A PROPOS DE L'ÉQUATION CYCLOTOMIQUE $X^{11} - 1 = 0$

Jacques DAUTREVAUX (*)

A la suite de mon article "*Des équations qui déterminent les sections circulaires*" ('*L'Ouvert*' n° 46 et 47), M. DAUTREVAUX a bien voulu prendre le temps de détailler certains calculs et d'en dégager la structure en termes modernes de théorie des groupes. Qu'il en soit vivement remercié. Un tel éclairage n'est pas inutile pour comprendre en profondeur ce qui restait caché aux acteurs mêmes de ce qu'ils inventaient peu à peu, péniblement, à la manière de somnambules, pour reprendre un titre célèbre de A. KOESTLER. Veillons simplement à ne pas confondre ce point de vue avec le point de vue historique dans lequel se situe l'article en question. Celui-ci avait pour objectif de présenter aux lecteurs un certain nombre de **faits et de textes historiques** constitutifs du laborieux processus d'émergence d'un nouveau concept, d'un nouvel outil : la structure de groupe. Il est à placer dans la série d'articles commencée dans '*L'Ouvert*' avec le n° 44 par "*Le problème de la résolution des équations algébriques dans l'émergence du concept de groupe*", et dont le plus récent est celui d'Etienne KOEHLER sur "*Un mémoire fondateur de* CAUCHY" ('*L'Ouvert*' n° 49).

J.-P. FRIEDELMEYER

Une étude fort détaillée parue dans '*L'Ouvert*' n° 46 sous la signature de Jean-Pierre FRIEDELMEYER mentionne la méthode mise en œuvre par VANDERMONDE.

L'équation $x^{11} - 1 = 0$, dont les racines sont les onze racines onzièmes de l'unité se réduit après élimination de la racine 1 à l'équation cyclotomique $x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 0$, dont les racines sont les dix racines onzièmes de l'unité non réelles. Selon la méthode bien connue de traitement des équations dites *réciproques* on obtient en posant $u = x + \frac{1}{x}$ (0 n'étant pas racine), selon la notation utilisée de nos jours l'équation résolvante :

$$\text{(E)} \qquad u^5 + u^4 - 4u^3 - 3u^2 + 3u + 1 = 0$$

dont les cinq racines sont réelles car elles représentent deux fois les parties réelles des racines onzièmes de l'unité : l'ensemble de ces racines est donc l'ensemble $\{2\cos\frac{2\pi}{11}, 2\cos\frac{4\pi}{11}, 2\cos\frac{6\pi}{11}, 2\cos\frac{8\pi}{11}, 2\cos\frac{10\pi}{11}\}$.

Le calcul effectif de ces racines, montrant que les racines de l'équation binôme $x^n - 1 = 0$ (que n soit premier ou non) s'expriment par radicaux, laisse le lecteur quelque peu sur sa faim : l'expression explicite des racines fait en effet intervenir quatre quantités de la forme Δ, définies chacune comme racine cinquième d'un nombre complexe, donc avec cinq déterminations possibles : il y a donc un problème de coordination des déterminations à choisir pour les quatre quantités Δ intervenantes.

(*) Maître-Assistant honoraire – Université de Haute Alsace

A signaler toutefois que la quantité Δ^5 n'étant pas symétrique par rapport aux racines de l'équation, n'est donc pas **directement** calculable au moyen des fonctions symétriques élémentaires des racines, et que, par ailleurs, les cinq racines cinquièmes de l'unité ne sont linéairement indépendantes ni sur $\mathbb{Z}$ (le rang y est 4) ni sur $\mathbb{R}$ (le rang est 2), ce qui rend difficile la comparaison de calculs et de résultats obtenus par différentes techniques calculatoires.

Dans ce qui suit, je vais m'efforcer de conduire le calcul rigoureux des racines de l'équation (E) par la méthode précitée, et ensuite de voir comment éviter les artifices rencontrés.

Soit donc l'équation (E), dont les racines a, b, c, d, e sont individualisées de la façon suivante :

$$a = 2\cos\frac{2\pi}{11}\ ,\ b = 2\cos\frac{4\pi}{11}\ ,\ c = 2\cos\frac{8\pi}{11}\ ,$$
$$d = 2\cos\frac{6\pi}{11}\ ,\ e = 2\cos\frac{10\pi}{11}.$$

Des calculs trigonométriques simples donnent les relations de linéarisation suivantes :

$a^2 = b + 2$	$ab = a + d$	$ac = d + e$	$ad = b + c$	$ae = c + e$
	$b^2 = c + 2$	$bc = b + e$	$bd = a + e$	$be = c + d$
		$c^2 = d + 2$	$cd = a + c$	$ce = a + b$
			$d^2 = e + 2$	$de = b + d$
				$e^2 = a + 2$

et par ailleurs on a $a + b + c + d + e = -1$ (somme des racines de (E)).

