NOUVELLES ANNALES DE MATHÉMATIQUES

S. RÉALIS

De la résolution algébrique de l'équation $x^p - 1 = 0$, quand l'exposant p est un nombre premier

Nouvelles annales de mathématiques 1re série, tome 2 (1843), p. 5-16

<http://www.numdam.org/item?id=NAM_1843_1_2__5_0>

NOUVELLES ANNALES

DE

MATHÉMATIQUES.

ALGÈBRE SUPÉRIEURE.

DE LA RÉSOLUTION ALGÉBRIQUE DE L'ÉQUATION $x^p - 1 = 0$, QUAND L'EXPOSANT p EST UN NOMBRE PREMIER.

PAR M. REALIS. (S.)

I.

Cas particuliers.

1. Le but que je me propose dans ce mémoire est de prouver que « toute équation à deux termes, dont l'exposant est un nombre premier, peut être décomposée rationnellement en d'autres équations, dont les degrés sont marqués par les facteurs premiers du nombre qui précède d'une unité ce nombre premier, » et de développer en même temps une méthode nouvelle et simple pour effectuer la décompo sition indiquée.

2. La considération des propriétés du cercle donne, pour tous les degrés, des expressions des racines de l'unité, au moyen desquelles on peut parvenir à la résolution algébrique

de l'équation $x^p - 1 = 0$; c'est pourquoi je rappellerai que les racines de cette équation sont données par la formule

$$x = \cos\frac{2k\pi}{p} \pm \sqrt{-1}\sin\frac{2k\pi}{p},$$

dans laquelle on doit donner à k les valeurs 0, 1, 2, 3,..... $\frac{p}{2}$ si p est pair, et les valeurs 0, 1, 2, 3,..... $\frac{p-1}{2}$ si p est impair. Dans le premier cas les deux valeurs extrêmes de k donnent $x = 1, x = -1$, et toutes les autres valeurs de x sont imaginaires, conjuguées et réciproques. Dans le second cas, la première valeur de k donne $x = 1$; les autres racines sont toutes imaginaires, conjuguées et réciproques.

3. Après avoir délivré l'équation $x^p - 1 = 0$ du facteur $x - 1$, on ramène, par la méthode connue, l'équation résultante

$$x^{p-1} + x^{p-2} + x^{p-3} + x^{p-4} + \dots . + x + 1 = 0$$

à une équation du degré $\frac{p-1}{2}$, en y faisant $x + \frac{1}{x} = z$. De cette manière les racines de l'équation en z seront

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

et serviront à déterminer les $\frac{p-1}{2}$ facteurs de la forme $x^2 - zx + 1$ qu'admet l'équation $x^p - 1 = 0$.

C'est dans la recherche des expressions algébriques de ces racines que consiste le problème de la résolution des équations binômes, auquel revient, ainsi qu'on le voit, celui de la division du cercle en parties égales.

La résolution de quelques équations particulières éclaircira la théorie générale que j'exposerai à la suite.

4. Soit d'abord $p=13$; l'équation $x^{13}-1=0$ conduit à

$$z^6+z^5-5z^4-4z^3+6z^2+3z-1=0,$$

dont les racines sont

$$z=2\cos\frac{2\pi}{13},\ 2\cos\frac{4\pi}{13},\ 2\cos\frac{6\pi}{13},\ 2\cos\frac{8\pi}{13},\ 2\cos\frac{10\pi}{13},\ 2\cos\frac{12\pi}{13}.$$

Une équation peut être abaissée à un degré inférieur à celui sous lequel elle se présente, quand il existe entre ses racines des relations particulières. S'il n'y a que deux racines qui soient liées par une relation connue, on sépare de l'équation un diviseur du premier degré qui contient l'une ou l'autre de ces deux racines. Si toutes les racines, en nombre $2n$, peuvent se distribuer par couples de manière qu'elles aient, deux à deux, une même relation donnée, on peut, au moyen d'équations du degré n, décomposer la proposée en ses facteurs du second degré : c'est ainsi qu'on abaisse l'équation $x^p-1=0$, divisée par $x-1$, au degré $\frac{p-1}{2}$. Si les racines, en nombre $3n$, sont assujetties, trois par trois, à une relation donnée, on peut, au moyen d'équations du $n^{ième}$ degré, décomposer la proposée en des facteurs du troisième degré, etc. (*V.* Lacroix, *Compl. des élém. d'Algèbre*, nos 58 et 59, 6e édit.)

