et on obtient $\frac{n}{2} - 1$ racines pour R_n : ce sont toutes ses racines, son degré étant $\frac{n}{2} - 1$.

On notera tout de suite que l'écriture $r_{k,n} = \frac{1}{4}(1+\tan^2\theta_{k,n})$ des racines de R_n permet de dire

si 3 divise n, $r_{\frac{n}{3},n} = \frac{1}{4}(1+\tan^2\frac{\pi}{3}) = 1$ est racine de R_n

si 4 divise n, $r_{\frac{n}{4},n} = \frac{1}{4}(1+\tan^2\frac{\pi}{4}) = \frac{1}{2}$ est racine de R_n

si 6 divise n, $r_{\frac{n}{6},n} = \frac{1}{4}(1+\tan^2\frac{\pi}{6}) = \frac{1}{3}$ est racine de R_n

Ces trois résultats peuvent se démontrer uniquement à partir de la relation de récurrence vérifiée par les R_n :

il suffit de montrer que $R_{3p}(1) = 0 \Rightarrow R_{3(p+1)}(1) = 0$, car $R_3(1) = 0$

il suffit de montrer que $R_{4p}(\frac{1}{2}) = 0 \Rightarrow R_{4(p+1)}(\frac{1}{2}) = 0$, car $R_4(\frac{1}{2}) = 0$

il suffit de montrer que $R_{6p}(\frac{1}{3}) = 0 \Rightarrow R_{6(p+1)}(\frac{1}{3}) = 0$, car $R_6(\frac{1}{3}) = 0$

On va montrer maintenant la réciproque de ce résultat, à savoir que R_n ne peut avoir que $\frac{1}{3}$ et/ou $\frac{1}{2}$ et/ou 1 comme racine(s) rationnelle(s), les conditions nécessaires étant celles ci-dessus.

Pour cela je vais utiliser les deux résultats suivants (φ désignant la fonction d'Euler et voir wiki)

pour $n > 6$, $\varphi(n) \ge \sqrt{n}$ ($\varphi(6) = 2 < \sqrt{6}$; $\varphi(7) = 6 \ge \sqrt{7}$)

pour $n \ge 4$, k et n premiers entre eux, $\tan\frac{k\pi}{n}$ est algébrique sur $\mathbb{Q}$ de degré $\frac{\varphi(n)}{2}$ si 4 divise n, sinon son degré est $\varphi(n)$.

(si $n = 4$, k et n premiers entre eux, $\tan\frac{k\pi}{4} = \pm 1 \in \mathbb{Q}$, donc son degré est 1 et $\frac{\varphi(4)}{2} = \frac{2^2-2}{2} = 1$)

On déduit de ces résultats que si $n \geq 36,\ \varphi(n) \geq 6$ et alors le degré de $\tan\frac{k\pi}{n}$ (k et n premiers entre eux) est $\geq \frac{6}{2} = 3,$ donc $r_{k,n} \notin \mathbb{Q}$, sinon $r_{k,n} = q \in \mathbb{Q}$ et $\tan\frac{k\pi}{n}$ est racine de $X^2 - (4q-1) \in \mathbb{Q}[X]$ et $\tan\frac{k\pi}{n}$ est de degré $\leq 2,$ d'où contradiction.
Pour $n \leq 35,$ la consultation d'une table de φ permet de constater que, exceptés $n = 1,2,3,4,5,6,8,10,12,$ on a $\frac{\varphi(n)}{2} \geq 3$ et $r_{k,n} \notin \mathbb{Q}$ (toujours pour k et n premiers entre eux).
Il reste à examiner ce qui se passe pour les cas $n = 3,4,5,6,8,10,12,$ pour lesquels $\frac{\varphi(n)}{2} \leq 2.$

si $n = 3,\ R_3(X) = -X + 1$: seule racine $r_{1,3} = 1$

si $n = 4,\ R_4(X) = -2X + 1$: seule racine $r_{1,4} = \frac{1}{2}$

si $n = 5,\ R_5(X) = X^2 - 3X + 1$: les racines sont $r_{1,5}$ et $r_{2,5}$ soit $\frac{3 \pm \sqrt{5}}{2}$ (résolution du second degré) qui ne sont pas dans $\mathbb{Q}$

si $n = 6,\ R_6(X) = 3X^2 - 4X + 1$: les racines sont $r_{1,6} = \frac{1}{3}$ et $r_{2,6} = 1$