On notera par ailleurs que, avec le choix ainsi fait de a, b, c, d, e on aura $-1 < e < c < d < 0 < b < a < 1$, classement qui nous sera utile à la fin pour découvrir les valeurs explicites de ces racines.

Considérons l'expression $\delta(r) = a + br + cr^2 + dr^3 + er^4$, dans laquelle r désigne une des racines cinquièmes de l'unité. Il est clair que $\delta(1) = -1$ et que, pour les quatre racines cinquièmes non réelles, qu'on peut noter $\omega, \omega^2, \omega^3, \omega^4$ (ω et ω^4 sont inverses, donc conjuguées, et de même ω^2 et ω^3), où ω est l'une quelconque d'entre elles, $\delta(r)$ prend quatre valeurs distinctes deux à deux conjuguées (car a, b, c, d, e sont réels) et on pourra alors écrire :

$$\begin{aligned}
a+b\ \ &+c\ \ &&+d\ \ &&+e\ \ &&= -1\\
a+b\omega\ &+c\omega^2 &&+d\omega^3 &&+e\omega^4 &&= \delta\\
a+b\omega^2 &+c\omega^4 &&+d\omega\ &&+e\omega^3 &&= \delta'\\
a+b\omega^3 &+c\omega\ &&+d\omega^4 &&+e\omega^2 &&= \overline{\delta'}\\
a+b\omega^4 &+c\omega^3 &&+d\omega^2 &&+e\omega\ &&= \overline{\delta}
\end{aligned}$$

La résolution de ce système donne immédiatement les valeurs de a, b, c, d, e lorsqu'on connaît δ et δ'.

Compte tenu de $1+\omega+\omega^2+\omega^3+\omega^4=0$, on voit facilement que l'on obtient :

$$a=\frac{1}{5}(-1+\delta+\delta'+\overline{\delta'}+\overline{\delta}) \qquad b=\frac{1}{5}(-1+\delta\omega^4+\delta'\omega^3+\overline{\delta'}\omega^2+\overline{\delta}w)$$
$$c=\frac{1}{5}(-1+\delta\omega^3+\delta'\omega+\overline{\delta'}\omega^4+\overline{\delta}\omega^2) \qquad d=\frac{1}{5}(-1+\delta\omega^2+\delta'\omega^4+\overline{\delta'}\omega+\overline{\delta}\omega^3)$$
$$e=\frac{1}{5}(-1+\delta w+\delta'\omega^2+\overline{\delta'}\omega^3+\overline{\delta}\omega^4)$$

ce qui résout complètement le problème à condition de connaître δ et δ'.

On peut observer aussi que :

$$\delta\overline{\delta}=(a+b\omega+c\omega^2+d\omega^3+e\omega^4)(a+b\omega^4+c\omega^3+d\omega^2+e\omega)$$

est une expression de la forme

$$A+B\omega+Cw^2+D\omega^3+E\omega^4$$

où

$$A=a^2+b^2+c^2+d^2+e^2=a+b+c+d+e+10=9$$
$$B=E=ab+bc+cd+de+ae=2(a+b+c+d+e)=-2$$
$$C=D=ac+ce+be+bd+ad=2(a+b+c+d+e)=-2$$

compte tenu des relations de linéarisation déjà vues, provenant de l'affectation à a,b,c,d,e des valeurs numériques précisées, soit :

$$\delta\overline{\delta}=9-2(\omega+\omega^2+\omega^3+\omega^4)=11 \text{ puisque } 1+\omega+\omega^2+\omega^3+\omega^4=0.$$

On a de même $\delta'\overline{\delta'}=11$ puisqu'il s'agit seulement du remplacement de ω par ω^2. Il en résulte que

$$\|\delta\|^2=\|\delta'\|^2=11.$$

On remarque que, par la permutation circulaire $(abcde)$ δ est transformé en $\delta\omega^4$, puis, en itérant cette transformation, successivement en $\delta\omega^3, \delta\omega^2$ et $\delta\omega$.

