

Sur les polynômes dont l'ensemble des racines est globalement conservé par la transformation $x \mapsto x^2 - 2$.

0) Introduction

On qualifiera de R -stable un polynôme à coefficients dans \mathbb{C} dont l'ensemble des racines est globalement conservé par l'application $Rx \mapsto x^2 - 2$.

Une première famille de tels polynômes sera la famille des polynômes minimaux Ψ_n de $\xi + \frac{1}{\xi}$ où ξ est une racine n -ième de 1 primitive, avec n impair.

Une caractérisation des polynômes R -stables sera donnée.

Ensuite on étudiera en détail la suite (S) de polynômes définie par la relation $S_{n+1}(X) = S_n(X) + 2T_{n+1}(\frac{1}{2}X)$ pour $n \geq 1$ avec $S_1(X) = X + 1$, les T_n étant les polynômes de Tchebychev de 1ère espèce (voir au 7.1 une liste de ces polynômes pour $n \leq 9$).

En particulier,

ils sont aussi R -stables

une formule explicite simple des coefficients de S_n est donnée

la relation $S_n(X + \frac{1}{X}) = \frac{Y^{2n+1} - 1}{(Y - 1)Y^n}$ donne les racines de S_n

cette famille de polynômes S_n contient tous les Ψ_n avec n premier impair

la décomposition en facteurs irréductibles dans $\mathbb{Q}[X]$ de S_n est donnée.

Un dernier chapitre sera consacré au groupe de Galois de certains polynômes Ψ_n .

En outre, en annexes, on verra deux exercices particuliers pouvant être traités sans lire cette page sur la R -stabilité :

un exercice a pour but de factoriser et trouver les racines de $X^8 - 8X^6 + 20X^4 - 16X^2 - X + 2$, polynôme qui n'est autre que $\Psi_1(X)\Psi_3(X)\Psi_7(X)\Psi_9(X) = R(R(R(X))) - X$.

l'autre exercice est sur la famille de polynômes $P_a(X) = X^3 - aX^2 - (a + 3)X - 1$ ($P_{-1} = \Psi_7$) : tous ces polynômes sont F -stables pour $F(X) = \frac{-1}{1 + X}$.

1) Sur polynômes irréductibles de $\mathbb{Q}[X]$ avec une relation rationnelle entre deux racines

Ce paragraphe peut être sauté en première lecture.

Soit $P \in \mathbb{Q}[X]$, irréductible de degré $d \geq 2$ (donc ses d racines dans C sont distinctes) et tel que deux de ses racines x_1 et x_2 vérifient $x_2 = F(x_1)$ avec F fonction rationnelle ($F \in F(X)$).

On notera $F^{(1)} = F, F^{(2)} = F \circ F, F^{(3)} = F \circ F \circ F$, etc.

On a alors les trois résultats suivants :

a) pour toute racine r de P , $F(r)$ est racine de P

b) il existe deux entiers naturels $n \geq 2$ et $m \geq 1$ tels que $d = nm$, les racines de P se partitionnant en m sous-ensembles de la forme $\{r, F(r), F^{(2)}(r), \dots, F^{(n-1)}(r)\}$ avec $F^{(n)}(r) = r$.

Cad, l'ensemble des racines de P est globalement invariant par F , F induisant une permutation des racines de P qui est un produit de m cycles à supports disjoints et tous de même longueur n .

c) si d est un nombre premier, le b) devient :

l'ensemble des racines de P est $\{r; F(r), F^{(2)}(r), \dots, F^{(d-1)}(r)\}$ avec $F^{(d)}(r) = r$, F induisant sur l'ensemble des racines de P une permutation se réduisant à un d -cycle.

On verra à P12.4 de la ref 1 la preuve de ces trois résultats.

d) du c) ci-dessus (où $d = d^\circ P$ est premier) on déduit facilement que le groupe de Galois (sur \mathbb{Q}) de P est cyclique d'ordre d , donc commutatif, donc résoluble et ainsi P est résoluble.

En effet, l'ordre du groupe de Galois de P est le degré de l'extension $[N : \mathbb{Q}]$ où N est le corps de décomposition de P .

Par définition N est le plus petit corps contenant \mathbb{Q} et les racines de P , c'est donc $\mathbb{Q}(r)$ puisque les autres racines s'obtiennent rationnellement à partir de r .

Donc $[N : \mathbb{Q}] = [\mathbb{Q}(r) : \mathbb{Q}] = d$ car P est irréductible (donc r est algébrique sur \mathbb{Q} de degré d), et ainsi le groupe de Galois de P est d'ordre d qui est un nombre premier, donc ce groupe de Galois est cyclique d'ordre d , donc commutatif, donc résoluble et ainsi P est résoluble.

On pourra voir au P12.5 de la ref 1 la preuve que le groupe de Galois de P est encore cyclique d'ordre d , sans supposer d premier, mais en supposant que les d racines de P forment l'ensemble $\{r; F(r), F^{(2)}(r), \dots, F^{(d-1)}(r)\}$.

Dans cette page où on considère surtout que le cas particulier $F(X) = R(X) = X^2 - 2$ (en annexe 2 on verra brièvement le cas $F(X) = \frac{-1}{1+X}$), je ferai des démonstrations ne faisant pas appel aux résultats a,b,c \square .

2) Analogie entre les polynômes $R^{(n)}$ et les polynômes T_n de Tchebychev

Rappelons d'abord quelques résultats sur les polynômes de Tchebychev de 1^{ère} espèce T_n (ces résultats, et d'autres, se trouvent dans tout ouvrage sur les polynômes orthogonaux) :

on sait que pour tout réel θ , $\cos(3\theta) = 4\cos^3\theta - 3\cos\theta$, d'où l'idée de considérer les polynômes $P \in \mathbb{R}[X]$ de degré n vérifiant la relation $P(\cos(\theta)) = \cos(n\theta)$ pour tout réel θ . Pour $n = 3$, $P(X) = 4X^3 - 3X$ est le seul qui convient.

En fait, pour tout $n \geq 0$, il existe un seul polynôme $P \in \mathbb{R}[X]$ de degré n vérifiant la relation $P(\cos(\theta)) = \cos(n\theta)$ pour tout réel θ : on le note T_n .

On a alors :

$$T_0 = 1, T_1(X) = X \text{ et pour tout } n \geq 1, T_{n+1} = 2XT_n(X) - 2T_{n-1}.$$

pour tout $n \geq 0$, T_n est de degré n , il a la parité de n , et si $n \neq 0$, son coefficient de tête est 2^{n-1} .

$$\text{pour tout } n \geq 0, T_n(1) = 1$$

$$\text{pour tout } n \geq 1, T_n(X) = 2^{n-1}X^n + \frac{n}{2} \sum_{k=1}^{E(\frac{n}{2})} (-1)^k \frac{C_{n-k-1}^{k-1}}{k} (2X)^{n-2k}$$

$$\text{pour tous } n \geq 0, m \geq 0, T_m(T_n(X)) = T_{nm}(X)$$

$$\text{par exemple } T_3 \circ T_2 = T_2 \circ T_3 = T_6 \text{ et en faisant } m = 0, T_n(1) = T_0(X) = 1$$

$$\text{conséquence : si on pose } Z_n(X) = 2T_n(\frac{1}{2}X) \text{ on a aussi } Z_n \circ Z_m = Z_{nm}$$

$$\text{pour tout } n \geq 0, X^n + \frac{1}{X^n} = 2T_n(\frac{1}{2}(X + \frac{1}{X})) : \text{cette relation montre évidemment que}$$

$X^n + \frac{1}{X^n}$ est un polynôme en $X + \frac{1}{X}$ et c'est en cherchant ce polynôme que j'ai été amené à considérer les polynômes S_n

Note : on verra au 7.1 une liste des premiers polynômes T_n .

Revenons à R et notons $R^{(1)} = R, R^{(2)} = R \circ R, R^{(3)} = R \circ R \circ R$, etc.

Pour tout entier $n \geq 1$, une récurrence évidente montre que $R^{(n)}(X + \frac{1}{X}) = X^{2^n} + \frac{1}{X^{2^n}}$,

relation qui rappelle le dernier résultat ci-dessus pour T_n et on a donc $R^{(n)}(X + \frac{1}{X}) = 2T_{2^n}(\frac{1}{2}(X + \frac{1}{X}))$.

On en déduit $R^{(n)}(X + \frac{1}{X}) = X + \frac{1}{X} \Leftrightarrow T_{2^n}(\frac{1}{2}(X + \frac{1}{X})) = \frac{1}{2}(X + \frac{1}{X})$.

Et puisque $T_n(\cos(\theta)) = \cos(n\theta)$, qu'en est-il de $R^{(n)}(\cos \theta)$?

$R^{(n)}(\cos \theta) = R^{(n)}(e^{i\theta} + \frac{1}{e^{i\theta}}) = e^{i2^n\theta} + \frac{1}{e^{i2^n\theta}}$ et ainsi pour tout

$n \geq 1$, $R^{(n)}(\cos \theta) = 2 \cos(2^n \theta)$.

En particulier $R(\cos \theta) = 2 \cos(2\theta)$, alors que $T_2(\cos \theta) = \cos(2\theta)$.

Malgré ces analogies, on verra au 7.2.3 que T_n n'est pas R -stable alors que $R^{(n)}(X) - X$ l'est (voir 5) \square .

3) Sur les polynômes Ψ_n

Pour $n \geq 1$, on appelle Ψ_n le polynôme minimal (sur \mathbb{Q}) de $\xi + \frac{1}{\xi}$ où ξ est une racine n -ième de 1 primitive, cad $\xi = e^{\frac{2ik\pi}{n}}$ avec k premier avec n .

3.1 On a évidemment $\Psi_1(X) = X - 2$ (car la seule racine 1-ième primitive de 1 est 1) et $\Psi_2(X) = X + 2$ (car la seule racine 2-ième primitive de 1 est -1)

3.2 Pour $n \geq 3$, $\xi + \frac{1}{\xi}$ (c'est la partie réelle de ξ) est algébrique sur \mathbb{Q} de degré $\frac{\varphi(n)}{2}$

($\varphi(n)$ = nombre d'entiers $\in \{1; 2; \dots; n\}$ premiers avec n ; $\varphi(n)$ pair pour $n \geq 3$) et son polynôme minimal (sur \mathbb{Q}) Ψ_n est défini par la relation

$\Phi_n(X) = X^{\frac{\varphi(n)}{2}} \Psi_n(X + \frac{1}{X})$ où Φ_n est le n ième polynôme cyclotomique.

Etant un polynôme minimal, Ψ_n est irréductible sur \mathbb{Q} .

Rappel : $\prod_{d|n} \Phi_d = X^n - 1$, donc si n est premier,

$\Phi_n(X) = \frac{X^n - 1}{X - 1} = X^{n-1} + X^{n-2} + \dots + X + 1$.

3.3 il y a $\varphi(n)$ racines n -ièmes de 1 primitives : les $\xi_k = e^{\frac{2ik\pi}{n}}$ avec k premier avec n et $1 \leq k < n$.

Pour $n \geq 3$, il est facile de vérifier que $\xi_k + \frac{1}{\xi_k} = 2 \cos \frac{2k\pi}{n}$ (c'est un réel) avec k premier avec n et $1 \leq k < n$ ne prend que $\frac{\varphi(n)}{2}$ valeurs distinctes : ce sont les $\frac{\varphi(n)}{2}$ racines de Ψ_n .

Ces $\frac{\varphi(n)}{2}$ racines de Ψ_n sont $2 \cos \frac{2k\pi}{n}$ avec k premier avec n et $1 \leq k < \frac{n}{2}$, et donc

si $n \geq 3$ est premier les $\frac{\varphi(n)}{2}$ racines de Ψ_n sont $2 \cos \frac{2k\pi}{n}$ avec

$$k = 1, 2, 3, \dots, \frac{\varphi(n)}{2} = \frac{n-1}{2}$$

3.4) Si $n \neq m$, Ψ_n et Ψ_m n'ont aucune racine commune.

3.5) Si $p \geq 3$ est un nombre premier, $\Psi_{2p}(X) = \Psi_p(-X)$.

Par contre $\Psi_4(X) = X \neq \Psi_2(-X) = -X + 2$

3.6) Pour $n \geq 1$, impair, $\neq 3$ on a $\Psi_n(1) = \pm 1$.

Mais $\Psi_2(1) = 3$, $\Psi_{42}(1) = 5$.

3.7) Exemples de calculs de Ψ_n

Pour les petites valeurs de n , on peut parfois déterminer Ψ_n uniquement à partir de sa définition.

$$\Psi_1(X) = X - 2$$

$$\Psi_2(X) = X + 2$$

$$\Psi_3(X) = X + 1 \text{ car } j \text{ est une racine 3-ième de 1 primitive et } j + \frac{1}{j} = -1$$

$$\Psi_4(X) = X \text{ car } i \text{ est une racine 4-ième de 1 primitive et } i + \frac{1}{i} = 0$$

$$\Psi_5(X) = X^2 + X - 1 \text{ car } X^4 + X^3 + X^2 + X + 1 = X^2 \Psi_5(X + \frac{1}{X}) \text{ or}$$

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

$$\Psi_6(X) = X - 1 \text{ car une racine 6-ième de 1 primitive est } e^{\frac{2i\pi}{6}} = e^{\frac{i\pi}{3}} \text{ et}$$

$$e^{\frac{i\pi}{3}} + \frac{1}{e^{\frac{i\pi}{3}}} = 1.$$

On pouvait aussi appliquer le 3.5).

$$\Psi_7(X) = X^3 + X^2 - 2X - 1 \text{ car } X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 = X^3 \Psi_7(X + \frac{1}{X}) \text{ or}$$

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

$$\Psi_8(X) = X^2 - 2 \text{ car une racine 8-ième de 1 primitive est } e^{\frac{2i\pi}{8}} = e^{\frac{i\pi}{4}} \text{ et}$$

$$e^{\frac{i\pi}{4}} + \frac{1}{e^{\frac{i\pi}{4}}} = \sqrt{2}$$

On aura remarqué que $\Psi_8(X) = R(X)$.