si $n = 8,\ R_8(X) = -4X^3 + 10X^2 - 6X + 1 : r_{2,8} = r_{1,4} = \frac{1}{2}$ et après division par $2X - 1$ et résolution d'un second degré on trouve que les deux autres racines $r_{1,8}$ et $r_{3,8}$ sont $1 \pm \frac{\sqrt{2}}{2}$ donc ne sont pas rationnelles

si $n = 10,\ R_{10}(X) = 1 - 8X + 21X^2 - 20X^3 + 5X^4 : r_{2,10} = r_{1,5}, r_{4,10} = r_{2,5}$ ne sont pas rationnelles (voir cas $n = 5$) ; mais aussi $r_{1,10}$ et $r_{3,10}$ ne sont pas rationnelles car $\tan\frac{\pi}{10}$ et $\tan\frac{3\pi}{10}$ sont de degré $\varphi(10) = \varphi(2)\varphi(5) = 4 \geq 3$

si $n = 12,\ R_{12}$ est de degré $\frac{12}{2} - 1 = 5$:

$r_{2,12} = r_{1,6} = \frac{1}{3}, r_{3,12} = r_{1,4} = \frac{1}{2}, r_{4,12} = r_{1,3} = 1$; de $\tan\frac{\pi}{6} = \frac{2\tan\frac{\pi}{12}}{1 - \tan^2\frac{\pi}{12}}$ on obtient $\tan\frac{\pi}{12} = 2 - \sqrt{3}$ par résolution du second degré $X^2 + 2\sqrt{3}X - 1 = 0$ (car par ailleurs $\tan\frac{\pi}{12} > 0$) ce qui donne $r_{1,12} = 2 - \sqrt{3} \notin \mathbb{Q}$ et de $\tan\frac{5\pi}{12} = \tan(\frac{\pi}{2} - \frac{\pi}{12}) = \frac{1}{2 - \sqrt{3}} = 2 + \sqrt{3}$ on tire $r_{5,12} = 2 + \sqrt{3} \notin Q.$

On constate donc, que si $n \geq 3,\ k$ et n premiers entre eux, il existe k $(1 \leq k \leq d°R_n)$ tel que $r_{k,n} \in Q$ équivaut à $n \in \{3;4;6;8;12\},$ et alors $r_{k,n} \in \{\frac{1}{3};\frac{1}{2};1\}.$

Mais si k et n ne sont pas premiers entre eux, $r_{k,n} = r_{k',n'}$ avec $\frac{k}{n} = \frac{k'}{n'}$ et k' et n' premiers entre eux ; mais forcément $n' \geq 3$ car $\frac{k}{n} \leq \frac{d°R_n}{n} < \frac{1}{2}$ et donc si $n' = 1$ c'est que $\frac{k}{n} \geq 1$ ce qui est impossible, et si $n' = 2$, c'est que $\frac{k}{n} \geq \frac{1}{2}$ ce qui est encore impossible.
Et donc dans ce cas $r_{k,n} = r_{k',n'} \in Q \Leftrightarrow n' \in \{3;4;6;8;12\}$ et on a encore $r_{k,n} \in \{\frac{1}{3};\frac{1}{2};1\}.$

Reste à préciser à quelles conditions ces racines rationnelles sont obtenues :

s'il existe k $(1 \leq k \leq d°R_n)$ tel que $r_{k,n} = 1,$

soit k et n sont premiers entre eux et $n = 3$ ou 6 ou 12 et 3 divise n

sinon, $r_{k,n} = r_{k',n'}$ avec $\frac{k}{n} = \frac{k'}{n'}$ et k' et n' premiers entre eux et $n' \geq 3$ et donc

$n' = 3$ ou 6 ou 12, et comme n' divise n, 3 divise n

réciproquement on a vu plus haut que si 3 divise n alors $r_{k,n} = 1$.

Les deux autres cas ($r_{k,n} = \frac{1}{2} \Leftrightarrow 4$ divise n, $r_{k,n} = \frac{1}{3} \Leftrightarrow 6$ divise n) se traitent de la même manière.

