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. 147-156

<http://www.numdam.org/item?id=NAM_1843_1_2__147_0>

DE LA RÉSOLUTION ALGÉBRIQUE DE L'ÉQUATION $x^p - 1 = 0$,

QUAND L'EXPOSANT p EST UN NOMBRE PREMIER.

PAR M. REALIS (S.).

—

II.

Théorie générale (*).

N. B. Dans tout ce qui suit, la lettre p désignera constamment un nombre premier.

8. *Si dans la suite des cosinus :*

$$\cos\frac{2\pi}{p}, \cos\frac{4\pi}{p}, \cos\frac{6\pi}{p}, \cos\frac{8\pi}{p}, \ldots \cos\frac{(p-3)\pi}{p}, \cos\frac{(p-1)\pi}{p},$$

formée des valeurs que prend $\cos\frac{2\alpha\pi}{p}$ *quand on y fait* α *égal successivement à tous les nombres entiers depuis* 1 *jusqu'à* $\frac{p-1}{2}$ *inclusivement, on multiplie chacun des arcs par un même nombre* m *premier avec* p : *on trouve pour résultat ces mêmes cosinus rangés dans un ordre différent.*

On a d'abord, en indiquant par $\cos\frac{2\alpha\pi}{p}$ un quelconque des cosinus de la suite, et par β le reste de la division de $2m\alpha$ par p,

$$\cos\frac{2m\alpha\pi}{p} = \cos\frac{\beta\pi}{p}, \text{ ou bien } \cos\frac{2m\alpha\pi}{p} = \cos\frac{(p-\beta)\pi}{p},$$

(*) Pour la première partie de ce mémoire, voyez pages 5... 16, t. II

selon que le quotient et le reste de la division sont des nombres pairs ou impairs, ce qui fait voir que $\cos\frac{\beta\pi}{p}$ dans le premier cas, et $\cos\frac{(p-\beta)\pi}{p}$ dans le second cas, est un des cosinus de la suite. Or, tant que 2α sera $< p$, les restes de la division de $2m\alpha$ par p seront tous différents, et ceux, parmi ces restes, qui sont impairs, retranchés de p donneront aussi des résultats différents, entre eux, et avec les restes pairs, ainsi qu'on peut facilement s'en convaincre. Donc, en faisant successivement $2\alpha = 2, 4, 6, 8, \ldots p-3, p-1$, on trouvera pour $\cos\frac{2m\alpha\pi}{p}$ tous les cosinus de la suite.

9. Soit h un diviseur de $\frac{p-1}{2}$, et qu'on fasse successivement dans $\cos\frac{2\alpha\pi}{p}$, $\alpha = 1, m, m^2, m^3, \ldots$ jusqu'à m^{h-1} inclusivement : si m rend entière une des quantités comprises dans l'expression $\frac{m^h \pm 1}{p}$, sans rendre entière aucune des quantités semblables dans lesquelles m est affecté d'un exposant moindre que h : $\cos\frac{2\alpha\pi}{p}$ prendra h valeurs toutes différentes entre elles et comprises dans la suite ci-dessus ; et si l'on continue à donner à α les valeurs m^h, m^{h+1}, $m^{h+2}, \ldots$ on retombera sur les valeurs de $\cos\frac{2\alpha\pi}{p}$ relatives à $\alpha = 1, m, m^2, \ldots$; lesquelles se reproduisent par périodes de h termes.

Cela résulte de ce que $\cos\frac{2m^{h+h'}\pi}{p} = \cos\frac{2m^{h'}\pi}{p}$ conduit à $\frac{m^h(m^h \pm 1)}{p} =$ entier, condition à laquelle la valeur de m satisfait par hypothèse, tandis que $\cos\frac{2m^h\pi}{p} = \cos\frac{2m^{h'}\pi}{p}$

conduirait à une condition à laquelle m ne satisfait pas, si h' et h'' sont $< h$.

Il suit de là que *si* h *est décomposable en deux facteurs* h', h'', *et qu'on veuille arranger les* h *cosinus en* h'' *groupes de* h' *termes, de la forme*

$$\cos\varphi,\ \cos m\varphi,\ \cos m^2\varphi,\ \cos m^3\varphi,\ \ldots\ \cos m^{h'-1}\varphi,$$

on pourra grouper les termes entre eux en h' *manières distinctes, selon qu'on commencera par* $\cos\frac{2\tau}{p}$ *ou par l'un quelconque des* $h'-1$ *termes suivants.* C'est ainsi que dans le n° 4, où $p=13$, $h'=2$, $h''=3$, en prenant $m=2$ on a trouvé deux manières différentes de distribuer les termes par couples.