$\Psi_9(X) = X^3 - 3X + 1$: c'est moins immédiat car 9 n'est pas premier et une racine 9-ième de 1 primitive de 1 est $e^{\frac{2i\pi}{9}}$ et $e^{\frac{2i\pi}{9}} + e^{-\frac{2i\pi}{9}} = 2 \cos \frac{2i\pi}{9}$ qui ne se simplifie pas!
Les $\frac{\varphi(9)}{2} = 3$ racines de Ψ_9 sont $2 \cos \frac{2i\pi}{9}$, $2 \cos \frac{4i\pi}{9}$, $2 \cos \frac{8i\pi}{9}$ mais cela ne permet pas de conclure.

$$\text{En fait } \Phi_9(X) = \frac{X^9 - 1}{\Phi_1(X)\Phi_3(X)} = \frac{X^9 - 1}{(X-1)(X^2 + X + 1)} = X^6 + X^3 + 1 = X^{\frac{\varphi(9)}{2}} \Psi(X + \frac{1}{X}) \text{ et}$$

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

$$\Psi_{10}(X) = X^2 - X - 1 \text{ car les } \frac{\varphi(10)}{2} = 2 \text{ racines de } \Psi_{10} \text{ sont } 2 \cos(\frac{2\pi}{10}) \text{ et } 2 \cos(\frac{6\pi}{10})$$

$$\text{soient } 2 \cos(\frac{\pi}{5}) = \frac{1 + \sqrt{5}}{2} \text{ et } 2 \cos(\frac{3\pi}{5}) = \frac{1 - \sqrt{5}}{2}$$

On pouvait aussi appliquer le 3.5).

$$\Psi_{11}(X) = X^5 + X^4 - 4X^3 - 3X^2 + 3X + 1 \text{ (voir remarque ci-dessous)}$$

$\Psi_{12}(X) = X^2 - 3$ car les $\frac{\varphi(12)}{2} = 2$ racines de Ψ_{10} sont $2\cos(\frac{2\pi}{12})$ et $2\cos(\frac{10\pi}{12})$
soient $2\cos(\frac{\pi}{6}) = \sqrt{3}$ et $2\cos(\frac{5\pi}{6}) = -\sqrt{3}$

$$\Psi_{13}(X) = X^6 + X^5 - 5X^4 - 4X^3 + 6X^2 + 3X - 1 \text{ (voir remarque ci-dessous)}$$

Remarque :

$\Psi_3(X), \Psi_5(X), \Psi_7(X), \Psi_{11}(X), \Psi_{13}(X)$ sont respectivement S_1, S_2, S_3, S_5, S_6 : voir début du 7.2.

On verra aussi au 7.3.2, les coefficients de Ψ_{15} et Ψ_{21}

3.8) S'il est facile de trouver tous les Ψ_n de degré 1 (outre Ψ_1 , il n'y a que Ψ_3, Ψ_4, Ψ_6 car pour $n \geq 2$, $\varphi(n) = 2 \Leftrightarrow n = 3$ ou 4 ou 6), pour un degré $d \geq 2$ quelconque c'est plus difficile.

Par exemple, pour $d = 6$, il y a six valeurs possibles pour n : 13; 21; 26; 28; 36; 42.

Pour les coefficients de Ψ_{13} voir ci-dessus, pour Ψ_{21} voir 7.3.2.

Je donne les autres :

$$\Psi_{26}(X) = \Psi_{13}(-X) = X^6 - X^5 - 5X^4 + 4X^3 + 6X^2 - 3X - 1, \text{ d'après le 3.5}$$

$$\Psi_{28}(X) = X^6 - 7X^4 + 14X^2 - 7$$

$$\Psi_{36}(X) = X^6 - 6X^4 + 9X^2 - 3$$

$$\Psi_{42}(X) = X^6 + X^5 - 6X^4 - 6X^3 + 8X^2 + 8X - 1$$

3.9) Une "curiosité" (liée à Ψ_7) : $-\frac{1}{3} + \frac{2\sqrt{7}}{3} \cos(\frac{1}{3} \arccos \frac{1}{2\sqrt{7}}) = 2\cos \frac{2\pi}{7}$.

preuve :

3.1) évident

3.2) admis

3.3) n étant ≥ 3 , si k et k' étant premiers avec n et dans $[1; n[$,

$$\cos \frac{2k\pi}{n} = \cos \frac{2k'\pi}{n} \Leftrightarrow k = \pm k' + Kn \Leftrightarrow k + k' = Kn \text{ ou } k - k' = Kn \Leftrightarrow k + k' = n \text{ ou } k = k'.$$

Comme k premier avec n et $k \in [1; \frac{n}{2}[$ équivaut à $n - k$ premier avec n et $n - k \in]\frac{n}{2}; n[$,

il y a $\frac{\varphi(n)}{2}$ entiers $k \in [1; \frac{n}{2}[$ premiers avec n et $\frac{\varphi(n)}{2}$ entiers $k \in]\frac{n}{2}; n[$ premiers avec n .

Les $\frac{\varphi(n)}{2}$ racines de Ψ_n sont donc $2\cos \frac{2k\pi}{n}$ avec $k \in [1; \frac{n}{2}[$ premier avec n

3.4) si Ψ_n et Ψ_m , avec n et $m \geq 3$, ont une racine commune, alors il existe k premier avec n et k' premier avec m tels que $\cos \frac{2k\pi}{n} = \cos \frac{2k'\pi}{m}$, soit $mk = \pm nk' + Knm$ et donc n divise mk , mais étant premier avec k , c'est que n divise m ; de même m divise n et ainsi $n = m$.

Reste à montrer que Ψ_n pour $n \geq 3$ n'a pas de racine commune avec Ψ_1 ou Ψ_2 :

soit $r = 2\cos \frac{2k\pi}{n}$, avec k premier avec $n \geq 3$, une racine de Ψ_n

si $r = 2$, alors $k = Kn$, ce qui contredit k premier avec n , donc Ψ_n et Ψ_1 n'ont pas de racine commune

si $r = -2$, alors $2k = (2K + 1)n$ donc n divise $2k$, soit n divise 2 , ce qui est impossible et donc Ψ_n et Ψ_2 n'ont pas de racine commune.

3.5) Cf le 3.3) les racines de Ψ_p sont $2\cos \frac{2k\pi}{p}$ pour $k = 1, 2, 3, \dots, \frac{p-3}{2}, \frac{p-1}{2}$ soit

$$2 \cos \frac{2\pi}{p}, 2 \cos \frac{4\pi}{p}, 2 \cos \frac{6\pi}{p}, \dots, 2 \cos \frac{(p-3)\pi}{p}, 2 \cos \frac{(p-1)\pi}{p}.$$

Celles de Ψ_{2p} sont $2 \cos \frac{2k'\pi}{2p}$ pour $k' < \frac{2p}{2} = p$ et k' premier avec $2p$.

Donc k' doit être impair, et comme p est premier, k' prend toute valeur impaire inférieure à p , c'est-à-dire les racines de Ψ_{2p} sont

$$2 \cos \frac{k'\pi}{p} \text{ pour } k' = 1, 3, 5, \dots, p-4, p-2.$$

Mais en posant $k' = p - k''$,

ces racines de Ψ_{2p} s'écrivent $2 \cos \frac{(p-k'')\pi}{p} = -2 \cos \frac{k''\pi}{p}$ pour $k'' = p-1, p-3, \dots, 4, 2$, cad k'' décrit les valeurs prises par $2k$, et donc les racines de Ψ_{2p} sont les opposées des racines de Ψ_p , et comme ces deux polynômes sont unitaires, on a $\Psi_{2p}(X) = \Psi_p(-X)$.

3.6) Voir la preuve du 7.3.4.

3.9) Les racines de $\Psi_7(X) = X^3 + X^2 - 2X - 1$ sont $2 \cos \frac{2\pi}{7}, 2 \cos \frac{4\pi}{7}, 2 \cos \frac{6\pi}{7}$, la seule racine positive étant évidemment $2 \cos \frac{2\pi}{7}$.

Mais $\Psi_7(Y - \frac{1}{3}) = Y^3 - \frac{7}{3}Y - \frac{7}{27}$ et en appliquant Viéte (voir ref 2) pour trouver les

racines de $Y^3 - \frac{7}{3}Y - \frac{7}{27}$, on trouve que les racines de Ψ_7 sont $-\frac{1}{3} + \frac{2\sqrt{7}}{3} \cos \frac{\theta}{3}$, $-\frac{1}{3} + \frac{2\sqrt{7}}{3} \cos \frac{\theta+2\pi}{3}$, $-\frac{1}{3} + \frac{2\sqrt{7}}{3} \cos \frac{\theta+4\pi}{3}$, avec $\theta = \arccos \frac{1}{2\sqrt{7}} \in]0; \frac{\pi}{2}[$.

On peut écrire θ à l'aide d'un arctan car $\cos^2 \theta = \frac{1}{1 + \tan^2 \theta}$, soit $\frac{1}{28} = \frac{1}{1 + \tan^2 \theta}$ et ainsi $\tan^2 \theta = 27$, donc $\tan \theta = \sqrt{27}$ (puisque $\theta \in]0; \frac{\pi}{2}[$) et $\theta = \arctan \sqrt{27}$.

Comme $-\frac{1}{3} + \frac{2\sqrt{7}}{3} \cos \frac{\theta}{3} = \frac{-1}{3} + \frac{2\sqrt{7}}{3} \cos \frac{\arctan \sqrt{27}}{3} \approx 1.2470$, c'est la seule racine positive de Ψ_7 et ainsi

$$\frac{-1}{3} + \frac{2\sqrt{7}}{3} \cos \frac{\arctan(\sqrt{27})}{3} = 2 \cos \frac{2\pi}{7}.$$

Si le lecteur a une preuve de cette égalité sans passer par un troisième degré, je suis preneur...□.

4) Sur la R -stabilité des polynômes Ψ_n

4.1) Pour $n \geq 1$, Ψ_n est R -stable $\Leftrightarrow n$ est impair

(si n est pair aucune racine de Ψ_n est transformée en une racine de Ψ_n).

4.2) Pour $n \geq 3$ et impair, la permutation σ induite par R sur l'ensemble des $\frac{\varphi(n)}{2}$ racines de Ψ_n se décompose en un produit de cycles (à supports disjoints) tous de même longueur $u \geq 1$, celle longueur u étant le plus entier ≥ 1 tel que $2^u \equiv \pm 1 (n)$.

On retrouve donc le b) du théorème de Galois rappelé au 1), avec en plus la caractérisation de la longueur commune des cycles.

Cette longueur u commune à tous les cycles de la décomposition est évidemment un diviseur de $\frac{\varphi(n)}{2}$ puisque si N est le nombre de cycles de la décomposition de σ , on a

$$Nu = \frac{\varphi(n)}{2}.$$

σ se réduit à un seul cycle si et seulement si $u = \frac{\varphi(n)}{2}$.

$\Psi_3(X) = X + 1$ étant le seul cas où $u = 1$ (auquel cas σ se réduit à un point fixe), pour $n \geq 5$, si $\frac{\varphi(n)}{2} = d^\circ \Psi_n$ est premier, alors σ se réduit à un seul cycle (u ne pouvant prendre la valeur 1, $u = \frac{\varphi(n)}{2}$) et on retrouve le c) du 1).

4.3) Pour n impair tel que $3 \leq n \leq 35$, la permutation induite par R sur l'ensemble des racines de Ψ_n est toujours un $\frac{\varphi(n)}{2}$ -cycle (par exemple excepté dans les trois cas suivants :

si $n = 17$ car $2^4 \equiv -1 \pmod{17}$ et $u = 4 < \frac{\varphi(17)}{2} = 8$: dans ce cas la permutation induite par R est le produit de deux 4-cycles à supports disjoints

si $n = 31$ car $2^5 \equiv 1 \pmod{31}$ et $u = 5 < \frac{\varphi(31)}{2} = 15$: dans ce cas la permutation induite par R est le produit de trois 5-cycles à supports disjoints

si $n = 33$ car $2^5 \equiv -1 \pmod{33}$ et $u = 5 < \frac{\varphi(33)}{2} = 10$: dans ce cas la permutation induite par R est le produit de deux 5-cycles à supports disjoints.

preuve :

4.1)

Evidemment $\Psi_1(X) = X - 2$ est R -stable et pas $\Psi_2(X) = X + 2$

si $n \geq 3$ est impair :

une racine quelconque de Ψ_n est $r = \xi + \frac{1}{\xi}$ avec $\xi = e^{\frac{2ik\pi}{n}}$ où k est premier avec n ,

donc $R(r) = R(\xi + \frac{1}{\xi}) = \xi^2 + \frac{1}{\xi^2}$; mais n étant impair 2 est premier avec n , et ainsi $2k$ est

premier avec n et $\xi^2 = e^{\frac{2i(2k)\pi}{n}}$ reste une racine n -ième de 1 primitive, donc $R(r)$ est racine de Ψ_n .

Reste à vérifier que si $r = \xi + \frac{1}{\xi}$ et $r' = \xi' + \frac{1}{\xi'}$ sont deux racines distinctes de Ψ_n on a $R(r) \neq R(r')$.

En fait $R(r) = R(r') \Leftrightarrow \xi^2 + \frac{1}{\xi^2} = \xi'^2 + \frac{1}{\xi'^2} \Leftrightarrow (\xi^2 - \xi'^2)((\xi\xi')^2 - 1) = 0 \Leftrightarrow \xi = \pm\xi'$ ou

$\xi = \pm\frac{1}{\xi'}$; mais $\xi = -\xi'$ et $\xi = -\frac{1}{\xi'}$ sont impossibles puisque par élévation à la puissance n on obtiendrait $1 = -1$.

Donc $R(r) = R(r') \Leftrightarrow \xi = \xi'$ ou $\xi = \frac{1}{\xi'} \Leftrightarrow r = r'$ ce qui prouve que si r et r' sont deux racines distinctes de Ψ_n on a $R(r) \neq R(r')$.

si $n \geq 3$ est pair :

posons $n = 2p$ et montrons que pour toute racine r de Ψ_n , $\Psi_n(r)$ n'est pas racine de Ψ_n .

En effet $r = \xi + \frac{1}{\xi} = 2 \cos \frac{2k\pi}{n} = \cos \frac{k\pi}{p}$ avec k premier avec $n = 2p$ et

$R(r) = \xi^2 + \frac{1}{\xi^2} = 2 \cos \frac{2k\pi}{p}$ qui sera racine de Ψ_n si et seulement si $2 \cos \frac{2k\pi}{p} = 2 \cos \frac{k'\pi}{p}$

avec k' premier avec $2p$.

Or $\cos \frac{2k\pi}{p} = \cos \frac{k'\pi}{p} \Leftrightarrow 2k = \pm k' + 2Kp$, donc k' est pair et ne peut être premier avec $2p$.
 Donc si r est racine Ψ_n , $R(r)$ n'est pas racine de Ψ_n .

4.2)

Commençons par deux résultats simples :

a) pour $n \geq 1$, on a évidemment $\cos \frac{2k\pi}{n} = \cos \frac{2k'\pi}{n} \Leftrightarrow k \equiv \pm k' (n)$

b) pour $n \geq 3$, si r est une racine quelconque de Ψ_n , cad $r = 2 \cos \frac{2k\pi}{n}$ avec k premier avec n , alors

pour tout $i \geq 1$, on a $R^{(i)}(r) = r \Leftrightarrow 2^i \equiv \pm 1 (n)$.

En effet, d'après le 1) $R^{(i)}(r) = r \Leftrightarrow 2 \cos \frac{2^i(2k\pi)}{n} = 2 \cos \frac{2k\pi}{n} \Leftrightarrow 2^i k \equiv \pm k (n)$, cela d'après le a).

Mais n et k sont premiers entre eux et donc, $2^i k \equiv \pm k (n) \Leftrightarrow 2^i \equiv \pm 1 (n)$.

Montrons maintenant le résultat annoncé.