5)

Les seules fonctions homographiques $f(X) = \frac{aX+b}{cX+d}$ avec $ad - bc \neq 0$

et appartenant à $\mathbb{Q}(X)$ et qui sont d'ordre n (fini) ≥ 2 sont d'ordre 2 ou 3 ou 4 ou 6.

preuve :

pour $n \geq 7, f(X) = \frac{aX+b}{cX+d}$ avec $\delta = ad - bc \neq 0$ et appartenant à $\mathbb{Q}(X)$ ne peut être d'ordre n, car sinon, d'après le 1.1) du II de cette annexe on aurait $s \neq 0$ et $u_n = 0$, cad $\frac{\delta}{s^2}$, (qui est un rationnel, a, b, c, d étant dans $\mathbb{Q}$) serait racine de R_n, donc $\frac{\delta}{s^2} = 1$ ou $\frac{1}{2}$ ou $\frac{1}{3}$:

soit $\frac{\delta}{s^2} = 1$ et alors $R_3(\frac{\delta}{s^2}) = 0$, cad $u_3 = 0$, soit $A^3 = v_3 I$ et $f^{(3)} = id$ et f est d'ordre ≤ 3, donc contradiction

soit $\frac{\delta}{s^2} = \frac{1}{2}$ et alors $R_4(\frac{\delta}{s^2}) = 0$, cad $u_4 = 0$, soit $A^4 = v_4 I$ et $f^{(4)} = id$ et f est d'ordre ≤ 4, donc contradiction

soit $\frac{\delta}{s^2} = \frac{1}{3}$ et alors $R_6(\frac{\delta}{s^2}) = 0$, cad $u_6 = 0$, soit $A^6 = v_6 I$ et $f^{(6)} = id$ et f est d'ordre ≤ 6, donc contradiction.

Et lors des exemples vus aux 2) 3) 4) 5) 6) du II ci-dessus, pour $n \leq 6$, c'est seulement pour $n = 2$ ou 3 ou 4 ou 6 qu'il existe $f(X) = \frac{aX+b}{cX+d}$ avec $ad - bc \neq 0$ et appartenant à $\mathbb{Q}(X)$ et d'ordre n.□

Annexe 2

Sur quelques familles de polynômes dont le groupe de Galois sur $\mathbb{Q}$ est cylique.

(il y a les deux exemples donnés pour illustrer le 2)PP)

1) Une famille de polyômes ayant tous C_3 comme groupe de Galois sur $\mathbb{Q}$.

On part de $f(X) = -\frac{X+3}{X+2}$ qui est d'ordre 3 (voir annexe 1 la formule générale des $f(X) = \frac{aX+b}{cX+d}$ avec $ad - bc \neq 0$ d'ordre 3) :

$f^{(2)}(X) = \frac{-2X-3}{X+1}$ et $f^{(3)}(X) = X$.

$X + f(X) + f^{(2)}(X) = X - \frac{X+3}{X+2} + \frac{-2X-3}{X+1} = \frac{X^3-9X-9}{X^2+3X+2} = \frac{N(X)}{D(X)}$

avec $N(X) = X^3 - 9X - 9$, $D(X) = X^2 + 3X + 2 = (X+2)(X+1)$.

Donc d'après le résultat 2.5) du 2)PP de la partie principale,

pour tout μ rationnel $P_\mu(X) = N(X) + \mu D(X) = X^3 + \mu X^2 + (3\mu - 9)X + 2\mu - 9$ pour racine $r, f(r), f^{(2)}(r)$, une racine étant dans $]-\infty;-2[$, une autre dans $]-2;-1[$ et l'autre dans $]-1;+\infty[$, et si P_μ est irréductible sur $\mathbb{Q}$ son groupe de Galois est C_3.

On peut vérifier, si on est courageux, par un calcul direct que $P_\mu(f(X)) = -\frac{P_\mu(X)}{(X+2)^3}$,

cela que P_μ soit irréductible ou non :

$(-\frac{X+3}{X+2})^3 - 9(-\frac{X+3}{X+2}) - 9 + \mu((-\frac{X+3}{X+2})^2 + 3(-\frac{X+3}{X+2}) + 2) = -\frac{1}{(X+2)^3}(2\mu - 9X + 3X\mu + X^2$

Ou alors on utilise le fait que $P_\mu(f(X)) = \frac{D(f(X))}{D(X)} P_\mu(X)$, voir le 2.5) du 2)PP, et

$$\frac{D(f(X))}{D(X)} = \frac{(-\frac{X+3}{X+2})^2 + 3(-\frac{X+3}{X+2}) + 2}{X^2+3X+2} = \frac{(X+3)^2 - 3(X+3)(X+2) + 2(X+2)^2}{(X+2)^2(X+2)(X+1)} = -\frac{1}{(X+2)^3}$$

Calcul des s_k :

par définition de N et D, $s_1(X) = X + f(X) + f^{(2)}(X) = \frac{N(X)}{D(X)}$ et comme on a pris $P_\mu = N + \mu D$, évidemment $s_1(X) = \frac{P_0(X)}{D(X)}$; $\mu = 0$ annule le coefficient de X^{3-1} de P_μ.