Dans le cas qui nous occupe, on voit que les valeurs de z sont liées entre elles de telle sorte que si u en désigne la première, les autres sont

$$u^2-2;\ u^3-3u;\ u^4-4u^2+2;\ u^5-5u^3+5u;\ u^6-6u^4+9u^2-2,$$

ainsi qu'on le déduit de la formule générale qui donne le cosinus du multiple d'un arc en fonction du cosinus de l'arc simple. Il ne faut pas conclure de là cependant que l'équation en z puisse être immédiatement abaissée; les relations ci-dessus demeurant les mêmes soit que la lettre u désigne la première racine, soit une autre racine quelconque, il s'ensuit que si l'on met, par exemple, z^2-2 à la place de z dans l'équation, et qu'on cherche le commun diviseur qui doit exister entre l'équation résultante et la proposée, ce commun diviseur montera au sixième degré et ne sera autre chose que le premier membre de la proposée elle-même.

On ne réussira pas non plus à abaisser le degré de l'équation en z, en la décomposant au hasard en des facteurs du second degré contenant des racines assujetties dans chacun d'eux à une même relation, car cette décomposition pourra généralement s'effectuer de deux manières différentes, et les équations d'où elle dépend monteront encore au sixième degré.

Je suppose, par exemple, qu'on veuille décomposer en trois facteurs de la forme

$$z^2-(2\cos\varphi+2\cos 2\varphi)z+2\cos\varphi\,.\,2\cos 2\varphi\ :$$

On pourra prendre les trois facteurs contenant respectivement les couples de racines

$$2\cos\frac{2\pi}{13},\,2\cos\frac{4\pi}{13};\quad 2\cos\frac{8\pi}{13},\,2\cos\frac{10\pi}{13};\quad 2\cos\frac{6\pi}{13},\,2\cos\frac{12\pi}{13};$$

ou bien les facteurs contenant les couples

$$2\cos\frac{10\pi}{13},\,2\cos\frac{6\pi}{13};\quad 2\cos\frac{12\pi}{13},\,2\cos\frac{2\pi}{13};\quad 2\cos\frac{4\pi}{13},\,2\cos\frac{8\pi}{13};$$

et par conséquent les équations que donnerait la méthode ordinaire d'abaissement pour déterminer les deux fontions

$$2\cos\frac{2\pi}{13}+2\cos\frac{4\pi}{13},\quad 2\cos\frac{2\pi}{13}.\ 2\cos\frac{4\pi}{13},$$

considérées comme des inconnues, seraient du sixième degré.

On voit maintenant que si l'on pouvait parvenir à combiner les racines deux à deux de manière qu'elles eussent dans chaque couple une même relation connue, et que les deux décompositions en facteurs du second degré rentrassent l'une dans l'autre, on réduirait par là de moitié le nombre de valeurs différentes des fonctions qui déterminent ces facteurs et le degré des équations d'où elles dépendent.

Soit m un nombre tel que l'équation puisse se décomposer en deux facteurs de la forme

$$z^2-(2\cos\varphi+2\cos m\varphi)z+2\cos\varphi.\,2\cos m\varphi\,:$$

tant que $\cos m^2\varphi$ aura une valeur différente de $\cos\varphi$, on pourra aussi décomposer l'équation en des facteurs de la forme

$$z^2-(2\cos m\varphi+2\cos m^2\varphi)z+2\cos m\varphi.\,2\cos m^2\varphi,$$

qui contiennent des racines liées dans chacun d'eux par la même relation que celles des premiers, et pour les déterminer on tombera sur des équations du même degré que la proposée. Mais si l'on avait $\cos m^2\varphi=\cos\varphi$, les deux décompositions se réduiraient à une seule, ce qui abaisserait les équations ci-dessus au troisième degré. Cela sera développé plus bas (*Théorie générale*); en attendant, j'observerai que le nombre m qui donne $\cos m^2\varphi=\cos\varphi$, φ étant de la forme $\frac{2\alpha\pi}{13}$, doit satisfaire à la condition de rendre entière la quantité $\frac{m^2+1}{13}$ ou la quantité $\frac{m^2-1}{13}$, et qu'ainsi c'est de la résolution de l'équation indéterminée $\frac{m^2\pm1}{13}=$ entier que dépend sa détermination.