Soit c un cycle quelconque de la décomposition en cycles à supports disjoints de la permutation σ de l'ensemble des racines de Ψ_n induite par R .

Si $k \geq 1$ est la longueur de c , c s'écrit $(x_1 x_2 \dots x_k)$ où les x_i sont k racines distinctes de Ψ_n .

On a alors, successivement,

$x_2 = R(x_1) \neq x_1$, donc 2 n'est pas congru à $\pm 1 \pmod n$

$x_3 = R(x_2) = R(R(x_1)) \neq x_1$, donc 2^2 n'est pas congru à $\pm 1 \pmod n$

$x_4 = R(x_3) = R^{(3)}(x_1) \neq x_1$, donc 2^3 n'est pas congru à $\pm 1 \pmod n$

etc ...

$x_k = R(x_{k-1}) = R^{(k-1)}(x_1) \neq x_1$, donc 2^{k-1} n'est pas congru à $\pm 1 \pmod n$

$R(x_k) = x_1$, soit $R^{(k)}(x_1) = x_1$ et $2^k \equiv \pm 1 (n)$.

Donc k est le plus petit entier $u \geq 1$ tel que $2^u \equiv \pm 1 (n)$.

Ainsi tous les cycles de la décomposition en cycles (à supports disjoints) de σ ont donc la même longueur, à savoir le nombre u ci-dessus.

Prouvons que $u = 1 \Leftrightarrow n = 3$:

$u = 1 \Leftrightarrow 2 \equiv 1 (n)$ ou $2 \equiv -1 (n)$: le premier cas est impossible car $n \geq 3$, et le deuxième cas n'est possible que si $n = 3$.

4.3)

Il sera très utile ici de savoir que si $\theta + \theta' = 2\pi$ alors $\cos \theta = \cos \theta' \dots$

Les huit racines de Ψ_{17} sont

$2 \cos \frac{2\pi}{17}, 2 \cos \frac{4\pi}{17}, 2 \cos \frac{6\pi}{17}, 2 \cos \frac{8\pi}{17}, 2 \cos \frac{10\pi}{17}, 2 \cos \frac{12\pi}{17}, 2 \cos \frac{14\pi}{17}, 2 \cos \frac{16\pi}{17}$.

On vérifie sans peine que la permutation induite par R sur les huit racines de Ψ_{17} est le produit des deux 4-cycles suivants :

$(2 \cos \frac{2\pi}{17} \ 2 \cos \frac{4\pi}{17} \ 2 \cos \frac{8\pi}{17} \ 2 \cos \frac{16\pi}{17})$: on vérifie que

$R(2 \cos \frac{16\pi}{17}) = 2 \cos \frac{32\pi}{17} = 2 \cos \frac{2\pi}{17}$ puisque $\frac{32\pi}{17} + \frac{2\pi}{17} = 2\pi$

et

$(2 \cos \frac{10\pi}{17} \ 2 \cos \frac{14\pi}{17} \ 2 \cos \frac{6\pi}{17} \ 2 \cos \frac{12\pi}{17})$: par exemple

$R(2 \cos \frac{10\pi}{17}) = 2 \cos \frac{20\pi}{17} = 2 \cos \frac{14\pi}{17}$

Les 15 racines de Ψ_{31} sont

$$2 \cos \frac{2\pi}{31}, 2 \cos \frac{4\pi}{31}, 2 \cos \frac{6\pi}{31}, 2 \cos \frac{8\pi}{31}, 2 \cos \frac{10\pi}{31}, 2 \cos \frac{12\pi}{31}, 2 \cos \frac{14\pi}{31}, 2 \cos \frac{16\pi}{31}, 2 \cos \frac{18\pi}{31},$$

et

$$2 \cos \frac{20\pi}{31}, 2 \cos \frac{22\pi}{31}, 2 \cos \frac{24\pi}{31}, 2 \cos \frac{26\pi}{31}, 2 \cos \frac{28\pi}{31}, 2 \cos \frac{30\pi}{31}$$

La permutation induite par R est le produit des trois 5-cycles suivants

$$(2 \cos \frac{2\pi}{31} \ 2 \cos \frac{4\pi}{31} \ 2 \cos \frac{8\pi}{31} \ 2 \cos \frac{16\pi}{31} \ 2 \cos \frac{30\pi}{31})$$

et

$$(2 \cos \frac{6\pi}{31} \ 2 \cos \frac{12\pi}{31} \ 2 \cos \frac{24\pi}{31} \ 2 \cos \frac{14\pi}{31} \ 2 \cos \frac{28\pi}{31})$$

et

$$(2 \cos \frac{10\pi}{31} \ 2 \cos \frac{20\pi}{31} \ 2 \cos \frac{22\pi}{31} \ 2 \cos \frac{18\pi}{31} \ 2 \cos \frac{26\pi}{31})$$

Les dix racines de Ψ_{33} sont

$$2 \cos \frac{2\pi}{33}, 2 \cos \frac{4\pi}{33}, 2 \cos \frac{8\pi}{33}, 2 \cos \frac{10\pi}{33}, 2 \cos \frac{14\pi}{33}, 2 \cos \frac{16\pi}{33}, 2 \cos \frac{20\pi}{33}, 2 \cos \frac{26\pi}{33}, 2 \cos \frac{28\pi}{33}, 2 \cos \frac{32\pi}{33}.$$

La permutation induite par R est le produit des deux 5-cycles suivants :

$$(2 \cos \frac{2\pi}{33} \ 2 \cos \frac{4\pi}{33} \ 2 \cos \frac{8\pi}{33} \ 2 \cos \frac{16\pi}{33} \ 2 \cos \frac{32\pi}{33})$$

et

$$(2 \cos \frac{10\pi}{33} \ 2 \cos \frac{20\pi}{33} \ 2 \cos \frac{26\pi}{33} \ 2 \cos \frac{14\pi}{33} \ 2 \cos \frac{28\pi}{33}) \square.$$

5) Sur $R^{(k)}(X) - X$ où $R^{(k)} = \underbrace{R \circ R \circ \dots \circ R}_{k-1 \text{ fois } \circ}$ avec $k \geq 1$

On a les résultats suivants :

5.1) Pour tout $k \geq 1$, $R^{(k)}(X) - X$ est R -stable

5.2) Pour tout $k \geq 1$, $R^{(k)}(X) - X = \prod_{j \in D} \Psi_j(X)$ où $D = \{\text{diviseurs de } 2^k - 1\} \cup \{\text{diviseurs de } 2^k + 1\}$

Remarque :

D ne contient que des entiers impairs et contient toujours 1 et 3 (car 2 c'est -1 modulo 3, et donc modulo 3, $2^k - 1$ ou $2^k + 1$ est nul).

1 est le seul diviseur commun à $2^k - 1$ et $2^k + 1$.

D contient toujours $2^k - 1$ et $2^k + 1$.

Les facteurs irréductibles Ψ_j de la décomposition de $R^{(k)}(X) - X$ sont toujours à la puissance 1.

5.3) si k divise k' alors $R^{(k)}(X) - X$ divise $R^{(k')}(X) - X$

Exemples :

$$R(X) - X = \Psi_1(X)\Psi_3(X) = (X - 2)(X + 1) = X^2 - X - 1$$

$$R^{(2)}(X) - X = \Psi_1(X)\Psi_3(X)\Psi_5(X) = (X - 2)(X + 1)(X^2 + X - 1) = X^4 - 4X^2 - X + 2$$

$$R^{(3)}(X) - X = \Psi_1(X)\Psi_3(X)\Psi_7(X)\Psi_9(X) = X^8 - 8X^6 + 20X^4 - 16X^2 - X + 2$$

$$R^{(4)}(X) - X = \Psi_1(X)\Psi_3(X)\Psi_5(X)\Psi_{15}(X)\Psi_{17}(X)$$

$$R^{(5)}(X) - X = \Psi_1(X)\Psi_3(X)\Psi_{11}(X)\Psi_{31}(X)\Psi_{33}(X)$$

$$R^{(6)}(X) - X = \Psi_1(X)\Psi_3(X)\Psi_5(X)\Psi_7(X)\Psi_9(X)\Psi_{13}(X)\Psi_{21}(X)\Psi_{63}(X)\Psi_{65}(X)$$

$$R^{(7)}(X) - X = \Psi_1(X)\Psi_3(X)\Psi_{43}(X)\Psi_{127}(X)\Psi_{129}(X)$$

$$R^{(8)}(X) - X = \Psi_1(X)\Psi_3(X)\Psi_5(X)\Psi_{15}(X)\Psi_{17}(X)\Psi_{51}(X)\Psi_{85}(X)\Psi_{255}(X)\Psi_{257}(X)$$

preuve :

5.1) il est facile de prouver que $R^{(k)}(X) - X$ est R-stable, en effet

si r est une racine de $R^{(k)}(X) - X$, alors $R^{(k)}(r) = r$, donc $R(R^{(k)}(r)) = R(r)$, soit $R^{(k)}(R(r)) = R(r)$ et $R(r)$ est aussi racine de $R^{(k)}(X) - X$

si r et r' sont racines de $R^{(k)}(X) - X$ avec $R(r) = R(r')$, alors $R^{(k)}(r) = R^{(k)}(r')$, et comme $R^{(k)}(r) = r$ et $R^{(k)}(r') = r'$, c'est que $r = r'$, donc deux racines distinctes de $R^{(k)}(X) - X$ ont pour image par R deux racines distinctes de $R^{(k)}(X) - X$.

5.2) Montrons maintenant que $R^{(k)}(X) - X = \prod_{j \in D} \Psi_j(X)$

a) montrons qu'ils ont même degré :

celui $R^{(k)}(X) - X$ est évidemment 2^k et celui de $\prod_{j \in D} \Psi_j(X)$ est $d = \sum_{\substack{j \in D \\ j \geq 3}} \frac{\varphi(j)}{2} + d^\circ \Psi_1$, puisque

$2 \notin D$

Compte-tenu que $\sum_{d|m} \varphi(d) = m$, et en appliquant cette formule pour $m = 2^k - 1$ et

$$m = 2^k + 1 \text{ on obtient } d = \frac{2^k - 1 - d^\circ \Psi_1}{2} + \frac{2^k + 1 - d^\circ \Psi_1}{2} + d^\circ \Psi_1 = 2^k.$$

b) montrons que tout Ψ_j , pour $j \in D$, divise $R^{(k)}(X) - X$:

si j divise $2^r - 1$: prenons comme racine j -ième de 1 $\xi = e^{\frac{2i\pi}{j}}$, donc $\xi + \frac{1}{\xi} = \cos \frac{2\pi}{j}$ est racine de Ψ_j .

Montrons qu'elle est aussi racine de $R^{(k)}(X) - X$, cf le 2), que

$$T_{2^k}\left(\frac{1}{2}\left(\xi + \frac{1}{\xi}\right)\right) = \frac{1}{2}\left(\xi + \frac{1}{\xi}\right).$$

$T_{2^k}\left(\frac{1}{2}\left(\xi + \frac{1}{\xi}\right)\right) = T_{2^k}\left(\cos \frac{2\pi}{j}\right) = \cos \frac{2^k \times 2\pi}{j}$ (d'après la définition même des polynômes de Tchebychev) mais $\frac{2^k \times 2\pi}{j} - \frac{2\pi}{j} = \frac{2^k - 1}{j} 2\pi$ est un multiple de 2π puisque j divise $2^r - 1$. Donc $T_{2^k}\left(\frac{1}{2}\left(\xi + \frac{1}{\xi}\right)\right) = \cos \frac{2\pi}{j} = \frac{1}{2}\left(\xi + \frac{1}{\xi}\right)$ et $\xi + \frac{1}{\xi}$ est aussi racine de $R^{(k)}(X) - X$.

Or Ψ_j est le polynôme minimal de $\xi + \frac{1}{\xi}$, donc Ψ_j divise $R^{(k)}(X) - X$.

si j divise $2^r + 1$, le même raisonnement que ci-dessus permet d'arriver à la même conclusion (cette fois $\frac{2^k \times 2\pi}{j} + \frac{2\pi}{j} = \frac{2^k + 1}{j} 2\pi$ et on utilise la parité de \cos).

Comme tout Ψ_j , pour $j \in D$, divise $R^{(k)}(X) - X$ et que les Ψ_j sont distincts et irréductibles (sur \mathcal{Q}), ils sont premiers entre eux 2 à 2 et ainsi leur produit divise $R^{(k)}(X) - X$.

$\prod_{j \in D} \Psi_j(X)$ et $R^{(k)}(X) - X$ étant unitaires et de même degré ils sont bien égaux.

5.3) On va utiliser le 5.2).

On a $k' = qk$:

si $q = 2s$, alors $2^{k'} - 1 = (2^{2k})^s - 1^s = (2^{2k} - 1)A$ (cf l'identité $a^s - b^s = (a - b)(a^{s-1} + a^{s-2}b + \dots + b^{s-1})$) et $2^{k'} - 1 = (2^k - 1)(2^k + 1)A$.

Donc si j divise $2^k - 1$ ou $2^k + 1$, j divise $2^{k'} - 1$ donc tout Ψ_j qui divise $R^{(k)}(X) - X$ divise aussi $R^{(k')}(X) - X$

si $q = 2s + 1$, alors $2^{k'} - 1 = (2^k)^{2s+1} - 1^{2s+1} = (2^k - 1)B$ et

$$2^{k'} + 1 = (2^k)^{2s+1} - (-1)^{2s+1} = (2^k + 1)C.$$

Donc si j divise $2^k - 1$, j divise $2^{k'} - 1$ et si j divise $2^k + 1$, j divise $2^{k'} + 1$, donc, là aussi, tout Ψ_j qui divise $R^{(k)}(X) - X$ divise aussi $R^{(k')}(X) - X \square$.

6)

Recherche de polynômes de $\mathbb{Q}[X]$, unitaires, à racines toutes simples, $\neq -1$ et 2 , et R -stables.

6.1) Pour tous les entiers naturels n_j , le polynôme $(X - 2)^{n_1}(X + 1)^{n_2} \prod_{j \in E} \Psi_j^{n_j}$ avec E un

sous-ensemble quelconque d'entiers naturels impairs autre que 1 et 3 est évidemment R -stable, chaque facteur l'étant

En particulier, $\prod_{j \in E} \Psi_j$ est un polynôme à coefficients dans \mathbb{Q} unitaire, à racines toutes

simples, distinctes de -1 et 2 , et R -stable : on va montrer la réciproque ci-après au 6.3.

6.2) Soit $P \in \mathbb{Q}[X]$ unitaire, à racines toutes simples, distinctes de -1 et 2 et R -stable : R induit donc une permutation σ de l'ensemble des racines de P .

Si c est un cycle de longueur l faisant partie de la décomposition en cycles à supports disjoints de σ , alors les racines de P appartenant au support de c sont toutes racines d'un même Ψ_j (avec j impair), Ψ_j divisant $R^{(l)}(X) - X$.