Déterminons les s_k suivants en utilisant le 2.7.1) du 2)PP :

$s_2 = \alpha_2 \frac{P_{\beta_2}}{D}$

β_2 est la seule valeur de μ qui annule le coefficient de X^{3-2} de P_μ : c'est 3.

$\alpha_2 = (-1)^{2+1} \times$coefficient de X^{3-2} dans $D = -3$

ou $s_2(0) = 0 + 0 + f(0)f^{(2)}(0) = \frac{9}{2}$ et $\frac{P_3(0)}{D(0)} = \frac{-3}{2}$ et donc $\alpha_2 = -3$,

finalement $s_2(X) = \frac{-3P_3(X)}{D(X)} = -3(s_1(X) + 3)$.

$s_3 = \alpha_3 \frac{P_{\beta_3}}{D}$

β_3 est la seule valeur de μ qui annule le coefficient de X^{3-3} de P_μ : c'est $\frac{9}{2}$.

$\alpha_3 = (-1)^{3+1} \times$coefficient de X^{3-3} dans $D = 2$

ou $s_3(0)$ et $P_{\frac{9}{2}}(0)$, étant nuls, pour trouver α_3 on utilise $s_3(1) = 1 \times f(1)f^{(2)}(1) = \frac{10}{3}$ et $\frac{P_{\frac{9}{2}}(1)}{D(1)} = \frac{10}{6}$ donc $\alpha_3 = 2$;

ou $\alpha_3 = \lim_{\infty} \frac{s_3(X)}{X}$ (car P_{β_3} et XD sont unitaires et de même degré ; et dans s_3 on ne garde que les produits où il y a le facteur $f^{(0)}(X) = X$, car les autres facteurs, divisés par X ont une limite nulle) et ainsi

$\alpha_3 = \lim_{+\infty} \sum_{1 \le i_1 < i_2 \le 2} f^{(i_1)}(X)f^{(i_2)}(X) = \lim_{+\infty} f^{(1)}(X)f^{(2)}(X) = 1 \times -1 \times -2 = 2,$

finalement $s_3(X) = \frac{2P_{\frac{9}{2}}(X)}{D(X)} = 2(s_1(X) + \frac{9}{2})$.

2) Une famille de polyômes ayant tous C_4 comme groupe de Galois sur $\mathbb{Q}$.

On part de $f_m(X) = m\frac{2X-m}{2X}$, laquelle est, pour tout $m \in \mathbb{Q}^*$ d'ordre 4 (voir annexe 1 la formule générale des $f(X) = \frac{aX+b}{cX+d}$ avec $ad - bc \neq 0$ d'ordre 4) :

$f_m^{(2)}(X) = m\frac{X-m}{2X-m}, f_m^{(3)}(X) = \frac{m^2}{2(m-X)}, f_m^{(4)}(X) = X$

$X + f_m(X) + f_m^{(2)}(X) + f_m^{(3)}(X) = \frac{2X^2+2mX-m^2}{2X} + \frac{(2X-m)m^2 - 2m(X-m)^2}{2(2X-m)(m-X)}$

$= \frac{(4X^4 - 12X^2m^2 + 8Xm^3 - m^4)}{2X(2X^2 - 3Xm + m^2)}$

=.....

$= \frac{-4X^4 + 12m^2X^2 - 8m^3X + m^4}{2X(2X-m)(m-X)} = \frac{X^4 - 3m^2X^2 + 2m^3X - \frac{m^4}{4}}{X(X-m)(X-\frac{m}{2})} = \frac{N(X)}{D(X)}$

avec $N(X) = X^4 - 3m^2X^2 + 2m^3X - \frac{m^4}{4}$ et $D(X) = X(X-m)(X-\frac{m}{2}) = X^3 - 3\frac{m}{2}X^2 + \frac{m^2}{2}X$

Donc d'après le 2.5) du 2)PP,

pour tout μ rationnel

$\underline{P_{\mu,m}(X)} = N(X) + \mu D(X) = X^4 + \mu X^3 - 3(m^2 + \mu\frac{m}{2})X^2 + (2m^3 + \mu\frac{m^2}{2})X - \frac{m^4}{4}$ a pour racine $r, f(r), f^{(2)}(r), f^{(3)}(r)$ et si $P_{\mu,m}$ est <u>irréductible</u> sur $\mathbb{Q}$, <u>son groupe de Galois est C_4</u>.