Il en résulte que l'expression $\Delta(r)=[\delta(r)]^5$ est invariante par la permutation circulaire $(abcde)$, donc par le groupe cyclique d'ordre 5 qu'elle engendre : $\Delta(r)$ ne prend donc que 24 valeurs distinctes correspondant aux $4!=24$ permutations possibles de l'ensemble $\{b,c,d,e\}$, un changement du choix de r parmi les 4 racines non réelles de l'unité $\{\omega,\omega^2,\omega^3,\omega^4\}$ étant équivalent à une permutation de l'ensemble $\{b,c,d,e\}$.

Calculons $\Delta(r)=[\delta(r)]^5=[a+br+cr^2+dr^3+er^4]^5$, pour un choix à préciser ultérieurement de r dans l'ensemble $\{\omega,\omega^2,\omega^3,\omega^4\}$, en utilisant les relations de linéarisation vues plus haut, provenant de l'affectation à a,b,c,d,e des valeurs numériques précisées.

On trouve tout d'abord :

$$\begin{aligned}[\delta(r)]^2 =&(2c - 2e - b) + (2a - 2c - e)r + (2d - 2a - c)r^2 \\ &+ (2b - 2d - a)r^3 + (2e - 2b - d)r^4 \\ =&(2r - 2r^2 - r^3)a + (-1 + 2r^3 - 2r^4)b + (2 - 2r - r^2)c \\ &+ (2r^2 - 2r^3 - r^4)d + (-2 - r + 2r^4)e \\ =&(2r - 2r^2 - r^3)(a + br^2 + cr^4 + dr + er^3) \\ =&(2r - 2r^2 - r^3)\delta(r^2)\end{aligned}$$

On a par suite la relation $\delta^2 = (2\omega - 2\omega^2 - \omega^3)\delta'$.

$2\omega - 2\omega^2 - \omega^3$ ayant pour conjugué $2\omega^4 - 2\omega^3 - \omega^2$, le carré de son module est

$$\begin{aligned}\|2\omega - 2\omega^2 - \omega^3\|^2 &= (2\omega - 2\omega^2 - \omega^3)(-\omega^2 - 2\omega^3 + 2\omega^4) \\ &= 9 - 2\omega - 2\omega^2 - 2\omega^3 - 2\omega^4 \\ &= 9 - 2(\omega + \omega^2 + \omega^3 + \omega^4) = 11\end{aligned}$$

et son inverse est $\frac{1}{11}(-\omega^2 - 2\omega^3 + 2\omega^4)$ de sorte que

$$\delta' = \frac{1}{11}(-\omega^2 - 2\omega^3 + 2\omega^4)\delta^2.$$

Il s'ensuit que la seule connaissance de δ (qui détermine ensuite $\overline{\delta}, \delta'$ et $\overline{\delta'}$) suffit pour obtenir les expressions explicites de a, b, c, d, e.

Continuons : $[\delta(r)]^3 = [\delta(r)]^2\delta(r) = (2r - 2r^2 - r^3)\delta(r^2)\delta(r)$ et, selon le même procédé que précédemment on obtient :

$$\begin{aligned}\delta(r^2)\delta(r) =&(2b - 2c - d) + (2d - 2e - a)r + (2a - 2b - c)r^2 \\ &+ (2c - 2d - e)r^3 + (2e - 2a - b)r^4 \\ =&(-r + 2r^2 - 2r^4)a + (2 - 2r^2 - r^4)b + (-2 - r^2 + 2r^3)c \\ &+ (-1 + 2r - 2r^3)d + (-2r - r^3 + 2r^4)e \\ =&(-r + 2r^2 - 2r^4)(a + br^3 + cr + dr^3 + er^2) \\ =&(-r + 2r^2 - 2r^4)\delta(r^3)\end{aligned}$$

et par suite

$$\begin{aligned}[\delta(r)]^3 &= (2r - 2r^2 - r^3)(-r + 2r^2 - 2r^4)\delta(r^3) \\ &= (-6 + 4r + 6r^3 - 3r^4)\delta(r^3)\end{aligned}$$

et la relation

$$\delta^3 = (-6 + 4\omega + 6\omega^3 - 3\omega^4)\overline{\delta'}.$$

Ensuite :

$$[\delta(r)]^4 = [\delta(r)]^3\delta(r) = (6r + 3r^2 + 10r^3 + r^4)\delta(r^3)\delta(r)$$

et comme précédemment :

$$\begin{aligned}\delta(r^3)\delta(r) =&(2b-2c-d)+(2a-2b-c)r+(2e-2a-b)r^2\\ &+(2d-2e-a)r^3+(2c-2d-e)r^4\\ =&(2r-2r^2-r^3)a+(2-2r-r^2)b+(-2-r+2r^4)c\\ &+(-1+2r^3-2r^4)d+(2r^2-2r^3-r^4)e\\ =&(2r-2r^2-r^3)(a+br^4+cr^3+dr^2+cr)\\ =&(2r-2r^2-r^3)\delta(r^4)\end{aligned}$$