Remarque : si σ se réduit au cycle c , alors $P = \Psi_j$ et aussi j (qui est impair) est tel que le plus petit $u > 0$ tel que $2^u \equiv \pm 1 \pmod{j}$ est $\frac{\varphi(j)}{2}$ (d'après le 4.2).

6.3) Si $P \in \mathbb{Q}[X]$ est unitaire, à racines toutes simples, distinctes de -1 et 2 et est R -stable, alors P est un produit de Ψ_j tous distincts, avec j impair autre que 1 et 3, et chaque Ψ_j divise un $R^{(l)}(X) - X$ avec $l \leq \deg(P)$.

6.4) Détermination des polynômes à coefficients dans \mathbb{Q} à racines toutes simples, distinctes de -1 et 2 , et R -stables de degré ≤ 8 :

d	polynôme R -stable de degré d
2	$\Psi_5 \{2\}$
3	$\Psi_7 \{3\} ; \Psi_9 \{3\}$
4	$\Psi_{15} \{4\}$
5	$\Psi_5 \Psi_7 \{2;3\} ; \Psi_5 \Psi_9 \{2;3\} ; \Psi_{11} \{5\}$
6	$\Psi_5 \Psi_{15} \{2;4\} ; \Psi_7 \Psi_9 \{2;4\} ; \Psi_{13} \{6\} ; \Psi_{21} \{6\}$
7	$\Psi_5 \Psi_{11} \{2;5\} ; \Psi_7 \Psi_{15} \{3;4\} ; \Psi_9 \Psi_{15} \{3;4\}$
8	$\Psi_5 \Psi_{13} \{2;6\} ; \Psi_5 \Psi_{21} \{2;6\} ; \Psi_7 \Psi_{11} \{3;5\} ; \Psi_9 \Psi_{11} \{3;5\} ; \Psi_{17} \{4;4\}$

Après le nom de chaque polynôme on indique les longueurs des cycles à supports disjoints composant la permutation induite par R : cela s'obtient par application du 4.3.

Par exemple $\Psi_{15} \{4\}$ signifie que la permutation induite par R sur les quatre racines de Ψ_{15} est un 4-cycle,

$\Psi_5 \Psi_9 \{2,3\}$ signifie que la permutation induite par R sur les cinq racines de $\Psi_5 \Psi_9$ est le produit de deux cycles : un de longueur 2 portant sur les deux racines de Ψ_5 , l'autre de longueur 3 portant sur les trois racines de Ψ_9 .

Et $\Psi_{17} \{4,4\}$ signifie que la permutation induite par R sur les huit racines de Ψ_{17} est le

produit de deux 4-cycles : un de longueur portant sur quatre racines de Ψ_{17} , l'autre portant sur les quatre autres racines de Ψ_{17} (voir solution du 4.3).

preuve :

6.1) évident

6.2) notons $c = (x_1 x_2 \dots x_l)$ où les x_i sont l racines de $P \in \mathbb{Q}[X]$: on a $R^{(l)}(x_1) = x_1$, donc x_1 est racine de $R^{(l)}(X) - X$, donc racine d'un facteur Ψ_j de sa décomposition (voir 5.2).

Mais Ψ_j est R -stable, donc tous les itérés par R de x_1 sont aussi racines de ce Ψ_j et comme ces itérés de x_1 sont toutes les racines appartenant au support du cycle celles-ci sont effectivement racines du même Ψ_j .

Evidemment, si $\sigma = c$, toutes les racines de P sont racines du même Ψ_j , donc P , qui est à racines simples divise, dans $\mathbb{Q}[X]$, Ψ_j .

Ψ_j étant irréductible c'est que $P = \Psi_j$ (les deux polynômes sont unitaires).

6.3) Soit σ la permutation induite par R sur les racines de P : σ est un produit de cycles à support disjoints, cad $\sigma = c_1 \circ c_2 \dots \circ c_k$.

Notons E_i l'ensemble des racines de P constituant le support de c_i et l_i la longueur de c_i : d'après ce qui précède,

pour $i = 1, 2, \dots, k$, $(\prod_{r \in E_i} (X - r))^{l_i} U_i = \Psi_{j_i}$, lequel divise, dans $\mathbb{Q}[X]$, $R^{(l_i)}(X) - X$. A noter que

les U_i ne sont pas à priori dans $\mathbb{Q}[X]$ mais dans $\mathbb{C}[X]$ puisque $\prod_{r \in E_i} (X - r)$ n'est pas

obligatoirement dans $\mathbb{Q}[X]$ et que les Ψ_{j_i} ne sont pas forcément distincts 2 à 2 (les racines des supports de deux cycles distincts c_i peuvent être racines d'un même Ψ).

Donc, en faisant le produit de ces k égalités, on obtient $PU = \prod_{i=1,2,\dots,k} \Psi_{j_i}$, avec

$$U = \prod_{i=1,2,\dots,k} U_i \in \mathbb{C}[X].$$

Mais là comme $P \in \mathbb{Q}[X]$, U aussi est dans $\mathbb{Q}[X]$: en effet la division euclidienne dans $\mathbb{Q}[X]$ de $\prod_{i=1,2,\dots,k} \Psi_{j_i}$ par P donne $\prod_{i=1,2,\dots,k} \Psi_{j_i} = PS + T$ avec $T = 0$ ou $\deg(T) < \deg(P)$, or par

différence on a $P(U - S) = T$, donc nécessairement $U = S$ donc $U \in \mathbb{Q}[X]$.

La décomposition en facteur irréductibles sur $\mathbb{Q}[X]$ de PU étant $\prod_{i=1,2,\dots,k} \Psi_{j_i}$, celle de P est

aussi un produit de certains de ces Ψ_{j_i} mais là ils tous distincts car P est à racines simples.

6.4) Méthode : comme on ne s'intéresse qu'aux polynômes de degrés ≤ 8 , il suffit de trouver tous les Ψ_i de degrés ≤ 8 et diviseurs de $R^{(j)}(X) - X$ pour $j \leq 8$.

Les factorisations des $R^{(j)}(X) - X$ pour $j \leq 8$ étant indiquées au 5, on en déduit que les seuls Ψ_i à considérer sont (les facteurs Ψ_1 et Ψ_3 sont à exclure car -1 et 2 ne sont pas racines des polynômes recherchés)

degré 2 : Ψ_5

degré 3 : Ψ_7, Ψ_9

degré 4 : Ψ_{15}

degré 5 : Ψ_{11}

degré 6 : Ψ_{13}, Ψ_{21}

degré 7 : aucun

degré 8 : Ψ_{17}

Donc pour obtenir

un degré 2, une seule possibilité Ψ_5

un degré 3, deux possibilités Ψ_7 et Ψ_9
 un degré 4, une possibilité Ψ_{15} (Ψ_5^2 est interdit car on veut que des racines simples)
 un degré 5 : trois possibilités $\Psi_5\Psi_7$, $\Psi_5\Psi_9$, Ψ_{11}
 etc

Remarque : le degré 2 peut se trouver directement.

En effet si a et b sont les deux racines distinctes de P (et différentes de -1 et 2) on doit avoir $R(a) = b$ (puisque $R(a) \neq a$) et $R(b) = a$ (puisque $R(b) \neq b$), soit $a^2 - 2 = b$ et $b^2 - 2 = a$, donc $a^2 - b^2 = b - a$ et comme a et b sont distinctes, $a + b = -1$ et $a^2 - 2 = -a - 1$ soit $a^2 + a - 1 = 0$, et de même $b^2 + b - 1 = 0$, cad a et b sont les racines de $X^2 + X - 1$, donc $P(X) = X^2 + X - 1 = \Psi_5 \square$.

7) **Sur la suite de polynômes** $S_n(X) = 2(T_n(\frac{1}{2}X) + T_{n-1}(\frac{1}{2}X) + \dots + T_1(\frac{1}{2}X)) + 1, n \geq 1$

Un rappel de quelques résultats sur les polynômes de Tchebychev a été donné au 2).

7.1) On pose $S_1(X) = 2T_1(\frac{1}{2}X) + 1 = X + 1$ et pour tout $n \geq 1$,

$$S_{n+1}(X) = S_n(X) + 2T_{n+1}(\frac{1}{2}X)$$

n	T_n	S_n
0	1	non défini
1	X	$X + 1 = \Psi_3(X)$
2	$2X^2 - 1$	$X^2 + X - 1 = \Psi_5(X)$
3	$4X^3 - 3X$	$X^3 + X^2 - 2X - 1 = \Psi_7(X)$
4	$8X^4 - 8X^2 + 1$	$X^4 + X^3 - 3X^2 - 2X + 1$
5	$16X^5 - 20X^3 + 5X$	$X^5 + X^4 - 4X^3 - 3X^2 + 3X + 1 = \Psi_{11}(X)$
6	$32X^6 - 48X^4 + 18X^2 - 1$	$X^6 + X^5 - 5X^4 - 4X^3 + 6X^2 + 3X - 1 = \Psi_{13}(X)$
7	$64X^7 - 112X^5 + 56X^3 - 7X$	$X^7 + X^6 - 6X^5 - 5X^4 + 10X^3 + 6X^2 - 4X - 1$
8	$128X^8 - 256X^6 + 160X^4 - 32X^2 + 1$	$X^8 + X^7 - 7X^6 - 6X^5 + 15X^4 + 10X^3 - 10X^2 - 4X + 1 = \Psi_{17}(X)$
9	$256X^9 - 576X^7 + 432X^5 - 120X^3 + 9X$	$X^9 + X^8 - 8X^7 - 7X^6 + 21X^5 + 15X^4 - 20X^3 - 10X^2 + 5X + 1$

Remarque 1 : on verra au 7.3.1 que la suite des polynômes S_n ne contient aucun Ψ d'indice pair, par contre (voir 7.3.2) elle contient tous les Ψ_p pour p premier impair (pas $\Psi_2(X) = X + 2$) : $S_{\frac{p-1}{2}} = \Psi_p$.

Par exemple $\Psi_{19} = S_9$.

Mais cette suite (S) ne contient pas tous les polynômes Ψ d'indice impair :

par exemple $\Psi_9(X) = X^3 - 3X + 1$ (voir 3.5), $\Psi_{15}(X)$ et $\Psi_{21}(X)$ (voir les coefficients au 7.3.2) ne sont pas des polynômes de la suite (S)

Remarque 2 : le polynôme $S_5 = \Psi_{11} = X^5 + X^4 - 4X^3 - 3X^2 + 3X + 1$ fait l'objet de l'exercice 8 de P12.5 de la référence 1.

7.2) Quelques propriétés des polynômes S_n

7.2.1) pour tout entier $n \geq 1$, $S_n = \sum_{p=0}^{E(\frac{n}{2})} w_p$ avec $w_p = (-1)^p (C_{n-p}^p X^{n-2p} + C_{n-p-1}^p X^{n-2p-1})$
avec la convention $C_i^j = 0$ si $j > i$ et $C_i^0 = 1$ si $i \geq 0$.

si n est pair, le w_p d'indice le plus grand est $w_{\frac{n}{2}} = (-1)^{\frac{n}{2}} = S_n(0)$

si n est impair, le w_p d'indice le plus grand est $w_{\frac{n-1}{2}} = (-1)^{\frac{n-1}{2}} (\frac{n+1}{2} X + 1)$ et
 $S_n(0) = (-1)^{\frac{n-1}{2}}$

en particulier, S_n est de degré n et $\in \mathbb{Z}[X]$; il est unitaire et le coefficient de X^{n-1} est 1

7.2.2) pour tout entier $n \geq 1$, $S_n(Y + \frac{1}{Y}) = \frac{Y^{2n+1} - 1}{(Y-1)Y^n}$

pour tout entier $n \geq 1$, S_n a n racines réelles distinctes : $2 \cos \frac{2k\pi}{2n+1} \in]-2; 2[-\{0\}$,
pour $k = 1, 2, \dots, n$.

la somme des racines est -1 ; si r est une racine, $-r$ n'est pas une racine

-1 est racine de S_n si et seulement si 3 divise $2n+1$ ($\Leftrightarrow n = 1, 4, 7, 10, \dots$)

7.2.3) S_n est R -stable et une racine est fixée par R si et seulement si 3 divise $2n+1$
(la seule racine fixée est alors -1)

A noter que les polynôme T_n (à l'aide desquels les S_n sont obtenus ne sont pas R -stable), en effet les racines r de T_n sont dans $] -1; 1[$ et alors $R(r) = r^2 - 2 < -1$.

7.2.4) pour tout entier $n \geq 1$, $S_n(R(X)) = (-1)^n S_n(X) S_n(-X)$

7.2.5) Quelques valeurs particulières de S_n pour $n \geq 1$

$S_n(-2) = (-1)^n$; $S_n(2) = 2n+1$; $S_n(0) = (-1)^{\frac{n}{2}}$ si n est pair et $(-1)^{\frac{n-1}{2}}$ sinon ;

si 3 ne divise pas $2n+1$ alors $S_n(1) = (-1)^n$ et $S_n(-1) = \pm 1$

si 3 divise $2n+1$ alors $S_n(1) = \pm 2$ (preuve au 7.3)

rappel : on a vu au 7.2.2 que si 3 divise $2n+1$ alors $S_n(-1) = 0$.

7.3) Décomposition en facteurs irréductibles de S_n

7.3.1) Pour tout $n \geq 1$, $S_n = \prod_{\substack{d|2n+1 \\ d \neq 1}} \Psi_d$

Le fait que S_n soit un produit de Ψ_d avec d impair n'est pas une surprise : S_n étant R -stable, cela correspond au 6.3, à ceci-près qu'ici d peut prendre la valeur 3 dans le cas où S_n a -1 comme racine (voir 7.2.2) et alors dans la factorisation de S_n il y a bien $X+1 = \Psi_3(X)$.

7.3.2) Si $2n+1$ est premier alors $S_n = \Psi_{2n+1}$; donc la suite des polynômes S_n contient tous les polynômes Ψ_p avec p premier impair, et compte-tenu du 7.2, on obtient alors la formule explicite des coefficients de ces Ψ_p .

Si p est un nombre premier impair alors $S_{\frac{p^2-1}{2}} = \Psi_p \Psi_{p^2}$

par exemple, $S_4 = \Psi_3 \Psi_9$

Si p et q sont deux nombres premiers distincts impairs alors $S_{\frac{pq-1}{2}} = \Psi_p \Psi_q \Psi_{pq}$

Application : $\Psi_{15} = \frac{S_7}{\Psi_3 \Psi_5}$, soit

$$\Psi_{15}(X) = \frac{X^7 + X^6 - 6X^5 - 5X^4 + 10X^3 + 6X^2 - 4X - 1}{(X+1)(X^2 + X - 1)} = X^4 - X^3 - 4X^2 + 4 + 1 \text{ et aussi}$$

$$\Psi_{21}(X) = \frac{S_{10}(X)}{\Psi_3(X)\Psi_7(X)} = X^6 - X^5 - 6X^4 + 6X^3 + 8X^2 - 8X + 1$$

7.3.3) S_n est irréductible sur $\mathbb{Q} \Leftrightarrow 2n+1$ est premier (et alors $S_n = \Psi_{2n+1}$)

Remarque : en utilisant les polynômes cyclotomiques (et pas les polynômes Ψ_n), on peut aussi prouver que S_n est irréductible si $2n+1$ est premier (mais on n'a pas l'équivalence).