$\frac{D(f_m(X))}{D(X)} = \frac{(m\frac{2X-m}{2X})^3 - 3\frac{m}{2}(m\frac{2X-m}{2X})^2 + \frac{m^2}{2}(m\frac{2X-m}{2X})}{X^3 - 3\frac{m}{2}X^2 + \frac{m^2}{2}X} = -\frac{m^4}{4X^4}$ (rappel : dans le 2.5) du 2)PP, on a montré que $\frac{D(f_m(X))}{D(X)} = \frac{N(f_m(X))}{N(X)}$).

<u>Calcul des s_k</u> : .

Par définition, $s_1(X) = X + f_m(X) + f_m^{(2)}(X) + f_m^{(3)}(X) = \frac{N(X)}{D(X)} = \frac{P_{0,m}(X)}{D(X)}$; $\mu = 0$ annule le coefficient de X^{4-1} de P_μ.

Déterminons les suivants en utilisant le 2.7.1) du 2)PP :

$s_2 = \sum_{0\le i<j\le 3} f_m^{(i)} f_m^{(j)} = \alpha_2 \frac{P_{\beta_2},m}{D}$

β_2 est la seule valeur qui annule le coefficient de X^{4-2} : c'est $-2m$

$\alpha_2 = (-1)^{2+1} \times$coefficient de X^{4-2} dans $D = \frac{3m}{2}$

ou $\alpha_2 = \lim_\infty \frac{s_2(X)}{X} = \lim_{+\infty}(f^{(1)}(X) + f^{(2)}(X) + f^{(3)}(X)) = (m + \frac{m}{2} + 0) = \frac{3m}{2}$,

finalement $s_2(X) = \frac{3m}{2}\frac{P_{-2m,m}(X)}{D(X)} = \frac{3m}{2}(s_1(X) - 2m)$

$s_3(X) = \sum_{0\le i<j\le 3} f_m^{(i)}(X) f_m^{(j)}(X) f_m^{(k)}(X) = \alpha_3 \frac{P_{\beta_3,m}}{D}$

β_3 est la seule valeur qui annule le coefficient de X^{4-3} : c'est $-4m$

$\alpha_3 = (-1)^{3+1} \times$coefficient de X^{4-3} dans $D = \frac{m^2}{2}$

ou

$\alpha_3 = \lim_\infty \frac{s_3(X)}{X} = \lim_{+\infty}(f^{(1)}(X)f^{(2)}(X) + f^{(1)}(X)f^{(3)}(X) + f^{(2)}(X)f^{(3)}(X)) = (\frac{m^2}{2} + 0 + 0) = \frac{m^2}{2}$,

finalement $s_3(X) = \frac{m^2}{2}\frac{P_{-4m,m}(X)}{D(X)} = \frac{m^2}{2}(s_1(X) - 4m)$.

$s_4(X) = Xf_m^{(1)}(X)f_m^{(2)}(X)f_m^{(3)}(X)$ ne peut pas s'obtenir à partir du 2.7.1) du 2)PP car le terme constant de P_μ est $\frac{-m^4}{4}$, constante non nulle ; mais le 2.7.2) du 2)PP donne tout de suite $s_4(X) = \frac{-m^4}{4}$, ce qu'un calcul direct (évident) confirme.

3) Une autre famille de polyômes ayant tous C_4 comme groupe de Galois sur $\mathbb{Q}$.

On prend $f(X) = \frac{mX + m^2}{-5X + 3m}$ avec $m \neq 0$ qui est d'ordre 4 car on a bien $s = a + d = 4m \neq 0$ et $2bc = -(a^2 + d^2)$.

$f^{(2)}(X) = \frac{mX - m^2}{mX - m}$

$f^{(3)}(X) = \frac{3mX - m^2}{5X + m}$.

Les racines de V_i sont $\frac{3m}{5}$ et $\pm\frac{m}{5}$.

On peut vérifier que $f^{(2)}$ est bien d'ordre 2 et est $\neq \frac{\lambda}{X}$: en fait, ici, aucun V_i n'a pour racine 0.