et par suite :

$$\begin{aligned}[\delta(r)]^4 &= (-6+4r+6r^3-3r^4)(2r-2r^2-r^3)\delta(r^4)\\ &= (-18-12r+23r^2-2r^3+8r^4)\delta(r^4)\\ &= (6r+41r^2+16r^3+26r^4)\delta(r^4)\end{aligned}$$

et la relation :

$$\delta^4 = (6\omega+41\omega^2+16\omega^3+26\omega^4)\overline{\delta}.$$

Enfin :

$$\begin{aligned}[\delta(r)]^5 &= [\delta(r)]^4\delta(r) = (6r+41r^2+16r^3+26r^4)\delta(r^4)\delta(r)\\ &= 11(6r+41r^2+16r^3+26r^4)\end{aligned}$$

puisque $\delta(r)$ et $\delta(r^4)$ sont conjugués, leur produit est $\|\delta(r)\|^2 = 11$.

On a donc, dans les hypothèses précisées au début, et avec les valeurs numériques précisées pour a, b, c, d, e :

$$\Delta(r) = 11(6r+41r^2+16r^3+26r^4).$$

La fin du calcul est alors évidente.

Soient $\Delta = 11(6\omega+41\omega^2+16\omega^3+26\omega^4)$ et δ_0 l'une quelconque des déterminations de la racine cinquième du nombre complexe Δ : les quatre autres déterminations sont les nombres complexes $\delta_0 r, \delta_0 r^2, \delta_0 r^3$ et $\delta_0 r^4$, où r est l'une quelconque des racines cinquièmes non réelles de l'unité, pour laquelle il nous est loisible de prendre $r = \omega$.

On pose $\delta_0' = \frac{1}{11}(-\omega^2-2\omega^3+2\omega^4)\delta_0^2$: il en résulte qu'à $\delta_0\omega$ est associé $\delta_0'\omega^2$, à $\delta_0\omega^2$ est associé $\delta_0'\omega^4$, à $\delta_0\omega^3$ est associé $\delta_0'\omega$ et à $\delta_0\omega^4$ est associé $\delta_0'\omega^3$.

L'expression $\frac{1}{5}(-1+\delta+\delta'+\overline{\delta}+\overline{\delta'})$ est susceptible de prendre cinq valeurs différentes, résumées dans la formule :

$$x_i = \frac{1}{5}(-1+\delta_0\omega^i+\delta_0'\omega^{2i}+\overline{\delta_0'}\omega^{3i}+\overline{\delta_0}\omega^{4i}) \quad \text{avec } 0 \le i \le 4$$

(où les exposants $2i, 3i, 4i$ sont réduits modulo 5), et l'on voit alors sans peine que le quintuplet $(x_0, x_1, x_2, x_3, x_4)$ représente à une permutation circulaire près

le quintuplet (a, b, c, d, e) des racines cherchées; en fait c'est celui des x_i qui est l'élément maximal du quintuplet qui représente effectivement a; mais le classement des cinq valeurs attribuées aux racines cherchées a, b, c, d, e permet effectivement d'attribuer à chacune d'elles chacune des cinq valeurs trouvées.

Le calcul de $\Delta(\omega)$ est alors aisé, il en résulte cinq valeurs de δ d'où la formule $\frac{1}{5}(-1 + \delta + \delta' + \overline{\delta'} + \overline{\delta})$ fournit les cinq racines a, b, c, d, e dans un ordre dépendant du choix de la première détermination de δ et de l'ordre dans lequel sont prises les suivantes, mais, en raison de la symétrie de la formule, indépendant du choix initial de ω.