En effet, d'après le 7.2.2, $Y^n S_n(Y + \frac{1}{Y}) = Y^{2n} + Y^{2n-1} + \dots + Y + 1$, lequel est le polynôme cyclotomique Φ_{2n+1} puisque $2n+1$ est premier. Or tout polynôme cyclotomique est irréductible, donc le polynôme $Y^n S_n(Y + \frac{1}{Y})$ est irréductible, ce qui implique que $S_n(X)$ le soit (si $S_n(X)$ est réductible, $Y^n S_n(Y + \frac{1}{Y})$ l'est).

Les exercices 8 et 9 de P12.5 de la ref 1 détaillent cet aspect.

7.3.4) Une autre application du 7.3.1 : si 3 divise $2n+1$ alors $S_n(1) = \pm 2$.

Cette démonstration est un peu longue : il y a peut être un raccourci..

preuve :

7.2.1) La formule est vraie pour $n=1$ puisque $S_1 = X+1$ et

$$w_0 = (-1)^0 (C_{1-0}^0 X^{1-2 \times 0} + C_{1-0-1}^0 X^{1-2 \times 0-1}) = X+1.$$

Supposons la vraie au rang $n \geq 1$.

On a $S_{n+1} = S_n + 2T_{n+1}(\frac{1}{2}X)$, et

$$\text{pour } n \geq 1, T_n(X) = 2^{n-1} X^n + \frac{n}{2} \sum_{k=1}^{E(\frac{n}{2})} (-1)^k \frac{C_{n-k-1}^{k-1}}{k} (2X)^{n-2k}, \text{ donc}$$

$$2T_{n+1}(\frac{1}{2}X) = X^{n+1} + (n+1) \sum_{k=1}^{E(\frac{n+1}{2})} (-1)^k \frac{C_{n-k}^{k-1}}{k} X^{n+1-2k}.$$

Il s'agit donc de montrer, pour que la formule soit vraie au rang $n+1$, que dans

$$S_n + 2T_{n+1}(\frac{1}{2}X),$$

le coefficient de X^{n+1-2p} soit $(-1)^p C_{n+1-p}^p$ et celui de X^{n-2p} soit $(-1)^p C_{n-p}^p$.

Cas du coefficient de X^{n+1-2p}

si $p=0$, X^{n+1} n'apparaît que dans $2T_{n+1}(\frac{1}{2}X)$ avec le coefficient 1 qui est bien

$$(-1)^0 C_{n+1-0}^0$$

si $p \geq 1$, dans S_n le coefficient de $X^{n+1-2p} = X^{n-2(p-1)-1}$ est $(-1)^{p-1} C_{n-(p-1)-1}^{p-1}$, et dans

$2T_{n+1}(\frac{1}{2}X)$ son coefficient est $(n+1)(-1)^p \frac{C_{n-p}^{p-1}}{p}$, soit une somme de

$$(-1)^{p-1} C_{n-p}^{p-1} (1 - \frac{n+1}{p}) = (-1)^p \frac{(n-p)!}{(p-1)!(n-2p+1)!} \times \frac{n+1-p}{p} = (-1)^p C_{n+1-p}^p, \text{ résultat}$$

attendu.

Cas du coefficient de X^{n-2p}

le coefficient de X^{n-2p} dans S_n étant $(-1)^p C_{n-p}^p$, et celui dans $2T_{n+1}(\frac{1}{2}X)$ étant 0, le coefficient de X^{n-2p} dans $S_n + 2T_{n+1}(\frac{1}{2}X)$ est bien $(-1)^p C_{n-p}^p$.

La formule $S_n = \sum_{p=0}^{E(\frac{n}{2})} w_p$ avec $w_p = (-1)^p (C_{n-p}^p X^{n-2p} + C_{n-p-1}^p X^{n-2p-1})$ prouve évidemment que S_n est de degré n et $\in \mathbb{Z}[X]$; il est unitaire et le coefficient de X^{n-1} est 1.

7.2.2) De la définition, pour tout $n \geq 1$, $S_n(X) = 2(T_n(\frac{1}{2}X) + T_{n-1}(\frac{1}{2}X) + \dots + T_1(\frac{1}{2}X)) + 1$, on tire évidemment (voir rappel sur T_n au 2)).

$$S_n(Y + \frac{1}{Y}) = \sum_{j=1}^n (Y^j + \frac{1}{Y^j}) + 1 = \frac{1-Y^n}{1-Y} + \frac{1}{Y} \times \frac{1-\frac{1}{Y^n}}{1-\frac{1}{Y}} \text{ (somme de deux progressions}$$

géométriques)

$$\text{et } S_n(Y + \frac{1}{Y}) = \frac{-1 + Y^n + 1 - \frac{1}{Y^n}}{Y-1} = \frac{Y^{2n+1} - 1}{Y^n(Y-1)}.$$

Donc $S_n(y + \frac{1}{y}) = 0 \Leftrightarrow y$ est racine $(2n+1)$ -ième de 1 et $y \neq 1$.

Comme les racines $(2n+1)$ -ième de 1 autres que 1 sont $y_k = e^{\frac{2ik\pi}{2n+1}}$ pour $k = 1, 2, \dots, 2n$,

$$S_n(y + \frac{1}{y}) = 0 \Leftrightarrow y + \frac{1}{y} = 2 \cos \frac{2k\pi}{2n+1} = r_k \text{ pour } k = 1, 2, \dots, 2n.$$

Mais si $k + k' = 2n+1$, $r_k = r_{k'}$, donc les valeurs distinctes prises par r_k sont à chercher parmi r_1, r_2, \dots, r_n . Comme pour $k \in \{1; 2; \dots; n\}$, $\frac{2k\pi}{2n+1} \in]0; \pi[-\{\frac{\pi}{2}\}$, r_1, r_2, \dots, r_n sont distinctes : ce sont donc les n racines de S_n , puisque celui-ci est de degré n .

Elles sont toutes situées dans $[-2; 2[-\{0\}$ et leur somme est -1 compte-tenu des relations coefficients-racines.

Si r_k est une racine, $-r_k$ ne peut être une autre racine $r_{k'}$ car il faudrait que $\frac{2k\pi}{2n+1} + \frac{2k'\pi}{2n+1} = \pi$ avec $1 \leq k, k' \leq n$: or $2k + 2k' = 2n+1$ est impossible.

Autre façon : si $r_k = \xi + \frac{1}{\xi}$ avec ξ racine n -ième de 1 autre que 1 et $r_{k'} = \xi' + \frac{1}{\xi'}$ avec ξ'

racine n -ième de 1 autre que 1 sont deux racines de S_n ,

$r_k = -r_{k'}$ implique $(\xi + \frac{1}{\xi})(1 + \frac{1}{\xi\xi'}) = 0$, soit $\xi = -\xi'$ ou $\xi\xi' = -1$, relations qui élevées à

la puissance $2n+1$ donnent $1 = -1$, ce qui est impossible.

Quant à -1 , -1 est racine de S_n si et seulement si il existe $k \in \{1; 2; \dots; n\}$ tel que $\cos \frac{2k\pi}{2n+1} = -\frac{1}{2}$, soit $\frac{k}{2n+1} = \pm \frac{1}{3} + K \Leftrightarrow 3k = \pm(2n+1) + 3(2n+1)K$.

Ceci implique que 3 divise $2n+1$; réciproquement si 3 divise $2n+1$, en prenant $k = \frac{2n+1}{3}$, valeur qui est bien dans $\{1; 2; \dots; n\}$ on a $r_k = -1$.

7.2.3) Montrons la R stabilité des polynômes S_n .

C'est évident si $n = 1$ car la seule racine de S_1 est -1 et $R(-1) = -1$.

On suppose maintenant $n \geq 2$.

Soit $r_k = 2 \cos \frac{2k\pi}{2n+1}$ pour $k \in \{1, 2, \dots, n\}$ une de ses racines.

D'après le 1), $R(r_k) = 2 \cos \frac{2(2k)\pi}{2n+1}$ et $2k \in \{2; 4; \dots; 2n\}$

soit $2 \leq 2k \leq n$: prenons $k' = 2k$, donc $2 \leq k' \leq n$ et $R(r_k) = r_{k'}$ est racine de S_n
 soit $n+1 \leq 2k \leq 2n$: prenons $k' = 2n+1-2k$, donc $1 \leq k' \leq n$ et $R(r_k) = r_{k'}$ est racine de S_n .

Donc R transforme toute racine de S_n en une racine de S_n , mais la transformation est-elle injective?

$R(r_k) = R(r_{k'}) \Leftrightarrow r_k^2 = r_{k'}^2 \Leftrightarrow r_k = \pm r_{k'}$; or on a vu plus haut que S_n ne peut avoir deux racines opposées, donc la seule possibilité est $r_k = r_{k'}$, cad R est injective, donc bijective et ainsi S_n est bien stable (l'ensemble des racines est globalement conservé). La seule racine fixée par R ne peut être qu'un des points fixes de R , soit -1 ou 2 : or 2 n'est jamais racine de S_n par contre -1 l'est si et seulement si 3 divise $2n+1$.

7.2.4) $S_n(R(X))$ et $(-1)^n S_n(X)S_n(-X)$ sont deux polynômes unitaires de degré $2n$: pour montrer qu'ils sont égaux, on va montrer qu'ils ont les mêmes racines :

Les racines de $(-1)^n S_n(X)S_n(-X)$ sont évidemment les n racines de S_n et leurs n opposées, toutes distinctes des précédentes puisqu'on a vu que S_n ne peut avoir deux racines opposées.

Comme R transforme toute racine de S_n en une racine de S_n (R -stabilité), R transforme aussi l'opposée de toute racine de S_n en une racine de S_n (parité) et donc les $2n$ racines, distinctes, de $(-1)^n S_n(X)S_n(-X)$ sont aussi $2n$ racines distinctes de $S_n(R(X))$.

7.2.5)

Du 7.2.4 on déduit $S_n(2) = (-1)^n S_n(2)S_n(-2)$ et comme $S_n(2) \neq 0$, on a $S_n(-2) = (-1)^n$. D'après la définition même de S_n , $S_n(2) = 2(T_n(1) + T_{n-1}(1) + \dots + T_1(1)) + 1 = 2n+1$ (voir propriété de T_n)

On déduit aussi du 7.2.4 $S_n(-2) = (-1)^n S_n^2(0)$, soit $S_n^2(0) = 1$; ce résultat a déjà été prouvé au 7.2.1 où il est précisé en plus le signe de $S_n(0)$.

Toujours grâce au 7.2.4, on a $S_n(-1) = (-1)^n S_n(-1)S_n(1)$: donc si 3 ne divise pas $2n+1$, $S_n(-1) \neq 0$ (voir 7.2.2) et $S_n(1) = (-1)^n$.

Reste à montrer que $S_n(-1) = \pm 1$ lorsque 3 ne divise pas $2n+1$.

Cette fois on utilise le 7.2.2 : $S_n(-1) = S_n(j + \frac{1}{j}) = \frac{j^{2n+1} - 1}{(j-1)j^n}$ pour tout $n \geq 1$.

Evidemment on retrouve que si 3 divise $2n+1$, $S_n(-1) = 0$ puisqu'alors $j^{2n+1} = 1$.

Mais ici, le cas qui nous intéresse est le cas où 3 ne divise pas $2n+1$, donc $j^{2n+1} = j$ ou j^2 :

$$\text{si } j^{2n+1} = j, \text{ donc } j^n = \pm 1, \text{ on a } S_n(-1) = \frac{j-1}{(j-1)j^n} = \pm 1$$

$$\text{si } j^{2n+1} = j^2, \text{ donc } (j^{n+1})^2 = 1, \text{ soit } j^{n+1} = \pm 1 \text{ et on a}$$

$$S_n(-1) = \frac{j^2-1}{(j-1)j^n} = \frac{j^2+j}{j^{n+1}} = \frac{-1}{\pm 1} = \pm 1.$$

7.3.1) On a vu au 7.2.2 que les racines de S_n sont $e^{\frac{2ik\pi}{2n+1}} + \frac{1}{e^{\frac{2ik\pi}{2n+1}}} = 2 \cos \frac{2k\pi}{2n+1}$

pour $k = 1, 2, \dots, n$.

Pour tout diviseur $d \neq 1$ de $2n+1$ on considère $k = \frac{2n+1}{d} \leq n + \frac{1}{2}$ et donc

$k \in \{1; 2; \dots; n\}$, d'où $e^{\frac{2ik\pi}{2n+1}} = e^{\frac{2i\pi}{d}}$ est une racine d -ième de 1 primitive et donc Ψ_d est le polynôme minimal $e^{\frac{2i\pi}{d}} + \frac{1}{e^{\frac{2i\pi}{d}}}$ (voir le 3) qui est évidemment aussi une racine

de S_n , donc Ψ_d divise S_n .

Donc $U = \prod_{\substack{d|2n+1 \\ d \neq 1}} \Psi_d$ divise S_n (puisque les Ψ_d sont irréductibles, donc premiers entre eux

deux à deux).

Mais U et S_n sont unitaires et

$$\deg U = \sum_{\substack{d|2n+1 \\ d \neq 1}} \frac{\varphi(d)}{2} = \sum_{d|2n+1} \frac{\varphi(d)}{2} - \frac{\varphi(1)}{2} = \frac{2n+1}{2} - \frac{1}{2} = n = \deg S_n, \text{ donc } U = S_n.$$

7.3.2) C'est une application directe du 7.3.1.

7.3.3) S_n sera irréductible si et seulement si sa factorisation en facteurs irréductibles

$\prod_{\substack{d|2n+1 \\ d \neq 1}} \Psi_d$ se réduit à un seul facteur : or il y a toujours le facteur Ψ_{2n+1} , lequel sera le seul

facteur si et seulement si $2n+1$ est divisible que par 1 et $2n+1$, cad si $2n+1$ est premier.

7.3.4) Montrons que si 3 divise $2n+1$ alors $S_n(1) = \pm 2$: je vais le faire en quatre étapes.

a) D'après le 3, pour $n \geq 3$, $\Phi_n(X) = X^{\frac{\varphi(n)}{2}} \Psi_n(X + \frac{1}{X})$, d'où en remplaçant X par $-j$, on

$$\text{obtient } \Psi_n(1) = (-1)^{\frac{-\varphi(n)}{2}} \Phi_n(-j).$$

Mais $\Phi_n \in \mathbb{Z}[X]$ et comme les puissances de j sont 1 ou j ou j^2 , $\Phi_n(-j) = aj^2 + bj + c$ avec a, b, c dans \mathbb{Z} .