En fait on a la caractérisation suivante

si $f(X) = \frac{aX + b}{cX + d}$ est d'ordre 4, pour $i = 1,2,3$, $V_i(0) \neq 0 \Leftrightarrow a \neq 0, d \neq 0, a \neq d$:

en effet, en posant $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, rappelons que $A^2 = sA - \delta I, A^3 = (s^2 - \delta)A - \delta sI$ et

que f étant d'ordre 4, $s \neq 0$ et $2bc = -(a^2 + d^2)$:

$V_1(0) = 0 \Leftrightarrow d = 0$

$V_2(0) = 0 \Leftrightarrow A^2 = \begin{pmatrix} \times & \times \\ \times & 0 \end{pmatrix} \Leftrightarrow (a + d)d - \delta = 0$

$\Leftrightarrow d^2 = -bc \Leftrightarrow d^2 = \frac{a^2 + d^2}{2} \Leftrightarrow a = d$

$V_3(0) = 0 \Leftrightarrow A^3 = \begin{pmatrix} \times & \times \\ \times & 0 \end{pmatrix} \Leftrightarrow (s^2-\delta)d - \delta s = 0 \Leftrightarrow bc(a+2d) = -d^3$

$\Leftrightarrow (a^2+d^2)(a+2d) = 2d^3 \Leftrightarrow a(a+d)^2 = 0 \Leftrightarrow a = 0.$

On calcule

$s_1(X) = X + f(X) + f^{(2)}(X) + f^{(3)}(X) = \frac{N(X)}{D(X)}$ avec

$N(X) = X^4 - \frac{6}{5}m^2X^2 + \frac{8}{25}m^3X + \frac{m^4}{125}$ et $D(X) = X^3 - \frac{3}{5}mX^2 - \frac{1}{25}m^2X + \frac{3m^3}{125}$.

$D_b(X) = \prod V_i = (-5X+3m)(5X-m)(5X+m) = -125D(X).$

$P_\mu(X) = N(X) + \mu D(X) = X^4 + \mu X^3 - (\frac{6m^2+3\mu m}{5})X^2 + (\frac{8m^3-\mu m^2}{25})X + \frac{m^4+3\mu m^3}{125}.$

Par rapport à l'exemple 2, le terme constant de P_μ dépend de μ.

Ce terme constant est donc nul pour $\mu = \frac{-m}{3}$ et le cas particulier du 2.7.1) du 2)PP nous dit que $P_{\frac{-m}{3}}(X) = \tau X U_1(X)U_2(X)U_3(X)$ où τ est une constante qui est ici $\frac{1}{3m^3}$ (l'inverse du produit des coefficients de tête des U_i).

On peut vérifier le 2.5) du 2)PP :

les racines des V_i ordonnées de façon croissante (on suppose $m > 0$) sont $\frac{-m}{5}, \frac{m}{5}, \frac{3m}{5}$ et les racines de $P_{\frac{-m}{3}}$ sont $-m, 0, \frac{m}{3}, m$ et

et $-m \in]-\infty; \frac{-m}{5}[$, $0 \in]-\frac{m}{5}; \frac{m}{5}[$, $\frac{m}{3} \in]\frac{m}{5}; \frac{3m}{5}[$, $m \in]\frac{3m}{5}; +\infty[$

4) Une autre famille de polyômes ayant tous C_4 comme groupe de Galois sur $\mathbb{Q}$.

On prend $f(X) = \frac{X+1}{-X+1}$ qui est d'ordre 4 car $s = 2 \neq 0$ et $2bc = -(a^2+d^2)$.

$f^{(2)}(X) = \frac{-1}{X}$ (de la forme $\frac{\lambda}{X}$ car $a = d$ voir 1.2)), $f^{(3)}(X) = \frac{-1}{f(X)} = \frac{X-1}{X+1}$;

$s_1(X) = X + f(X) + f^{(2)}(X) + f^{(3)}(X) = \frac{N(X)}{D(X)}$

avec $N(X) = X^4 - 6X^2 + 1 = (X^2-2X-1)(X^2+2X+1)$ et $D(X) = X^3 - X$.

$P_\mu(X) = X^4 + \mu X^3 - 6X^2 - \mu X + 1.$

L'application du 2.7.1) du 2)PP donne $s_3(X) = \alpha_3 \frac{P_3(X)}{D(X)} = -1 \times \frac{P_0(X)}{D(X)} = -s_1(X).$

On peut le vérifier facilement ici car

$s_3(X) = Xf(X)(f^{(2)}(X) + f^{(3)}(X)) + (X + f(X))f^{(2)}(X)f^{(3)}(X)$

$s_3(X) = X\frac{X+1}{-X+1}(-\frac{1}{X} + \frac{X-1}{X+1}) + (X + \frac{X+1}{-X+1}) \times \frac{-(X-1)}{X(X+1)}$

$s_3(X) = \frac{X^2-2X-1}{-X+1} + \frac{-X^2+2X+1}{X(X+1)} = (-X^2+2X+1)(\frac{1}{X-1} + \frac{1}{X(X+1)})$

$s_3(X) = \frac{-(X^2-2X-1)(X^2+2X+1)}{X(X^2-1)} = -s_1(X).$

Pour s_2, le coefficient de X^{4-2} étant -6, constant, le 2.7.2) du 2)PP donne $s_2(X) = -6$.