La méthode de calcul ainsi exposée donne lieu, en apparence, à des calculs assez aisés dont la raison principale aura été le choix d'une indexation convenable des racines de l'équation (E) : si on tente de refaire les calculs en intervertissant les valeurs numériques attribuées à deux des racines, a et b par exemple, on ne retrouve plus la lumineuse simplicité et la symétrie constatées. Si par exemple vous n'affectez pas de valeurs aux cinq racines a, b, c, d, e, vous pouvez calculer effectivement la quantité $\Delta(r)$ sous la forme $A + Br + Cr^2 + Dr^3 + Er^4$, dans laquelle chacun des coefficients A, B, C, D, E est effectivement invariant par toutes les permutations circulaires itérées du cyle $(abcde)$, mais seulement par celles-là et ne s'exprimant donc pas au moyen des fonctions symétriques élémentaires des racines de (E). A titre d'exemple, on obtient :

$$B = 5\Sigma a^4 b + 10\Sigma a^3 b^2 + 30\Sigma a^2 bd^2 + 20\Sigma abe^3 + 60\Sigma a^2 bde$$

où chaque Σ est étendu aux seules cinq permutations circulaires itérées de la permutation circulaire $(abcde)$. La raison essentielle du succès du mode de calcul adopté est que l'on a pu classer les cinq racines de (E) selon la formule $u_k = 2\cos\frac{2^{k+1}\pi}{11}$, où k décrit l'ensemble $\{0, 1, 2, 3, 4\}$: $a = u_0$, $b = u_1$, $c = u_2$, $d = u_3$, $e = u_4$ et que cela assure que le tableau des relations de linéarisation est de la sorte invariant par les cinq permutations itérées de la permutation circulaire $(abcde)$. Ce fait est général pourvu que les racines u_k soient indexées par les exposants d'un générateur du groupe multiplicatif $(\mathbb{Z}/11\mathbb{Z})^*$, groupe cyclique, ici d'ordre 10.

Soit donc n premier impair, avec $n = 2p+1$. L'équation $x^n - 1 = 0$ après élimination de la seule racine réelle 1 se réduit à l'équation cyclotomique $x^{n-1} + x^{n-2} + \cdots + x + 1 = 0$ dont les $n - 1$ racines, non réelles, sont les racines n-ièmes de l'unité autres que 1, qui, n étant premier, sont toutes primitives (il est inutile, on le sait, de faire l'étude lorsque n est composé, car on se ramène en fait, à une succession d'équations binômes de degré premier). Si ω est l'une d'elles, l'ensemble de ces racines peut être représenté par ω^k, où k décrit l'ensemble des éléments autres que 0 dans le corps (puisque n est premier) $\mathbb{Z}/n\mathbb{Z}$, d'où l'idée de base commune aux méthodes de GAUSS et de LAGRANGE, qui est d'associer les racines cherchées aux éléments du groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$, lequel est, on le sait, cyclique, en écrivant ces $n - 1$ racines (cet entier est pair) sous la forme : $x_k = e^{ig^k\alpha}$, où

$\alpha = \frac{2\pi}{n}$ et g un générateur du groupe cyclique $(\mathbb{Z}/n\mathbb{Z})^*$. Le conjugué (ou, si l'on veut, l'inverse) de x_k est un $x_{k'}$ tel que l'on ait, modulo n, $g^k + g^{k'} = 0$, ou encore $g^{|k-k'|} = -1$. Puisque g est générateur, on a : $g^{n-1} = g^{2p} = 1$ (c'est le "*petit*" théorème de FERMAT), on a: $g^{2p} - 1 = (g^p - 1)(g^p + 1) = 0$, soit, puisque $\mathbb{Z}/n\mathbb{Z}$ est un corps et que $g^p - 1 \neq 0$ (sinon g ne serait pas générateur), $g^p + 1 = 0$, et p est évidemment l'exposant de g qu'il nous faut, de sorte que $\overline{x_k} = x_{k+p}$, et on retrouve alors bien que :

$$\overline{x_k} = e^{ig^{k+p}\alpha} = e^{-ig^k\alpha} \text{ puisque } g^p = -1.$$

On est ainsi amené à décrire les $2p$ racines de l'équation cyclotomique $x^{n-1} + x^{n-2} + \cdots + x + 1 = 0$ en deux suites de racines conjuguées respectivement $\{x_k\}$ et $\{x_{k+p}\}$ où k décrit l'ensemble $\{0, 1, 2, \ldots, p-1\}$. Selon la méthode traditionnelle, cela revient à regrouper les racines deux par deux selon la transformation $u = x + \frac{1}{x}$ (dans la théorie de GAUSS, ces regroupements correspondent aux éléments du groupe-quotient de $(\mathbb{Z}/n\mathbb{Z})^*$ selon le sous-groupe d'ordre 2 engendré par $g^p = -1$).

Il n'y a rien de mystérieux donc à écrire les racines de l'équation résolvante en u (polynôme de degré p que l'on sait écrire dans le cas général en fonction de n) sous la forme $u_k = 2\cos g^k\alpha$, avec $\alpha = \frac{2\pi}{n}$.