On voit de suite que $m=5$ est le nombre cherché; et en effet, il n'y a qu'une seule manière de décomposer l'équation en z en des facteurs de la forme

$$z^2-(2\cos\varphi+2\cos5\varphi)z+2\cos\varphi.\,2\cos5\varphi,$$

savoir par les facteurs qui contiennent les trois couples de racines

$$2\cos\frac{2\pi}{13},\ 2\cos\frac{10\pi}{13};\quad 2\cos\frac{4\pi}{13},\ 2\cos\frac{6\pi}{13};\quad 2\cos\frac{8\pi}{13},\ 2\cos\frac{12\pi}{13}.$$

Le procédé ordinaire d'abaissement se simplifie beaucoup à l'égard des équations en z qu'on tire des équations binômes dont il est question ici.

Dans l'équation ci-dessus en z, u étant une quelconque des racines, celle qui lui correspond dans le même facteur du second degré, est u^5-5u^3+5u (*voy.* page 7), de façon que ce facteur est de la forme

$$z^2-(u^5-5u^3+6u)z+u^6-5u^4+5u^2,$$

les fonctions u^5-5u^3+6u, $u^6-5u^4+5u^2$ devant être données par des équations du troisième degré. Voici comment on peut parvenir au résultat par une seule opération, sans avoir à s'occuper séparément de chacune de ces fonctions.

Soit $u^5-5u^3+6u=y$, ou ce qui est la même chose,

$$u^5-5u^3+6u-y=0;$$

si dans cette équation on mettait pour y une quelconque de ses trois valeurs, censées connues, elle devrait être vérifiée par deux valeurs de u et s'accorder avec l'équation

$$u^6+u^5-5u^4-4u^3+6u^2+3u-1=0$$

qu'on obtient en écrivant u à la place de z dans la proposée : il doit donc exister entre ces deux équations un commun diviseur. Si l'on procède à la recherche de ce commun diviseur, on doit *nécessairement* rencontrer un polynôme *du troisième degré* en y qui, égalé à zéro, servira à déterminer les trois valeurs de y et à rendre diviseur commun des deux équations un polynôme *du second degré* en u.

On trouve, en effet, que le trinôme $u^2-yu-\dfrac{y^2-2}{y-1}$ divise les deux équations si l'on fait

$$y^3+y^2-4y+1=0.$$

On voit que le commun diviseur, sauf le changement de z en u, n'est autre chose que le facteur du second degré qu'il s'agissait de déterminer, et qu'en y mettant successivement à la place de y les trois racines de la dernière équation, on obtient précisément les trois facteurs dans lesquels se décompose la proposée, et qu'on est ainsi dispensé de s'occuper à part de la fonction $u^6-5u^4+5u^2$. On peut faire disparaître le dénominateur du dernier terme du commun diviseur, car de l'équation en y on déduit $-\dfrac{y^2-2}{y-1}=y^2+y-3$

La résolution de l'équation $x^{13}-1=0$ se réduit donc à celle des trois équations combinées

$$x^2-zx+1=0\,;\quad z^2-yz+y^2+y-3=0\,,\quad y^3+y^2-4y+1=0.$$

5. L'équation en z qu'on vient de traiter peut aussi se décomposer en deux facteurs de la forme

$$z^3-(2\cos\varphi+2\cos m\varphi+2\cos m^2\varphi)\,z^2+(\ldots\ldots)z+(\ldots\ldots).$$

Tant qu'on ne choisit pas convenablement le nombre m, à chaque manière qu'on trouvera d'effectuer cette décomposition, il en correspondra deux autres distinctes, de sorte que pour déterminer les coefficients des termes du facteur on tombera sur des équations du sixième degré; mais si m est tel qu'on ait $\cos m^3\varphi=\cos\varphi$, ce qui arrive quand $\dfrac{m^3\pm1}{13}=$ entier (sans dépendance mutuelle entre les deux signes), les trois décompositions se réduisent à une seule qu'on effectue par la résolution d'une équation du second degré.