On le vérifie aussi facilement car

$s_2(X) = X(f(X) + f^{(2)}(X) + f^{(3)}(X)) + f(X)f^{(2)}(X) + f(X)f^{(3)}(X) + f^{(2)}(X)f^{(3)}(X)$

$s_2(X) = X(\frac{X^4-6X^2+1}{X^3-X} - X) + \frac{X+1}{X(X-1)} - 1 - \frac{X-1}{X(X+1)}$

$s_3(X) = \frac{X(-5X^2+1)}{X^3-X} + \frac{1}{X} + \frac{4X}{X^2-1} - 1 = \frac{-5X^3+X+4X-X^3+X}{X^3-X} = -6.$

5) Une autre famille de polyômes ayant tous C_6 comme groupe de Galois sur $\mathbb{Q}$.

On prend $f(X) = \frac{3mX+m^2}{-3X+3m}$ avec $m \neq 0$ qui est d'ordre 6 car on a bien $s = a + d = 6m \neq 0$ et $3bc = -(a^2 + d^2 - ad)$.

$f^{(2)}(X) = \frac{mX+m^2}{-3X+m}$

$f^{(3)}(X) = \frac{m^2}{-3X}$, d'ordre 2 (de la forme $\frac{\lambda}{X}$ car $a = d$ voir 1.2) de l'annexe 1)

$f^{(4)}(X) = \frac{mX-m^2}{3X+m} = \frac{-m^2}{3} \times \frac{1}{f(X)}$, d'après $f^{(3)}$

$f^{(5)}(X) = \frac{3mX-m^2}{3X+3m} = \frac{-m^2}{3} \times \frac{1}{f^{(2)}(X)}$, d'après $f^{(3)}$

Les V_i ont pour racines $0, \pm m, \pm\frac{m}{3}$.

$s_1(X) = X + f(X) + \ldots + f^{(5)}(X) = \frac{N(X)}{D(X)}$ avec

$N(X) = X^6 - 5m^2X^4 + \frac{5}{3}m^4X^2 - \frac{1}{27}m^6$ et $D(X) = X^5 - \frac{10}{9}m^2X^3 + \frac{1}{9}m^4X.$

On notera qu'ici, comme à l'exemple 4 où $f^{(\frac{n}{2})}(X) = \frac{\lambda}{X}$, N est pair,D impair.

$P_\mu(X) = X^6 + \mu X^5 - 5m^2X^4 - \frac{10}{9}\mu m^2X^3 + \frac{5}{3}m^4X^2 + \frac{1}{9}\mu m^4X - \frac{1}{27}m^6.$

Calcul des s_k par application des 2.7.1) et 2.7.2) du 2)PP :

$s_2 = (-1)^2(-5m^2) = -5m^2$, le coefficient de X^{6-2} dans P_μ étant indépendant de μ

$s_3 = \alpha_3 \frac{P_{\beta_3,m}(X)}{D(X)}$

β_3 est la seule valeur de μ qui annule le coefficient de X^{6-3} de $P_{\mu,m}$: c'est 0.

$\alpha_3 = (-1)^{3+1} \times$coefficient de X^{6-3} dans $D = -\frac{10}{9}m^2$

finalement $s_3(X) = -\frac{10}{9}m^2\frac{P_{0,m}(X)}{D(X)} = -\frac{10}{9}m^2 s_1(X).$

$s_4 = (-1)^4(\frac{5}{3}m^4) = \frac{5}{3}m^4$, le coefficient de X^{6-4} dans P_μ étant indépendant de μ

$s_5 = \alpha_5 \frac{P_{\beta_5,m}(X)}{D(X)}$

β_5 est la seule valeur de μ qui annule le coefficient de X^{6-5} de $P_{\mu,m}$: c'est 0.