Mais si, au lieu de prendre le nombre m tel qu'on vient de le dire, on prenait une solution de $\frac{m^{h'}\pm 1}{p}=$ entier, on aurait $\cos m^{h'}\varphi=\cos\varphi$, et les manières de grouper les termes se réduiraient a une seule.

10. *Parmi les nombres entiers* 1, 2, 3, 4,... $p-2, p-1$ *compris entre* 0 *et* p, *il y en a toujours* h *qui mis à la place de* m *rendent entière la quantité* $\frac{m^h+1}{p}$, *et* h *qui rendent entière la quantité* $\frac{m^h-1}{p}$, *et parmi ces* 2 h *nombres différents, outre l'unité, il y en a* $h-1$ *qui ne dépassent pas* $\frac{p-1}{2}$, *h est,* comme ci-dessus, un diviseur de $\frac{p-1}{2}$.

On sait que chacun des nombres 1, 2, 3, 4,... $p-2, p-1$ mis à la place de m dans l'expression $\frac{m^{p-1}-1}{p}$, donne pour résultat un nombre entier cela résulte du théorème de *Fermat.* Si de $m^{p-1}-1$ on sépare le facteur $m^{th}-1$, on voit

que, parmi les $p-1$ solutions de $\frac{m^{p-1}-1}{p}$ = entier, il doit s'en trouver $2h$ qui satisferont à $\frac{m^{2h}-1}{p}$ = entier (*). Ces dernières peuvent à leur tour se partager en deux groupes contenant les solutions de $\frac{m^h+1}{p}$ = entier et de $\frac{m^h-1}{p}$ = entier, respectivement. Il est donc prouvé qu'on satisfera à chacune de ces conditions au moyen de nombres compris entre 0 et p; mais il est bien facile de voir que, parmi ces nombres, il y en aura h qui ne dépasseront pas $\frac{p-1}{2}$. En effet, si pour $m=\alpha$ on a $\frac{\alpha^h-1}{p}$ = entier, pour $m=p-\alpha$ on aura $\frac{(p-\alpha)^h+1}{p}$ = entier, ou bien $\frac{(p-\alpha)^h-1}{p}$ = entier, selon que h est un nombre impair ou pair, ce qui prouve qu'à chaque valeur de m plus grande que $\frac{p-1}{2}$ il en correspond une autre qui ne dépasse pas $\frac{p-1}{2}$, et que par conséquent il ne saurait y avoir plus (ni moins) de h valeurs $> \frac{p-1}{2}$.

11. On peut encore demontrer que *aucune valeur de* α *comprise entre* 1 *et* $p-1$ *ne pourra donner* $\frac{\alpha^t \pm 1}{p}$ = entier, *si l'exposant* t, *qu'on suppose moindre que* $p-1$, *est premier avec* $p-1$.

Soit en effet $p-1 = kt+t'$, k étant le quotient de la division de $p-1$ par t, et t' le reste; et supposons que $\frac{\alpha^t+1}{p}$ soit un nombre entier, il en résultera : $\frac{\alpha^{kt}+1}{p}$ = entier, ou

(*) Cela est fondé sur une propriété connue des *congruences*.

$\frac{\alpha^{kt}-1}{p}$ = entier, suivant que k sera impair ou pair. D'ailleurs, leurs, $\frac{\alpha^{p-1}-1}{p}$ = entier donne $\frac{\alpha^{kt+t'}-1}{p}$ = entier, puisque $p-1=kt+t'$. Ajoutant $\frac{\alpha^{kt}+1}{p}$ et $\frac{\alpha^{kt+t'}-1}{p}$ on a $\frac{\alpha^{kt}(\alpha^{t'}+1)}{p}$, qui doit être entier si k est impair, d'où $\frac{\alpha^{t'}+1}{p}$ = entier; et si k est pair, retranchez $\frac{\alpha^{kt}-1}{p}$ de $\frac{\alpha^{kt+t'}-1}{p}$, il s'ensuivra $\frac{\alpha^{t'}-1}{p}$ = entier. On démontrera, de même, que si $\frac{\alpha^{t}-1}{p}$ est entier, il faut que $\alpha^{t'}+1$, ou $\alpha^{t'}-1$, soit divisible par p.