Et puisque $(-1)^{\frac{-\varphi(n)}{2}} = \pm 1$, $\Psi_n(1) = aj^2 + bj + c$ avec a, b, c dans \mathbb{Z} , soit

$$\Psi_n(1) = -\frac{a+b}{2} + (-a+b)\frac{\sqrt{3}}{2}i + c.$$

Par ailleurs Ψ_n est à coefficients dans \mathbb{Q} (polynôme minimal sur \mathbb{Q}) donc $\Psi_n(1)$ est réel et $a = b$, d'où $\Psi_n(1) = -a + c \in \mathbb{Z}$. Ce qui est encore vrai si $n = 1$ ou 2 .

b) $R(1) = R(-1) = -1$, donc $R^{(k)}(1) = -1$ pour tout $k \geq 1$.

D'après le 5.2, $R^{(k)}(X) - X = \prod_{j \in D} \Psi_j(X)$ où $D = \{\text{diviseurs de } 2^k - 1\} \cup \{\text{diviseurs de}$

$2^k + 1\}$, d'où en remplaçant X par 1, on obtient

$$-2 = \Psi_1(1)\Psi_3(1) \prod_{j|2^k \pm 1} \Psi_j(1), \text{ soit } 1 = \prod_{\substack{j|2^k \pm 1 \\ j \neq 1, j \neq 3}} \Psi_j(1).$$

Or on vient de voir que pour tout $n \geq 1$, $\Psi_n(1) \in \mathbb{Z}$: donc pour tout $k \geq 1$ et pour tout $j \neq 1$ et 3 et diviseur de $2^k \pm 1$, on a $\Psi_j(1) = \pm 1$; c'est en fait vrai pour $j = 1$

($\Psi_1(X) = X - 2$) mais pas pour $j = 3$ ($\Psi_3(X) = X + 1$).

c) Soit j un entier impair quelconque : on a $2^{\varphi(j)} \equiv 1 \pmod{j}$ d'après Euler, cad j divise $2^k - 1$ avec $k = \varphi(j) \geq 1$. Donc pour tout j impair autre que 1, on a $\Psi_j(1) = \pm 1$.

d) Enfin, puisque $S_n(1) = \prod_{\substack{d|2n+1 \\ d \neq 1}} \Psi_d(1)$ et qu'ici 3 divise $2n+1$, on a

$$S_n(1) = \Psi_3(1) \prod_{\substack{d|2n+1 \\ d \neq 1 \\ d \neq 3}} \Psi_d(1) = 2 \times \pm 1 = \pm 2 \quad \square.$$

8) Sur une famille de polynômes à coefficients réels R -stables mais n'appartenant pas à $\mathbb{Q}[X]$

Pour $n \geq 1$, on pose $U_n(X) = \prod_{i=1}^n (X - 2 \cos \frac{2^i \pi}{2^n - 1})$.

8.1) $U_1 = \Psi_1, U_2 = \Psi_3^2, U_3 = \Psi_7, U_4 = \Psi_{15}$

8.2) Pour $n \geq 3$, U_n a n racines distinctes et différentes de -1 et 2 .

8.3) Pour tout $n \geq 1$, U_n est R -stable, et pour $n \geq 3$, la permutation induite par R sur les n racines de U_n est un n -cycle.

8.4) $U_n \in \mathbb{Q}[X] \Leftrightarrow 1 \leq n \leq 4$.

preuve :

8.1) $U_1(X) = X - 2 = \Psi_2(X)$

$U_2(X) = (X - 2 \cos \frac{2\pi}{3})(X - 2 \cos \frac{4\pi}{3}) = (X + 1)^2 = \Psi_3^2$

$U_3(X) = (X - 2 \cos \frac{2\pi}{7})(X - 2 \cos \frac{4\pi}{7})(X - 2 \cos \frac{8\pi}{7}) = \Psi_7$

$U_4(X) = (X - 2 \cos \frac{2\pi}{15})(X - 2 \cos \frac{4\pi}{15})(X - 2 \cos \frac{8\pi}{15})(X - 2 \cos \frac{16\pi}{15}) = \Psi_{15}$

8.2) Notons $x_i = 2 \cos \frac{2^i \pi}{2^n - 1}$ pour $i = 1, 2, \dots, n$.

a) Pour $1 \leq i \leq n - 1$, $\frac{2^i \pi}{2^n - 1} \in]0; \pi[$, donc x_1, x_2, \dots, x_{n-1} sont distinctes deux à deux.

Peut-on avoir $x_n = x_i \Leftrightarrow 2^n = \pm 2^i + K(2^n - 1)$ pour un $1 \leq i \leq n - 1$?

Cas 1 : $2^n = 2^i + K(2^n - 1) \Leftrightarrow 2^n - 2^i = K(2^n - 1)$.

Comme $0 < 2^n - 2^i < 2^n - 1$ on a $0 < K(2^n - 1) < 2^n - 1$, soit $0 < K < 1$ ce qui est impossible

Cas 2 : $2^n = -2^i + K(2^n - 1) \Leftrightarrow 2^n + 2^i = K(2^n - 1)$

Cette fois on a $2^n + 1 < 2^n + 2^i \leq 2^n + 2^{n-1} = 3 \times 2^{n-1}$ et

$\frac{2^n + 1}{2^n - 1} < K < \frac{3 \times 2^{n-1}}{2^n - 1} = 2 + \frac{2(1 - 2^{n-2})}{2^n - 1}$, soit $1 < K < 2$ (car $n \geq 3$), ce qui est aussi impossible.

Donc x_1, x_2, \dots, x_n sont distinctes.

b) Peut-on avoir $x_i = 2$ pour $1 \leq i \leq n$?

$x_i = 2 \Leftrightarrow 2^{i-1} = K(2^n - 1) \Leftrightarrow K = \frac{2^{i-1}}{2^n - 1} \Leftrightarrow 0 < K < 1$ (car $2^{i-1} + 1 < 2^{n-1} + 2^{n-1} = 2^n$), ce qui est impossible.

c) Peut-on avoir $x_i = -1$ pour $1 \leq i \leq n$?

$x_i = -1 \Leftrightarrow \frac{2^{i-1}}{2^n - 1} = \pm \frac{1}{3} + K \Leftrightarrow 3 \times 2^{i-1} = (\pm 1 + 3K)(2^n - 1)$

$K \leq -1$ implique $\pm 1 + 3K < 0$ ce qui est impossible

$K = 0$ implique $3 \times 2^{i-1} = (2^n - 1)$ ce qui est impossible si $i \geq 2$ (pair \neq impair) et c'est aussi impossible pour $i = 1$ car $n \geq 3$.

Donc nécessairement $K \geq 1$ et $\pm 1 + 3K \geq 2$. Par ailleurs 3 étant premier avec $\pm 1 + 3K$, 3 doit diviser $2^n - 1$, donc n doit être pair, car si n était impair, puisque $2 \equiv -1 \pmod{3}$, on aurait $2^n \equiv -1 \pmod{3}$, soit $2^n - 1 \equiv -2 \pmod{3}$ et 3 ne diviserait pas $2^n - 1$.

Posons $n = 2p$ (avec $p \geq 2$, puisque $n \geq 3$) : on a alors

$3 \times 2^{i-1} = (\pm 1 + 3K)(4^p - 1) \Leftrightarrow 2^{i-1} = (\pm 1 + 3K)(4^{p-1} + 4^{p-2} + \dots + 4 + 1) > 2 \times 4^{p-1} = 2^{n-1}$ ce qui est impossible.

8.3) D'après le 2), pour $i = 1, 2, \dots, n-1$ on a $R(2 \cos \frac{2^i \pi}{2^n - 1}) = 2 \cos \frac{2^{i+1} \pi}{2^n - 1}$ et $R(2 \cos \frac{2^n \pi}{2^n - 1}) = 2 \cos \frac{2^{n+1} \pi}{2^n - 1} = 2 \cos \frac{2\pi}{2^n - 1}$ puisque $\frac{2^{n+1} \pi}{2^n - 1} - \frac{2\pi}{2^n - 1} = 2\pi$.

Donc U_n est toujours R -stable, et pour $n \geq 3$, les racines de U_n étant distinctes, R induit un n -cycle sur ses racines.

8.4) On a vu que $\Psi_1, \Psi_2, \Psi_3, \Psi_4$ sont dans $\mathbb{Q}[X]$.

On va montrer que pour $n \geq 5$, $\Psi_n \notin \mathbb{Q}[X]$.

Si pour $n \geq 5$, $U_n \in \mathbb{Q}[X]$, comme U_n est R -stable, à racines distinctes différentes de -1 et 2 , alors d'après le 6.3, la décomposition en facteurs irréductibles de U_n est constituée de Ψ_j (j impair) tous distincts.

Supposons qu'il y ait effectivement dans la décomposition de U_n au moins deux Ψ_j , disons Ψ_{j_1} et Ψ_{j_2} .

La permutation σ induite par R sur les racines de U_n est un n -cycle, donc par exemple, si x_1 est une racine de Ψ_{j_1} , toutes les racines de U_n sont des $R^{(i)}(x_1)$; or tous ces $R^{(i)}(x_1)$ restent des racines de Ψ_{j_1} et donc on n'obtient pas les racines de Ψ_{j_2} , donc on n'obtient pas toutes les racines de U_n , d'où une contradiction.

Nécessairement, si $U_n \in \mathbb{Q}[X]$, il existe j (impair) tel que $U_n = \Psi_j$, ce qui implique

$$n = \frac{\varphi(j)}{2} \text{ (} U_n \text{ et } \Psi_j \text{ ont même degré)}$$

il existe k premier avec j tel que $2 \cos \frac{2\pi}{2^n - 1} = 2 \cos \frac{2k\pi}{j}$ ($2 \cos \frac{2\pi}{2^n - 1}$ est racine de U_n , donc racine de Ψ_j)

La deuxième condition s'écrit $\frac{1}{2^n - 1} = \pm \frac{k}{j} + K$, soit $\theta = \pm k + Kj$ avec $\theta = \frac{j}{2^n - 1}$: θ étant entier, $2^n - 1$ divise j et ainsi θ divise j .

Donc θ divise aussi k , et comme k et j sont premier entre eux, c'est que $\theta = 1$, soit $j = 2^n - 1$.

La première condition donne alors $\varphi(2^n - 1) = 2n$: on va montrer que cette condition n'est pas vérifiée pour $n \geq 5$ (elle est effectivement vraie pour $n = 3$ et $n = 4$).

Je laisse au lecteur les cas $n = 5$ à $n = 10$ ($\varphi(1023) = \varphi(3)\varphi(11)\varphi(31) \neq 2 \times 10$).

Pour $n \geq 11$, je vais utiliser la minoration $\varphi(k) \geq \frac{\sqrt{k}}{2}$ pour tout $k \geq 1$ (minoration large : $\varphi(16) = 12$ et $\frac{\sqrt{16}}{2} = 2$).

On a donc $\varphi(2^n - 1) \geq \frac{\sqrt{2^n - 1}}{2}$ pour $n \geq 1$: on va montrer que pour $n \geq 11$,

$$\frac{\sqrt{2^n - 1}}{2} > 2n \text{ (c'est faux pour } n = 10\text{)}.$$

$$\frac{\sqrt{2^n - 1}}{2} > 2n \Leftrightarrow 2^n - 16n^2 - 1 > 0 \Leftrightarrow (2 \frac{n}{2} - 4n)(2 \frac{n}{2} + 4n) > 1.$$

Posons $d(x) = 2 \frac{x}{2} - 4x$: $d'(x) = \frac{\ln 2}{2} 2 \frac{x}{2} - 4$ et $d'(x) > 0 \Leftrightarrow x > \rho$ avec

$$\rho = \frac{2(\ln 8 - \ln(\ln 2))}{\ln 2} \simeq 3.$$

d est strictement croissante sur $[\rho; +\infty[$, donc pour $n \geq 11$ on a $d(n) \geq d(11) \simeq 1.25 > 1$ et $(2 \frac{n}{2} - 4n)(2 \frac{n}{2} + 4n) > 1$, soit $\frac{\sqrt{2^n - 1}}{2} > 2n$ et donc $\varphi(2^n - 1) \neq 2n$.

Donc si $n \geq 5$, U_n ne peut être dans $\mathbb{Q}[X]$ \square .

9) Résolubilité, groupe de Galois (sur \mathbb{Q}) des polynômes Ψ_n et S_n .

Rappelons que $P \in \mathbb{Q}[X]$ est résoluble (par radicaux) signifie que toutes ses racines s'obtiennent à partir des coefficients de P par les opérations algébriques usuelles (+, -, \times , \div) et par calculs de radicaux (éventuellement emboîtés), cad les racines de P sont dans une extension radicale de \mathbb{Q} (voir ref 1 ou 3).

Bien entendu, P est résoluble équivaut à dire que son groupe de Galois est résoluble (ref 1 ou 3).

9.1) Pour tout $n \geq 1$, Ψ_n et S_n sont résolubles

9.2) Pour tout $n \geq 3$ tel que $\frac{\varphi(n)}{2}$ est premier, le groupe de Galois de Ψ_n est cyclique d'ordre $\frac{\varphi(n)}{2}$.

preuves :

9.1) Les racines de Ψ_n sont de la forme $\xi + \frac{1}{\xi}$ où ξ est une racine n -ième de 1 primitive, donc Ψ_n est résoluble.

Les racines de S_n sont $2 \cos \frac{2k\pi}{2n+1} = \xi + \frac{1}{\xi}$ où ξ est une racine n -ième de 1, donc S_n est résoluble.

9.2) Pour $n \geq 3$, $d^\circ \Psi_n = \frac{\varphi(n)}{2}$ est donc premier, et d'après le 4.2) R induit un $\frac{\varphi(n)}{2}$ -cycle sur les racines de Ψ_n et comme Ψ_n est irréductible sur \mathbb{Q} , les hypothèses du 1)c et 1)d sont vérifiées et donc le groupe de Galois de Ψ_n est cyclique d'ordre $\frac{\varphi(n)}{2}$ \square .

Références

Référence 1 : <http://alain.pichereau.pagesperso-orange.fr/equation7.pdf>, paragraphe 12, propriétés 12.4, 12.5, 12.6.

Référence 2 : <http://alain.pichereau.pagesperso-orange.fr/equation45.pdf>

Référence 3 : Théorie de Galois de Jean-Pierre Escofier chez Dunod

Annexe 1

Exercice sur la factorisation de $P(X) = X^8 - 8X^6 + 20X^4 - 16X^2 - X + 2$

J'ai trouvé cet exercice fin 2016 sur un forum : la question 5 a soulevé beaucoup de problèmes, certains jugeant, à tort, l'énoncé incomplet et la nécessité de faire appel à Galois pour pouvoir conclure.

Ce polynôme est en fait $\Psi_1(X)\Psi_3(X)\Psi_7(X)\Psi_9(X) = R(R(R(X))) - X$, mais l'exercice peut être traité en ignorant tout ce qui précède.

1) Déterminer les racines rationnelles de P et factoriser P dans $\mathbb{Q}[X]$ en un produit de deux facteurs unitaires dont l'un n'a aucune racine rationnelle : ce facteur sera noté T .