Les relations de linéarisation s'écrivent alors aisément : $u_k^2 = 4\cos^2 g^k\alpha = 2(1 + \cos 2g^k\alpha) = 2 + u_{k+j}$ car 2 étant un élément de $(\mathbb{Z}/n\mathbb{Z})^*$ on est assuré de trouver un j tel que $2 = g^j$, et de même pour les mêmes raisons :

$$u_i u_j = 4\cos g^i\alpha \cos g^j\alpha = 2(\cos(g^i + g^j)\alpha + \cos(g^i - g^j)\alpha) = u_k + u_{k'},$$

où

$$g^i + g^j = g^k \text{ ou } g^{k+p} \text{ et } g^i - g^j = g^{k'} \text{ ou } g^{k'+p}.$$

Il est alors clair que l'ensemble des formules de linéarisation ainsi obtenues est invariant par toutes les permutations de $\{0, 1, 2, \ldots, p-1\}$ itérées de la permutation circulaire $(0\ 1\ 2\ \ldots p-1)$, tant il semble évident que $u_{k+1}^2 = 2 + u_{k+j+1}$ et $u_{i+1}u_{j+1} = u_{k+1} + u_{k'+1}$.

De là la méthode de VANDERMONDE, consistant à poser :

$$\delta(r) = \sum_{i=0}^{p-1} u_i r^i,$$

où r est une racine p-ième de l'unité ($r^p = 1$). On a évidemment $\delta(1) = -1$; et si ω est une racine p-ième **primitive** de l'unité, on obtiendra entre les u_i $p-1$ autres équations de la forme :

$$\delta_k = \sum_{i=0}^{p-1} u_i \omega^{ki}$$

où tous les δ_j peuvent se calculer à partir de l'un d'eux, δ_1 par exemple. Si on remarque en outre que $\Delta(r) = [\delta(r)]^p$ est invariant par toutes les permutations de $\{0, 1, 2, \ldots, p-1\}$ itérées de la permutation circulaire $(0, 1, 2, \ldots, p-1)$, le calcul de $\Delta(\omega)$ en utilisant les relations de linéarisation conduira à une expression de type linéaire ayant de type d'invariance, donc nécessairement de la forme :

$$\Delta(\omega) = \sum_{i=0}^{p-1} A_i \omega^i, \text{ où } A_i = K_i + L_i \sum_{j=0}^{p-1} u_j = K_i - L_i.$$

Les p déterminations de la racine p-ième de $\Delta(\omega)$ fournissent alors les p racines cherchées $u_0, u_1, u_2, \ldots, u_{p-1}$ à une permutation circulaire près, ainsi qu'il a été observé sur l'exemple traité $n = 11$. La plupart des particularités observées étaient dans ce cas masquées par le fait que $p = 5$ est premier et aussi que 2 est générateur du groupe $(\mathbb{Z}/11\mathbb{Z})^*$. Si on essaie de reprendre le calcul pour $n = 17$ selon cette méthode, on verra les racines u_i se regrouper par 4, puis par 2 selon les sous-groupes de $(\mathbb{Z}/17\mathbb{Z})^*$, groupe d'ordre $16 = 2^4$ dont 2 n'est pas un générateur (il faut prendre 3 par exemple).

Exemple : Le cas $n = 13$.

Le groupe $(\mathbb{Z}/13\mathbb{Z})^*$ est d'ordre 12; un de ses générateurs est 2, de sorte que les racines u_k de l'équation résolvante $u^6 + u^5 - 5u^4 - 4u^3 + 6u^2 + 3u - 1 = 0$ peuvent s'écrire $u_k = 2\cos 2^k\alpha$, où $\alpha = \frac{2\pi}{13}$ et où l'entier k décrira l'ensemble $\{0, 1, 2, 3, 4, 5, 6\}$ en vertu du tableau des valeurs de 2^k modulo 13, qui définissent l'indexation des racines x_k de l'équation cyclotomique en x (de degré 12) :

$k =$	0	1	2	3	4	5	6	7	8	9	10	11	12
$2^k =$	1	2	4	−5	3	6	−1	−2	−4	5	−3	−6	1
	x_0	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}	

Le groupe cyclique $(\mathbb{Z}/13\mathbb{Z})^*$, d'ordre 12, de générateur 2, contient trois sous-groupes, cycliques aussi, d'ordre 2 (engendré par -1), 4 (engendré par 5) et 6 (engendré par 4).