On trouve ici deux valeurs de m, savoir $m=3$ et $m=4$ (il suffit de considérer les valeurs de m moindres que $\dfrac{13-1}{2}=6$; les autres conduiraient aux mêmes résultats), qui satisfont à la condition $\dfrac{m^3\pm1}{13}=$ entier, selon qu'on prend le signe inférieur ou le supérieur ; il n'en résulte cependant qu'une seule décomposition de la proposée en facteurs du troisième degré, ainsi qu'on peut s'en assurer et qu'il sera démontré dans la théorie générale. Les deux facteurs contiendront respectivement les deux groupes suivants de racines, savoir :

$$2\cos\frac{2\pi}{13},\ 2\cos\frac{6\pi}{13},\ 2\cos\frac{8\pi}{13};\ \text{et}\ 2\cos\frac{4\pi}{13},\ 2\cos\frac{12\pi}{13},\ 2\cos\frac{10\pi}{13}.$$

Si u désigne une quelconque des racines, les deux autres du même groupe seront u^3-3u et u^4-4u^2+2 ; représentant par y la somme de ces trois racines, il doit exister un commun diviseur de troisième degré en u entre les équations

$$u^4+u^3-4u^2-2u+2-y=0,$$
$$u^6+u^5-5u^4-4u^3+6u^2+3u-1=0.$$

On trouve, en effet, que $u^3-yu^2-u+y-1$ divise ces deux équations si l'on fait $y^2+y-3=0$. Mettant successivement dans le commun diviseur les deux valeurs de y données par l'équation précédente et changeant u en z, on obtient les deux facteurs dans lesquels la proposée peut se décomposer.

La résolution de l'équation $x^{13}-1=0$ peut donc encore se réduire à celle des trois équations

$$x^2-zx+1=0;\quad z^3-yz^2-z+y-1=0;\quad y^2+y-3=0.$$

On remarquera que les procédés qu'on vient d'employer conduisent tous les deux à la résolution de l'équation en x, au moyen de deux equations du second degré et d'une du troisième, conformément aux énoncés généraux des nos 1 et 14.

6. Soit maintenant l'équation $x^{17}-1=0$. Après en avoir séparé le facteur $x-1$, on la décompose en huit facteurs de la forme x^2-zx+1 au moyen de l'équation

$$z^8+z^7-7z^6-6z^5+15z^4+10z^3-10z^2-4z+1=0,$$

dont les racines sont représentées par les expressions

$$2\cos\frac{2\pi}{17},\ 2\cos\frac{4\pi}{17},\ 2\cos\frac{6\pi}{17},\ 2\cos\frac{8\pi}{17},$$

$$2\cos\frac{10\pi}{17},\ 2\cos\frac{12\pi}{17},\ 2\cos\frac{14\pi}{17},\ 2\cos\frac{16\pi}{17},$$

et ont entre elles les relations connues du double cosinus d'un arc aux doubles cosinus de différents multiples de cet arc.

Puis on décompose l'équation en z en deux facteurs contenant chacun quatre racines de la forme

$$2\cos\varphi,\ 2\cos m\varphi,\ 2\cos m^2\varphi,\ 2\cos m^3\varphi;$$

pour cela on prendra pour m un nombre tel qu'on ait $\cos m^4\varphi = \cos\varphi$, c'est-à-dire qui satisfasse à la condition $\frac{m^4 \pm 1}{17} =$ entier, sans quoi il y aurait quatre manières différentes de faire la décomposition, et l'on tomberait sur des équations du même degré que l'équation en z. Les nombres 2, 4, 8 satisfont à la condition ci-dessus, et les deux extrêmes servent à partager les racines en deux groupes, savoir

$$2\cos\frac{2\pi}{17},\ 2\cos\frac{4\pi}{17},\ 2\cos\frac{8\pi}{17},\ 2\cos\frac{16\pi}{17}$$

$$\text{et } 2\cos\frac{6\pi}{17},\ 2\cos\frac{12\pi}{17},\ 2\cos\frac{10\pi}{17},\ 2\cos\frac{14\pi}{17},$$

dans chacun desquels les racines sont assujetties à une même relation. Quant au nombre 4, il satisfait aussi à la condition $\frac{m^2+1}{17} =$ entier, et sera employé plus bas pour une nouvelle décomposition. Au moyen d'une racine quelconque u on exprimera les trois autres du même groupe, et puis la somme y des quatre. On aura par là les deux équations

$$u^8 - 8u^6 + 21u^4 - 19u^2 + u + 2 - y = 0,$$

$$u^8 + u^7 - 7u^6 - 6u^5 + 15u^4 + 10u^3 - 10u^2 - 4u + 1 = 0,$$

qui seront divisibles par le facteur commun

$$u^4-yu^3-(y+2)u^2+(2y+3)u-1,$$

si l'on fait $y^2+y-4=0$. Ce facteur commun, au moyen des deux valeurs de y, produit les deux facteurs dans lesquels se partage l'équation en z.