2) On pose $R(X) = X^2 - 2$ et $R^{(2)}(X) = R(R(X))$, $R^{(3)}(X) = R(R(R(X)))$.

Montrer que

2.1) $P(X) = 0 \Leftrightarrow R^{(3)}(X) = X$

2.2) $P'(X) = 8XR(X)R^{(2)}(X) - 1$

2.3) Si r est racine de P , alors $P'(R(r)) = P'(r)$.

3) Montrer que si r est une racine de P , $R(r)$ est aussi racine de P et que si r est simple, $R(r)$ aussi.

Dans quels cas $R(r) = r$?

4) Soit a une racine (dans \mathbb{C}) de T : montrer que $a, R(a), R^{(2)}(a)$ sont trois racines distinctes simples de T .

5)

5.1) Montrer que T a six racines distinctes de la forme $a, R(a), R^{(2)}(a), b, R(b), R^{(2)}(b)$ et que $(P'(a) + 1)(P'(b) + 1) = -64$.

On pose $U(X) = (X - a)(X - R(a))(X - R^{(2)}(a))$ et $V(X) = (X - b)(X - R(b))(X - R^{(2)}(b))$.

5.2) Vérifier que R conserve globalement les racines de U et conserve globalement les racines de V .

5.3) Montrer que l'expression $r + R(r) + R^{(2)}(r)$ ne prend que deux valeurs lorsque r décrit les racines de T .

5.4) Déterminer la décomposition en facteurs irréductibles dans $\mathbb{Q}[X]$ de T .

6) Montrer que pour tout θ réel, $R(2 \cos \theta) = 2 \cos(2\theta)$; en déduire toutes les racines de P et on précisera les racines de chacun des deux facteurs irréductibles de T .

solution :

1) Si une racine de P est de la forme $\frac{p}{q}$ avec p et q entiers premiers entre eux, alors $p^8 - 8p^7q + 20p^4q^4 - 16p^2q^5 - pq^6 + 2q^7 = 0$: donc q divise p^8 donc divise p donc $q = \pm 1$ et p doit diviser alors 2, donc la seule possibilité de racine rationnelle est $\frac{p}{q} = \pm 1$ ou ± 2 .

On vérifie alors que seules -1 et 2 sont les racines rationnelles de P .

Donc $P(X) = (X + 1)(X - 2)T(X) = (X^2 - X - 2)T(X)$, le polynôme T s'obtenant par division euclidienne : $T(X) = X^6 + X^5 - 5X^4 - 3X^3 + 7X^2 + X - 1$.

Remarquons que T n'ayant pas de racine rationnelle, -1 et 2 sont racines simples de P .

2)

2.1) $R_2(X) = R(R(X)) = (R(X))^2 - 2 = X^4 - 4X^2 + 2$
 $R^{(3)}(X) = R(R^{(2)}(X)) = (X^4 - 4X^2 + 2)^2 - 2 = P(X) + X$,
donc $P(X) = R^{(3)}(X) - X$ et $P(X) = 0 \Leftrightarrow R^{(3)}(X) = X$.

2.2) $P'(X) = R_3'(X) - 1$

et

$R^{(3)'}(X) = R'(R^{(2)}(X))R^{(2)'}(X) = 2R^{(2)}(X)R'(R(X))R'(X) = 2R^{(2)}(X) \times 2R(X) \times 2X = 8XR(X)R^{(2)}(X)$
soit $P'(X) = 8XR(X)R^{(2)}(X) - 1$.

2.3) De 2.1) et 2.2) on déduit

$P'(R(r)) = 8R(r)R^{(2)}(r)R^{(3)'}(r) - 1 = 8R(r)R^{(2)}(r)r - 1 = P'(r)$.

3) Soit r une racine de P : $P(R(r)) = R^{(3)}(R(r)) - R(r) = R(R^{(3)}(r)) - R(r)$, puisque
 $R \circ R^{(3)} = R^{(3)} \circ R = R^{(4)}$,

et ainsi $P(R(r)) = R(r) - R(r) = 0$ et $R(r)$ est aussi racine de P .

Si r est simple alors $P'(r) \neq 0$ et comme (voir 2.3) $P'(R(r)) = P'(r)$, $R(r)$ est aussi racine simple.

$R(r) = r \Leftrightarrow r^2 - r - 2 = 0$ soit $r = -1$ ou $r = 2$: seules les racines rationnelles, -1 et 2 , de P sont conservées par R .

4) Notons que a n'est ni -1 , ni 2 puisque a est racine de T .

D'après 3), $R(a)$ et $R_2(a) = R(R(a))$ sont aussi racines de P .

Elles sont distinctes, car $a = R(a)$ est exclu d'après le 3), $a = R_2(a)$ implique (par composition par R) $R(a) = R^{(3)}(a)$, soit (d'après le 2.1)) $R(a) = a$ donc cas exclu aussi, et $R(a) = R^{(2)}(a)$ est aussi exclu car il implique (par composition par $R^{(2)}$) $R^{(3)}(a) = R(R^{(3)}(a))$ soit encore $a = R(a)$.

Reste à voir qu'elles sont racines de T , cad qu'elles sont distinctes de -1 et 2 .

Pour a c'est acquis par hypothèse ;

$R(a) = -1 \Leftrightarrow a^2 = 1$ ce qui est impossible car $a \neq -1$ et aussi $a \neq 1$ car 1 pas racine de T (puisque pas racine de P)

$R(a) = 2 \Leftrightarrow a^2 = 4$ ce qui est impossible car $a \neq 2$ et aussi $a \neq -2$ car -2 pas racine de T (puisque pas racine de P)

$R^{(2)}(a) = -1 \Leftrightarrow R^{(3)}(a) = R(-1) \Leftrightarrow a = -1$, ce qui est exclu

$R^{(2)}(a) = 2 \Leftrightarrow R^{(3)}(a) = R(2) \Leftrightarrow a = 2$, ce qui est exclu.

Donc $a, R(a), R^{(2)}(a)$ sont trois racines distinctes de T .

Montrons qu'elles sont simples.

Si aucune n'est simple c'est que $T(X) = (X - a)^2(X - R(a))^2(X - R^{(2)}(a))^2$ et

$T(X) = (X^3 + uX^2 + vX + w)^2$.

Or $T(X) = X^6 + X^5 - 5X^4 - 3X^3 + 7X^2 + X - 1$, d'où par identification des termes en X^5 , en X^2 , en X et du terme constant, on obtient

$2u = 1$, $v^2 + 2uw = 7$, $2vw = 1$, $w^2 = -1$, soit $v^2 = -\frac{1}{4}$, $-\frac{1}{4} + w = 7$ ce qui est contradictoire avec $w^2 = -1$.

Donc au moins une des trois racines $a, R(a), R^{(2)}(a)$ de T est simple : mais d'après le 3), R conserve la simplicité d'une racine de P , donc ces trois racines sont simples
 $(R(R(a))) = R^{(2)}(a)$, $R(R^{(2)}(a)) = R^{(3)}(a) = a$.

5)

5.1) Soit a une racine de T : d'après le 4), $a, R(a), R^{(2)}(a)$ sont trois racines distinctes et simples de T .

T étant de degré 6, il existe une racine b de T qui soit distinctes des trois précédentes et

d'après le 4), $b, R(b), R^{(2)}(b)$ sont trois racines distinctes et simples de T .

b a été choisi en dehors de $E = \{a; R(a); R^{(2)}(a)\}$: mais est-ce le cas de $R(b)$ et $R^{(2)}(b)$?

Notons que E est invariant par R , puisque $R^{(2)}(a) = a$.

Donc si $R(b) \in E$, par composition par $R^{(2)}$, b est dans E , ce qui est exclu, de même si $R^{(2)}(b) \in E$, par composition par R , b est dans E , ce qui est exclu, donc

$a, R(a), R^{(2)}(a), b, R(b), R^{(2)}(b)$ sont six racines distinctes de T , donc ce sont les six racines de T .

D'après le 2.2), $P'(a) = 8aR(a)R^{(2)}(a) - 1$ et $P'(b) = 8bR(b)R^{(2)}(b) - 1$; donc

$\frac{(P'(a) + 1)(P'(b) + 1)}{64}$ est le produit des six racines de T , et vu le terme constant de T est -1 , c'est que $(P'(a) + 1)(P'(b) + 1) = -64$.

5.2) Evident : par exemple les racines de U , à savoir $a, R(a), R^{(2)}(a)$ sont respectivement transformées par R en $R(a), R^{(2)}(a), R^{(3)}(a) = a$.

5.3) Pour toute r une racine de T on pose

$$s(r) = r + R(r) + R^{(2)}(r) = r + r^2 - 2 + r^4 - 4r^2 + 2 = r^4 - 3r^2 + r.$$

D'après le 5.2), pour tout $r \in \{a; R(a); R^{(2)}(a)\}$, $s(r)$ est invariant donc $s(r)$ prend une seule valeur notée m , à priori dans C .

De même pour tout $r \in \{b; R(b); R^{(2)}(b)\}$, $s(r)$ est invariant donc $s(r)$ prend une seule valeur notée n , à priori dans C .

Notons, à ce niveau que $m + n$ étant la somme des racines de T , $m + n = -1$.

Considérons $S(X) = (X^4 - 3X^2 + X - m)(X^4 - 3X^2 + X - n)$: les six racines de T sont donc racines de S et donc T divise S (du moins dans $C[X]$).

Donc il existe β et γ tels que

$$X^8 - 6X^6 + 2X^5 + (9 - (m + n))X^4 - 6X^3 + (1 + 3(m + n))X^2 - (m + n)X + mn \\ = (X^6 + X^5 - 5X^4 - 3X^3 + 7X^2 + X - 1)(X^2 + \beta X + \gamma), \text{ ce qui donne}$$

$$1 + \beta = 0, -5 + \beta + \gamma = -6, 7 - 3\beta - 5\gamma = 9 - (m + n), -\gamma = mn.$$

Donc $\beta = -1$, $\gamma = 0$ et $m + n = -1$ (ce que l'on avait déjà vu) et $mn = 0$.

Ainsi $\{m; n\} = \{-1; 0\}$ et donc

pour toute racine r de T , $s(r) = r + R(r) + R^{(2)}(r)$ est égal à -1 ou 0 .

5.4) D'après ce qui précède, T se factorise en un produit de deux facteurs unitaires du troisième degré, l'un des facteurs ayant pour somme de ses racines 0 que l'on notera U et l'autre ayant pour somme de ses racines -1 que l'on notera V .

Donc $T(X) = U(X)V(X)$ avec $U(X) = X^3 + sX + t$ et $V(X) = X^3 + X^2 + s'X + t'$ et par identification on obtient le système

$$s + s' = -5, s + t + t' = -3, ss' + t = 7, st' + s't = 1, tt' = -1.$$

D'où $s' = -s - 5$, $t' = -3 - s - t$, puis

$$s(-s - 5) + t = 7, s(-3 - s - t) + (-s - 5)t = 1, \text{ lesquelles donnent}$$

$$t = s^2 + 5s + 7 \text{ et } s^2 + 3s + 5t + 2st + 1 = 0 \text{ et finalement}$$

$$2s^3 + 16s^2 + 42s + 36 = 0, \text{ soit } (s + 3)^2(s + 2) = 0.$$

Donc, à priori, il y a deux possibilités pour s . Mais si $s = -2$, alors $s' = -3, t = 1$ et $U(X) = X^3 - 2X + 1$ qui a pour racine 1 qui n'est pas racine de T , donc la seule possibilité est en fait $s = -3$ qui donne $s' = -2, t = 1, t' = -1$ et ainsi $U(X) = X^3 - 3X + 1$ et $V(X) = X^3 + X^2 - 2X - 1$.

U et V n'ont pas de racine rationnelle, T en n'ayant pas, donc ils sont de degré 3 , ils sont irréductibles : la décomposition en facteurs irréductibles sur $\mathbb{Q}[X]$ de T est donc

$$T(X) = (X^3 - 3X + 1)(X^3 + X^2 - 2X - 1).$$

6) $R(2 \cos \theta) = 4 \cos^2 \theta - 2 = 4 \frac{\cos(2\theta) + 1}{2} - 2 = 2 \cos(2\theta)$ et donc

$$R^{(2)}(2 \cos \theta) = R(2 \cos(2\theta)) = 2 \cos(4\theta) ; \text{ de même } R^{(3)}(2 \cos \theta) = 2 \cos(8\theta).$$

Or $P(2 \cos \theta) = 0 \Leftrightarrow R^{(3)}(2 \cos \theta) = 2 \cos \theta$, d'après 2.1) ; et donc

$$P(2 \cos \theta) = 0 \Leftrightarrow \cos(8\theta) = \cos \theta.$$

On va voir que cela permet d'obtenir huit racines de P , donc toutes les racines de P , lesquelles sont donc toutes en fait de la forme $2 \cos \theta$.