$\alpha_5 = (-1)^{5+1} \times$coefficient de X^{6-5} dans $D = \frac{1}{9}m^4$

ou $s_5(X) = s_6(X)(\frac{1}{X} + \frac{1}{f(X)} + \frac{1}{f^{(2)}(X)} + \frac{1}{f^{(3)}(X)} + \frac{1}{f^{(4)}(X)} + \frac{1}{f^{(5)}(X)})$

et comme pour $i \neq 3$, $\lim_\infty f^{(i)}(X)$ est finie non nulle et $\frac{1}{f^{(3)}(X)} = \frac{-3X}{m^2}$,

$\alpha_5 = \lim_\infty \frac{s_5(X)}{X} = \lim_\infty -\frac{1}{27}m^6(\frac{1}{Xf^{(3)}(X)}) = -\frac{1}{27}m^6 \times \frac{-3}{m^2} = \frac{1}{9}m^4$

finalement $s_5(X) = \frac{1}{9}m^4\frac{P_{0,m}(X)}{D(X)} = \frac{1}{9}m^4 s_1(X).$

$s_6 = (-1)^6(-\frac{1}{27}m^6) = -\frac{1}{27}m^6$, le coefficient de X^{6-6} dans P_μ étant indépendant de μ

On peut aussi vérifier le 1.2) de l'annexe 1 et le 2.8) du 2)PP :

$f^{(\frac{n}{2})}(X) = \frac{\lambda}{X}$ avec $\lambda = \frac{-m^2}{3}$ car $a = b = 3m$ et $P_{\mu,m}(0) = N(0) = \lambda^{\frac{6}{2}} = -\frac{1}{27}m^6$.

Remarque (souvenir) : j'ai voulu vérifier la valeur de s_2 en utilisant mon logiciel de calcul formel, et j'ai commencé par lui faire simplifier $A = f(f + f^{(2)} + f^{(3)} + f^{(4)})$.
A s'écrit $\frac{3mX + m^2}{-3X + 3m}(\frac{mX + m^2}{-3X + m} + \frac{m^2}{-3X} + \frac{3mX - m^2}{3X + 3m}) - \frac{m^2}{3}$.
A la main, j'ai trouvé $A = \frac{m^2}{3} \times \frac{-27X^4 + 42mX^3 + 36m^2X^2 - 2m^3X - m^4}{3X(3X - m)(X^2 - m^2)}$:

le lecteur peut vérifier que la limite en l'infini est bien la même des deux côtés, à savoir $-m^2$

et que la valeur en $X = 2$ et $m = 1$ est bien la même des deux côtés, à savoir $\frac{43}{270}$

Par contre mon logiciel m'a donné pour A une fraction rationnelle dont la limite en l'infini n'était pas $-m^2$! J'ai eu beau vérifier, revérifier ce que j'ai tapé, le taper dans un autre ordre, j'obtenais toujours le même résultat faux (que de temps perdu...).
Par contre en lui faisant calculer $F(X) = X(f + f^{(2)} + f^{(3)} + f^{(4)} + f^{(5)})(X)$, puis $f(X)(\frac{F(X)}{X} - f(X))$, il m'a donné la valeur ci-dessus pour A! Mystère...

6) Une autre famille de polyômes ayant tous C_6 comme groupe de Galois.

On prend $f(X) = \frac{mX + m^2}{-X + 2m}$ avec $m \neq 0$ qui est d'ordre 6 car on a bien $s = a + d = 3m \neq 0$ et $3bc = -(a^2 + d^2 - ad)$.
Mais ici, $a \neq d$, et donc $f^{(3)}(X)$ ne sera pas de la forme $\frac{\lambda}{X}$ car $a \neq d$, voir 1.2) de l'annexe 1.
$f^{(2)}(X) = \frac{m^2}{-X + m}$
$f^{(3)}(X) = \frac{-mX + 2m^2}{-2X + m}$, d'ordre 2
$f^{(4)}(X) = \frac{mX - m^2}{X}$
$f^{(5)}(X) = \frac{2mX - m^2}{X + m}$
Les V_i ont pour racines $0, \pm m, \frac{m}{2}, 2m$.
On peut vérifier le 2.3.5) du 2)PP puisque $f^{(4)}(X) = \frac{U_4}{\xi X}$ avec $\xi = 1$ et on doit donc avoir $V_i = c_i U_{i-4} = c_i U_{i+2}$:
$V_1 = \frac{1}{m}U_3, V_2 = \frac{-1}{m}U_4, V_3 = \frac{-1}{m}U_5, V_4(X) = X = U_0(X), V_5 = \frac{1}{m}U_1$.
$s_1(X) = \frac{N(X)}{D(X)}$ avec $N(X) = X^6 - 15m^2X^4 + 20m^3X^3 - 6m^5X + m^6$ et
$D(X) = X^5 - \frac{5m}{2}X^4 + \frac{5m^3}{2}X^2 - m^4X$
$P_{\mu,m}(X) = X^6 + \mu X^5 - (15m^2 + \frac{5m}{2}\mu)X^4 + 20m^3X^3 + \frac{5m^3}{2}\mu X^2 - (6m^5 + m^4\mu)X + m^6$.