Il s'agit maintenant de décomposer à son tour l'équation

$$z^4-yz^3-(y+2)z^2+(2y+3)z-1=0,$$

dont les racines sont celles du premier ou du second groupe, selon qu'on y met pour y l'une ou l'autre de ses deux valeurs. La condition $\frac{m^2+1}{17}=$ entier, qui est satisfaite par $m=4$, indique la décomposition en deux facteurs contenant les racines

$$2\cos\frac{2\pi}{17},\ 2\cos\frac{8\pi}{17},\ \text{et}\ 2\cos\frac{4\pi}{17},\ 2\cos\frac{16\pi}{17}$$

respectivement, ou celles de l'autre groupe arrangées semblablement; selon la valeur qu'on suppose à y.

Soit s la somme des deux racines appartenant à un quelconque de ces derniers facteurs; on aura les deux équations

$$u^4-4u^2+u+2-s=0,$$
$$u^4-yu^3-(y+2)u^2+(2y+3)u-1=0,$$

qui admettront le commun diviseur $u^2-su+\frac{2s-y-2}{y}$, pourvu qu'on fasse $s^2-ys-1=0$. Le commun diviseur peut aussi s'écrire $u^2-su+\frac{s^2+s-y-4}{2}$. Si l'on change u en z et qu'on mette successivement pour s ses deux valeurs, on obtient les deux facteurs qui composent la dernière équation en z. Et comme dans chacun de ces facteurs on a deux valeurs à mettre pour y, on en conclut les quatre facteurs dans lesquels se partage l'équation du huitième degré en z.

Par ce qui précède, la résolution de l'équation $x^{17}-1=0$ se trouve ramenée à celle des quatre équations combinées

$$x^2-zx+1=0\,;\ z^2-sz+\frac{s^2+s-y-4}{2}=0\,;\ s^2-ys-1=0\,;$$
$$y^2+y-4=0.$$

Ces quatre équations n'étant que du second degré, il s'ensuit qu'on peut effectuer, avec la règle et le compas, la division du cercle en 17 parties égales (*).

7. Soit encore l'équation $x^{19}-1=0$. Après l'avoir divisée par $x-1$, et représenté par z la somme $x+\frac{1}{x}$ de deux racines réciproques, on en tire l'équation

$$z^9+z^8-8z^7-7z^6+21z^5+15z^4-20z^3-10z^2+5z+1=0,$$

dont il faut grouper les racines trois par trois de manière qu'elles se trouvent assujetties, dans chaque groupe, à une même relation qui ne puisse subsister entre elles à l'aide d'aucun autre arrangement. Les nombres 7 et 8 qui satisfont à la condition $\frac{m^3\pm 1}{19}=$ entier, conduisent à partager les racines en trois groupes comme il suit :

$$2\cos\frac{2\pi}{10},\ 2\cos\frac{14\pi}{19},\ 2\cos\frac{16\pi}{19};\ 2\cos\frac{4\pi}{19},\ 2\cos\frac{10\pi}{19},\ 2\cos\frac{6\pi}{19};$$
$$2\cos\frac{8\pi}{19},\ 2\cos\frac{18\pi}{19},\ 2\cos\frac{12\pi}{19}.$$

Si l'on désigne par u une racine quelconque, et par y la somme des trois du même groupe, on aura les deux équations

$$u^8+u^7+8u^6-7u^5+20u^4+14u^3-16u^2-6u+2-y=0,$$
$$u^9+u^8-8u^7-7u^6+21u^5+15u^4-20u^3-10u^2+5u+1=0,$$

(*) *Voir* Legendre, Trigon. CX. Tm.

qui doivent admettre un facteur commun du troisième degré, déterminé à l'aide d'une équation aussi du troisième degré.

Un court calcul conduit en effet au commun diviseur

$$u^3-yu^2+(y^2-5)u+\frac{1}{y+1},$$

dans lequel y doit être déterminé par l'équation

$$y^3+y^2-6y-7=0\,;$$

au moyen des trois valeurs de y, on en conclut l'un après l'autre les trois facteurs dans lesquels se décompose l'équation en z. L'équation en y fait voir qu'à la place du dernier terme $\frac{1}{y-1}$ on peut écrire y^2-6.

En dernière analyse, l'équation $x^{19}-1=0$ se trouve résolue au moyen de ces trois autres

$$x^2-zx+1=0\,;\quad z^3-yz^2+(y^2-5)z+y^2-6=0\,;$$
$$y^3+y^2-6y-7=0.$$

(La suite prochainement.)