En effet,

$$\cos(8\theta) = \cos \theta \Leftrightarrow 8\theta = \theta + 2k\pi \text{ ou } 8\theta = -\theta + 2k\pi$$

$$\Leftrightarrow \theta = \frac{2k\pi}{7} \text{ (cas 1) ou } \theta = \frac{2k\pi}{9} \text{ (cas 2)}.$$

Le cas 1 donne 7 points ($k = 0, 1, \dots, 6$) sur le cercle trigonométrique : $\theta = 0$ et six autres ayant le même cosinus 2 à 2

$$\frac{2\pi}{7} \text{ et } \frac{12\pi}{7} = 2\pi - \frac{2\pi}{7}, \frac{4\pi}{7} \text{ et } \frac{10\pi}{7} = 2\pi - \frac{2\pi}{7}, \frac{2\pi}{7} \text{ et } \frac{12\pi}{7} = 2\pi - \frac{2\pi}{7}, \text{ ce qui donne 4 racines distinctes de } P :$$

$$2, 2 \cos \frac{2\pi}{7}, 2 \cos \frac{4\pi}{7}, 2 \cos \frac{8\pi}{7}.$$

Le cas 2 donne 9 points ($k = 0, 1, \dots, 7$) sur le cercle trigonométrique : $\theta = 0$ et huit autres ayant le même cosinus 2 à 2

$$\frac{2\pi}{9} \text{ et } \frac{16\pi}{9} = 2\pi - \frac{2\pi}{9}, \frac{4\pi}{9} \text{ et } \frac{14\pi}{9} = 2\pi - \frac{4\pi}{9}, \frac{6\pi}{9} \text{ et } \frac{12\pi}{9} = 2\pi - \frac{6\pi}{9} \text{ (le cosinus est } \frac{-1}{2}), \frac{8\pi}{9} \text{ et } \frac{10\pi}{9} = 2\pi - \frac{8\pi}{9} \text{ ce qui donne 4 nouvelles racines distinctes de } P :$$

$$-1, 2 \cos \frac{2\pi}{9}, 2 \cos \frac{4\pi}{9}, 2 \cos \frac{8\pi}{9}.$$

On obtient donc huit racines de P , donc toutes les racines de P :

-1 et 2 qui sont les deux racines rationnelles de P

$$\text{et les six racines de } T : 2 \cos \frac{2\pi}{7}, 2 \cos \frac{4\pi}{7}, 2 \cos \frac{8\pi}{7}, 2 \cos \frac{2\pi}{9}, 2 \cos \frac{4\pi}{9}, 2 \cos \frac{8\pi}{9}.$$

En fait puisque $R(2 \cos \theta) = 2 \cos(2\theta)$ les six racines de T sont

$$2 \cos \frac{2\pi}{7}, R(2 \cos \frac{2\pi}{7}), R^{(2)}(2 \cos \frac{2\pi}{7}), 2 \cos \frac{2\pi}{9}, R(2 \cos \frac{2\pi}{9}), R^{(2)}(2 \cos \frac{2\pi}{9}) : \text{ on retrouve le 5.1.}$$

Reste à préciser quelles sont celles qui sont racines de $U(X) = X^3 - 3X + 1$ et celles racines de $U(X) = X^3 + X^2 - 2X - 1$ (définis au 5.4 par le fait que les racines de U sont de la forme $a, R(a), R^{(2)}(a)$ et sont de somme 0, alors que V a ses racines de la forme $b, R(b), R^{(2)}(b)$ mais elles sont de somme -1).

$$\text{En fait si } \theta = \frac{2\pi}{9} \text{ ou } \frac{4\pi}{9} \text{ ou } \frac{8\pi}{9} \text{ on a } \cos(3\theta) = \frac{-1}{2}, \text{ donc } 4 \cos^3 \theta - 3 \cos \theta = \frac{-1}{2}, \text{ soit } (2 \cos \theta)^3 - 3(2 \cos \theta)\theta + 1 = 0 :$$

$$\text{les racines de } U(X) = X^3 - 3X + 1 \text{ sont donc } 2 \cos \frac{2\pi}{9}, 2 \cos \frac{4\pi}{9}, 2 \cos \frac{8\pi}{9}, \text{ ce qui implique que celles de } U(X) = X^3 + X^2 - 2X - 1 \text{ sont } 2 \cos \frac{2\pi}{7}, 2 \cos \frac{4\pi}{7}, 2 \cos \frac{8\pi}{7}.$$

$$\text{Remarque 1 : } \cos \frac{8\pi}{7} = \cos \frac{6\pi}{7}$$

Remarque 2 : des termes constants de U et V on déduit que

$$\cos \frac{2\pi}{9} \cos \frac{4\pi}{9} \cos \frac{8\pi}{9} = \frac{-1}{8} \text{ et } \cos \frac{2\pi}{7} \cos \frac{4\pi}{7} \cos \frac{8\pi}{7} = \frac{1}{8} \square.$$

Annexe 2

Exercice sur la famille de polynômes $P_a(X) = X^3 - aX^2 - (a+3)X - 1$ pour $a \in \mathbb{Q}$

Cette famille apparaît (pour $a \geq -1$) dans un document de Daniel Shanks intitulé : The Simplest Cubic Fields dans Mathematics of Computation, vol 28, number 128, october 1974, pages 1137-1152.

On peut remarquer que $P_{-1} = \Psi_7$ (voir d'ailleurs le 3.9) et aussi que dans l'exercice précédent on a aussi rencontré le facteur $U(X) = \Psi_7$.

- 1) Montrer que pour tout $a \in \mathbb{Q}$, P_a est irréductible sur $\mathbb{Q}[X]$.
- 2) Déterminer le discriminant de P_a et montrer que P_a a trois racines réelles distinctes que l'on précisera à l'aide de la méthode de Viète (ref 2).

Cas $a = -\frac{3}{2}$.

3) On pose $F(X) = -\frac{1}{1+X}$

3.1) Déterminer $F \circ F(X) = F(F(X)) = F^{(2)}(X)$ puis $F^{(3)}(X)$. Quels sont les points fixes de F ?

3.2) Déterminer tous les polynômes de degré trois à coefficients réels et unitaires tels que $P(F(X)) = -\frac{P(X)}{(1+X)^3}$.

3.3) Montrer que pour tout $a \in \mathbb{Q}$, P_a est F -stable et que la permutation induite par F sur l'ensemble des racines de P_a est un 3-cycle.

Remarque : donc Ψ_7 est non seulement R -stable, mais il est aussi F -stable.

3.4) Déterminer, à un isomorphisme près, le groupe de Galois (sur \mathbb{Q}) de P_a pour $a \in \mathbb{Q}$.

4) Déterminer tous les polynômes de degré trois à coefficients complexes et unitaires tels que $P(F(X)) = c \frac{P(X)}{(1+X)^3}$ où c est une constante complexe distincte de -1 .

Vérifier que les polynômes obtenus sont F -stables ; préciser la permutation induite par F sur les racines de ces polynômes.

solution :

1) P_a n'a pas de racines rationnelles (si $r = \frac{p}{q}$, avec p, q entiers premiers entre eux, est racine de P_a , nécessairement $q = \pm 1$, donc r est un entier qui doit diviser 1, or -1 et 1 ne sont pas racines de P_a) et il est de degré ≤ 3 , donc P_a est irréductibles sur \mathbb{Q} .

2) Le discriminant de P_a est $D = (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2$ où les x_i sont les trois racines dans \mathbb{C} de P_a .

On réduit $P_a : Q_a(X) = P_a(X + \frac{a}{3}) = X^3 + pX + q$ avec

$$p = -\frac{a^2}{3} - a - 3 = -\frac{a^2 + 3a + 9}{3} \text{ et } q = -\frac{2a^3}{27} - \frac{a^2}{3} - a - 1 = -\frac{(2a+3)(a^2 + 3a + 9)}{27}.$$

Or le discriminant de Q_a est $-(4p^3 + 27q^2) = \frac{4(a^2 + 3a + 9)^3}{27} - \frac{(2a+3)^2(a^2 + 3a + 9)^2}{27}$,

soit $-(4p^3 + 27q^2) = (a^2 + 3a + 9)^2$ puisque $4(a^2 + 3a + 9) = (2a+3)^2 + 27$.

Et comme les racines de Q_a sont les translatées de celles de P_a , ces deux polynômes

ont le même discriminant.

En notant $\delta = a^2 + 3a + 9 > 0$, le discriminant de P_a est δ^2

Note : Shanks s'intéresse aux cas où δ est premier : $a = -1, 1, 2, 410$.

$4p^3 + 27q^2$ étant négatif, Q_a a trois racines réelles distinctes, donc P_a aussi.

En appliquant les formules de Viète (voir référence 2) les racines de Q_a sont

$$2\sqrt{\frac{-p}{3}} \cos \frac{\theta}{3}, 2\sqrt{\frac{-p}{3}} \cos \frac{\theta+2\pi}{3}, 2\sqrt{\frac{-p}{3}} \cos \frac{\theta+4\pi}{3}$$

$$\text{avec } \theta = \arccos \frac{3q}{2p\sqrt{\frac{-p}{3}}}.$$

$$\text{Comme } \sqrt{\frac{-p}{3}} = \frac{\sqrt{\delta}}{3}, \text{ on a } \theta = \arccos \frac{2a+3}{2\sqrt{\delta}} = \arccos \frac{2a+3}{\sqrt{(2a+3)^2 + 27}} \in]0; \pi[$$

Si $a = -\frac{3}{2}$, on a évidemment $\theta = \frac{\pi}{2}$.

Précisons, pour $a \neq -\frac{3}{2}$, θ en terme d'arctan.

Pour $2a+3 \neq 0$, posons $\theta' = \arctan \frac{\sqrt{27}}{2a+3} : \theta' \in]-\frac{\pi}{2}; \frac{\pi}{2}[$.

$$\cos^2 \theta' = \frac{1}{1 + \tan^2 \theta'} = \frac{(2a+3)^2}{4\delta}, \text{ donc } \cos \theta' = \pm \frac{2a+3}{2\sqrt{\delta}}.$$

D'où,

si $2a+3 > 0$, $\theta' \in]0; \frac{\pi}{2}[$ donc $\cos \theta' = \frac{2a+3}{2\sqrt{\delta}} = \cos \theta$ et $\theta = \theta'$ car θ et θ' dans $]0; \pi[$

si $2a+3 < 0$, $\theta' \in]-\frac{\pi}{2}; 0[$ donc $\cos \theta' = \frac{-(2a+3)}{2\sqrt{\delta}} = -\cos \theta$, soit $\cos \theta = \cos(\theta' + \pi)$ et

$\theta = \theta' + \pi$ car θ et $\theta' + \pi$ sont dans $]0; \pi[$.

Finalement les trois racines réelles de P_a sont

$$\frac{a}{3} + \frac{2\sqrt{\delta}}{3} \cos \frac{\theta}{3}, \frac{a}{3} + \frac{2\sqrt{\delta}}{3} \cos \frac{(\theta+2\pi)}{3}, \frac{a}{3} + \frac{2\sqrt{\delta}}{3} \cos \frac{(\theta+4\pi)}{3}$$

avec

$\delta = a^2 + 3a + 9 > 0$ et $\theta = \arccos \frac{2a+3}{2\sqrt{\delta}}$ (ou $\arctan \frac{\sqrt{27}}{2a+3}$ si $a > -\frac{3}{2}$, $\arctan \frac{\sqrt{27}}{2a+3} + \pi$ si $a < -\frac{3}{2}$).

Si $a = -\frac{3}{2}$ alors $\theta = \frac{\pi}{2}$, $\delta = \frac{27}{4}$ et les trois racines sont

$$-\frac{1}{2} + 2 \times \frac{3\sqrt{3}}{6} \cos \frac{\pi}{6} = 1, -\frac{1}{2} + 2 \times \frac{3\sqrt{3}}{6} \cos \frac{5\pi}{6} = -2 \text{ et } -\frac{1}{2} + 2 \times \frac{3\sqrt{3}}{6} \cos \frac{3\pi}{2} = -\frac{1}{2}$$

$$3.1) F^{(2)}(X) = -\frac{1+X}{X}; F^{(3)}(X) = X.$$

$F(x) = x \Leftrightarrow x^2 + x + 1 \Leftrightarrow x = j$ ou $x = j^2$: les points fixes de F sont imaginaires conjugués.

3.2) Pour $P(X) = X^3 + uX^2 + vX + w$,

$$P(F(X)) = -\frac{P(X)}{(1+X)^3} \Leftrightarrow \frac{-1 + u(1+X) - v(1+X)^2 + w(1+X)^3}{(1+X)^3} = \frac{-P(X)}{(1+X)^3}$$

Ce qui équivaut par identification des numérateurs à

$w = -1$, $3w - v = -u$, $3w - 2v + u = -v$, $w - v + u - 1 = -w$
 soit $w = -1$ et $u - v = 3$ c'est-à-dire $P = P_a$ avec $a = -u$.

3.3) Soit r une des trois racines de P_a , d'après le 3.2), $F(r) = -\frac{1}{1+r}$ et $F^{(2)}(r) = -\frac{1+r}{r}$
 sont aussi racines de P_a .

Vérifions qu'on obtient ainsi les trois racines de P_a , c'est-à-dire que $r, F(r), F^{(2)}(r)$ sont distinctes :

$F(r) = r$ est impossible car r est réel et les points fixes de F ne le sont pas

$F^{(2)}(r) = r \Rightarrow F^{(3)}(r) = F(r) \Rightarrow r = F(r)$ qui est impossible

$F^{(2)}(r) = F(r) \Rightarrow F^{(3)}(r) = F^{(2)}(r) \Rightarrow r = F^{(2)}(r)$ qui est impossible.

Donc les trois racines de P_a sont $\{r, F(r), F^{(2)}(r)\}$ avec $F(F^{(2)}(r)) = F^{(3)}(r) = r$: donc P_a est F -stable et la permutation induite par F sur l'ensemble des racines de P_a est un 3-cycle.

On vient de vérifier sur un autre exemple le 1)c.

Remarque : la somme des racines de P_a , est

$$r + F(r) + F^{(2)}(r) = r - \frac{1}{1+r} - \frac{1+r}{r} = \frac{r^3 - 3r - 1}{r^2 + r} = \frac{ar^2 + (a+3)r + 1 - 3r - 1}{r^2 + r} = a.$$

3.4) Je refais ici la preuve du 1)d dans le cas particulier P_a : l'ordre du groupe de Galois de P_a (noté $Gal(P_a)$) est le degré de l'extension $[N : Q]$ où N est le corps de décomposition de P_a .

Par définition N est le plus petit corps contenant Q et les trois racines de P_a , c'est donc $Q(r)$ où r est une racine quelconque de P_a , puisque les deux autres racines s'obtiennent rationnellement à partir de r .

Donc $[N : Q] = [Q(r) : Q] = 3$ car P_a est irréductible, et ainsi $Gal(P_a)$ est d'ordre 3 qui est un nombre premier, donc $Gal(P_a)$ est un groupe cyclique d'ordre 3.

Remarque : on a vu à la question 2 que le discriminant de P_a est le carré d'un rationnel, donc $Gal(P_a)$ doit être isomorphe à un sous-groupe de A_3 . C'est bien le cas, car A_3 est un groupe d'ordre 3 (c'est le seul sous-groupe d'ordre 3 de S_3), donc cyclique et deux sous-groupes cycliques de même ordre sont forcément isomorphes.

4) Par rapport à 3.2, on cherche cette fois les polynômes

$$P(X) = X^3 + uX^2 + vX + w \in \mathbb{C}[X] \text{ tels que } P\left(\frac{-1}{1+X}\right) = \frac{cP(X)}{(1+X)^3} \text{ où } c \text{ est une constante}$$

complexe autre que -1 .

On a cette fois le système

$$w = c, 3w - v = cu, 3w - 2v + u = cv, w - v + u - 1 = cw.$$

$$\text{Donc } (3-u)w = v, (3-v)w = 2v - u, w^2 - w + 1 = u - v.$$

$$\text{On en déduit } w(-u+v) = -v+u, \text{ soit } (v-u)(w+1) = 0.$$

Comme $w = c \neq -1$, nécessairement $u = v$ et $w^2 - w + 1 = 0$, soit $w = -j$ ou $w = -j^2$.

Donc ici, on ne trouve pas une infinité de polynômes, mais au plus deux polynômes.

si $w = -j$, de $(3-u)(-j) = u$ on tire $u = \frac{-3j}{1-j} = 1-j$ et alors on obtient

$$P(X) = X^3 + (1-j)(X^2 + X) - j \text{ dont les racines sont } j \text{ (double) et } j^2 \text{ (simple).}$$

si $w = -j^2$, on trouve $u = \frac{-3j^2}{1-j^2} = 1-j^2$ et alors on obtient

$$P(X) = X^3 + (1-j^2)(X^2 + X) - j^2 \text{ dont les racines sont } j \text{ (simple) et } j^2 \text{ (double).}$$

Réciproquement, on vérifie que ces deux polynômes conviennent, et comme les points

fixes de F sont j et j^2 , leur ensemble de racines qui est $\{j, j^2\}$ est conservé (élément par élément) par F : F induit la permutation identité sur leur ensemble de racines \square .