Le sous-groupe d'ordre 2 partage le groupe complet en six classes composées chacune de deux éléments et qui sont :

$$\{1, -1\}, \{2, -2\}, \{4, -4\}, \{-5, 5\}, \{3, -3\} \text{ et } \{6, -6\},$$

ce qui correspond à un partage de l'ensemble des douze racines x_k en six groupes de deux $\{x_0, x_6\}, \{x_1, x_7\}, \{x_2, x_8\}, \{x_3, x_9\}, \{x_4, x_{10}\}$ et $\{x_5, x_{11}\}$, tous de la forme $\{x_k, x_{k+6}\}$ avec $x_k x_{k+6} = 1$ et $x_k + x_{k+6} = u_k$: quand on connaît les six u_k, x_k et x_{k+6} sont obtenus comme racines de l'équation du second degré $x^2 - u_k x + 1 = 0$:

on obtient ainsi la raison profonde de la transformation $u = x + \frac{1}{x}$ qui, appliquée classiquement à l'équation cyclotomique $x^{12} + x^{11} + x^{10} + \cdots + x^2 + x = 0$ donne comme résolvante l'équation en u : $u^6 + u^5 - 5u^4 - 4u^3 + 6u^2 + 3u + 1 = 0$, de degré 6, dont le groupe "*pilotant*" les racines est le groupe-quotient de $(\mathbb{Z}/13\mathbb{Z})^*$ par son sous-groupe $\{1, g^6\}$ d'ordre 2. G est un groupe cyclique d'ordre 6 engendré par l'élément $\overline{2} = \{2, -2\}$ qu'on peut assimiler à 2 (au signe près — si l'on peut dire car il s'agit d'entiers modulo 13 —); il contient un sous-groupe C d'ordre 2 contenant les éléments 1 et 5 et un sous-groupe d'ordre 3 contenant les éléments 1, 3 et 4 (isomorphe au quotient de G par le premier de ces sous-groupes).

Posant $\alpha = \frac{2\pi}{13}$ on a : $u_k = 2\cos 2^k\alpha$, ce qui permet d'établir, d'une part les quatre relations de linéarisation :

$$u_0^2 = u_1 + 2\ ,\ u_0u_1 = u_0 + u_4\ ,\ u_0u_2 = u_3 + u_4 \text{ et } u_0u_3 = u_2 + u_5$$

dont toutes les autres se déduisent par des permutations circulaires itérées du cycle (0 1 2 3 4 5), et d'autre part la relation $u_{k+1} = u_k^2 - 2$ qui permet d'obtenir à partir de l'une d'elles, les six racines dans l'ordre $u_0, u_1, u_2, u_3, u_4, u_5$ **à une permutation circulaire près**, ce qui n'est pas une réelle difficulté car il est facile de positionner u_0 sachant que u_0 est (toujours) la plus grande des racines, ainsi qu'on le voit aisément.

Le quotient de G par son sous-groupe d'ordre 2 comporte trois éléments auxquels sont associées les trois paires $\{u_0, u_3\}, \{u_1, u_4\}$ et $\{u_2, u_5\}$ de racines. Posant $v_k = u_k + u_{k+3}$ $(k \in \{0, 1, 2\}$, entier modulo 3) on voit que, si on connaît v_0, v_1 et v_2, u_k et u_{k+3} sont les racines de l'équation du second degré $u^2 - v_ku + v_{k+2} = 0$.

On détermine aisément pour les v_k des relations de linéarisation analogues à celles des u_k, se déduisant des deux suivantes :

$$v_0^2 = 3 - v_0 + v_2 \text{ et } v_0v_1 = v_1 - 1$$

par toutes les permutations circulaires itérées du cyle (0 1 2).

De $v_0 + v_1 + v_2 = -1$ on tire $v_0^2 + v_0v_1 + v_0v_2 = -v_0 = v_0^2 + v_0 + v_1 - 2$, ce qui donne $v_1 = -v_0^2 - 2v_0 + 2$, puis $v_2 = v_0^2 + v_0 - 3$. Comme $v_0v_2 = v_0 - 1 = v_0^3 + v_0^2 - 3v_0$ on a $v_0^3 + v_0^2 - 4v_0 + 1 = 0$, équation à laquelle satisfont aussi v_1 et v_2 car elle est invariante par toute permutation circulaire itérée du cycle (0 1 2). On obtient ainsi l'équation du troisième degré $v^3 + v^2 - 4v + 1 = 0$ dont les trois racines sont v_0, v_1 et v_2, équation qu'on aurait pu former directement en calculant au moyen des formules de linéarisation les fonctions symétriques élémentaires des trois racines v_0, v_1, v_2. La résolution de cette équation donne effectivement les valeurs numériques des trois racines, sans qu'on aie la possibilité *a priori* de les affecter aux trois quantités v_0, v_1 et v_2 parfaitement définies.

Du fait qu'il suffit, ainsi qu'on a vu, de connaître l'une quelconque des racines u_k, la méthode se simplifie finalement beaucoup et se ramène à calculer **une** racine v de l'équation du troisième degré $X^3 + X^2 - 4X + 1 = 0$, et **une** racine u de l'équation du second degré $X^2 - vX + v^2 + v - 3 = 0$.

Cette racine u est l'un des u_k, et l'utilisation itérée de la relation $u_{k+1} = u_k^2 - 2$ ($k \in \{0,1,2,3,4,5\}$, entier modulo 6) permet d'obtenir, ainsi qu'il a été vu, les affectations exactes à $u_0, u_1, u_2, u_3, u_4, u_5$ des six valeurs numériques ainsi obtenues.

Remarque : la méthode de calcul de LEGENDRE est elle-même applicable à la résolution de l'équation du troisième degré $v^3 + v^2 - 4v + 1 = 0$. Appelant j, selon l'usage, l'une des racines cubiques primitives de l'unité, et posant $\delta = v_0 + jv_1 + j^2v_2$, on a $\overline{\delta} = v_0 + j^2v_1 + jv_2$, et comme $v_0 + v_1 + v_2 = -1$, l'une des racines (ici v_0) serait $v = \frac{1}{3}(-1 + \delta + \overline{\delta})$. Un calcul aisé, utilisant les formules de linéarisation des v_k, montre que :

$$\delta\overline{\delta} = 13\ ,\ \delta^2 = (-1 + 3j^2)\overline{\delta} \text{ et enfin } \delta^3 = 13(-1 + 3j^2).$$

Il s'ensuit que, pour obtenir l'une, v, des racines, il suffit de prendre pour δ l'une des trois racines cubiques de $\Delta = 13(-1 + 3j^2)$.

On aurait évidemment pu procéder dans l'ordre inverse,c'est-à-dire partir du sous-groupe d'ordre 3 de G : le groupe quotient correspond aux deux triplets $\{u_0, u_2, u_4\}$ et $\{u_1, u_3, u_5\}$ de racines u_k. Posant :

$$y_0 = u_0 + u_2 + u_4 \text{ et } y_1 = u_1 + u_3 + u_5 \text{ on a } : y_0 + y_1 = -1 \text{ et } y_0y_1 = -3$$

(ainsi qu'il résulte des relations de linéarisation), de sorte que y_0 et y_1 sont les racines de l'équation du second degré $X^2 + X - 3 = 0$, mais sans qu'on dispose du moyen *a priori* d'attribuer à y_0 et à y_1 l'une et l'autre des valeurs numériques trouvées pour ces deux racines : si l'on désigne l'une d'elles par y, l'autre est naturellement $-y - 1$ (leur somme étant -1).

Le calcul (au moyen des relations de linéarisation) des fonctions symétriques élémentaires de u_0, u_2 et u_4 montre que ces trois quantités sont racines de l'équation du troisième degré : $u^3 - y_0u^2 - u - (y_1 + 2) = 0$, sous réserve que y ait effectivement la valeur numérique à attribuer à y_0, sinon on obtient les racines u_1, u_3 et u_5. Mais comme tout à l'heure, la relation $u_{k+1} = u_k^2 - 2$ nous tire d'affaire car il suffit alors de connaître l'une quelconque des racines u_k. Dès lors, il suffit de calculer d'abord l'une, y, des racines de $X^2 + X - 3 = 0$, puis l'une, u, des racines de $X^3 - yX^2 - X + y - 1 = 0$. Pour cette dernière équation la méthode de LEGENDRE est utilisable, mais les calculs sont plus complexes et conduisent à $u = \frac{1}{3}(y + \delta + \overline{\delta})$, où δ serait l'une des racines cubiques de $3(4 + j^2) - 2(4 + 3j)y$, ce qui rend préférable la première méthode exposée.

Pour en savoir plus, le lecteur consultera avec fruit les chapitres consacrés aux équations abéliennes dans le "*Cours d'Algèbre Supérieure*" de J.-A. SERRET (Gauthier-Villars, 1877). LEGENDRE a, lui aussi, consacré à la résolution de l'équation binôme $X_n - 1 = 0$ (pour n premier) toute une partie de sa "*Théorie des Nombres*" (Paris 1830, réédité en 1955 chez Blanchard).