En opérant sur t' comme on vient de le faire sur t, on parviendra à $\frac{\alpha^{t''}\pm 1}{p}$ = entier, t'' étant le reste de la division de t par t'. Or, les nombres $p-1$ et t étant supposés premiers entre eux, un des restes succcessifs t', t'', t'''..., sera égal à l'unité; donc, l'égalité $\frac{\alpha^{t}\pm 1}{p}$ = entier conduira à $\frac{\alpha\pm 1}{p}$ = entier, condition impossible à remplir, car aucun des deux nombres $\alpha+1$, $\alpha-1$ n'est divisible par p, puisque α doit être compris entre 1 et $p-1$.

12. Je vais maintenant exposer en peu de mots les conséquences qu'on déduit des propositions précédentes relativement à la résolution de l'équation $x^p-1=0$, et parvenir au résultat annoncé au n° 1.

On sait d'abord que l'équation

$$x^{p-1}+x^{p-2}+x^{p-3}+x^{p-4}+\ldots\ldots+x+1=0,$$

qu'on obtient en divisant la proposée par $x-1$, se décompose en $\frac{p-1}{2}$ facteurs de la forme x^2-zx+1, au moyen d'une équation en z du degré $\frac{p-1}{2}$. Les racines de celle-ci sont repré-

sentées par les cosinus de la suite du n° 8, multipliés chacun par 2, et ont entre elles les relations connues du double cosinus d'un arc aux doubles cosinus des différents multiples de cet arc ; en sorte que u, désignant la première de ces racines, les autres se déduiront de l'expression

$$u^m - mu^{m-2} + \frac{m(m-3)}{2}u^{m-4} - \frac{m(m-4)(m-5)}{2.3}u^{m-6} + \frac{m(m-5)(m-6)(m-7)}{2.3.4}u^{m-8} - \text{etc.},$$

en y faisant successivement $m = 2,3.4,5.....\frac{p-3}{2}, \frac{p-1}{2}$. Il est à remarquer que les racines peuvent toutes se déduire ainsi de l'une quelconque d'entre elles, et qu'il n'y a que l'ordre dans lequel elles se trouveront écrites, qui variera selon que u désignera la première racine $2\cos\frac{2\pi}{p}$, ou toute autre racine (8).

Il arrive donc qu'on ne peut immédiatement abaisser l'équation en z à l'aide des relations qui existent entre ses racines, à cause que le commun diviseur que donnerait la méthode ordinaire d'abaissement, contiendrait toutes les racines et reviendrait au premier membre de la proposée elle-même. Pour que l'abaissement ait lieu à l'aide d'équations de degré inférieur à celui de la proposée, il faut décomposer celle-ci en des facteurs contenant un même nombre de racines assujetties dans chacun d'eux à une même relation donnée ; il faut de plus que parmi les différentes manières qu'on peut trouver d'opérer cette décomposition quand on a déterminé le nombre des facteurs et des racines correspondantes, on choisisse celle qu'on n'obtient qu'en combinant d'une seule façon les racines pour les partager en groupes. C'est ce qu'on a fait dans les cas particuliers des n°s 4, 5, 6, 7.

Soient h', h'' deux facteurs dont le produit forme le nom-

bre $\frac{p-1}{2}$ et m un nombre compris entre 1 et $\frac{p+1}{2}$, qui ne rende entière aucune quantité $\frac{m^t \pm 1}{p}$, t étant $< \frac{p-1}{2}$. Si l'on veut partager les racines en h'' groupes égaux, de manière qu'une racine étant représentée par $2\cos\varphi$, les $h'-1$ autres le soient par

$$2\cos m\varphi,\quad 2\cos m^2\varphi,\quad 2\cos m^3\varphi,\ldots\ldots 2\cos m^{h'-1}\varphi,$$

on pourra faire ce partage en h' manières differentes, de sorte que pour décomposer l'équation en h'' facteurs contenant ces groupes de racines, on aura une équation du degré $h'h''$ à résoudre. Cela résulte du n° 9, en y supposant $h=\frac{p-1}{2}$.

Mais si l'on choisit pour m une des solutions de $\frac{m^{h'}\pm 1}{p}=$ entier, il n'y aura plus qu'une manière d'effectuer le partage des racines (9), et la décomposition dépendra d'une équation du degré h''. Il est d'ailleurs facile de se convaincre que les solutions de $\frac{m^{h'}\pm 1}{p}=$ entier, comprises entre 1 et $\frac{p+1}{2}$ (10), qui ne satisferont à aucune condition semblable où l exposant de m soit $< h'$, mèneront toutes au même résultat. Prenant donc pour m une de ces solutions, et appelant y la somme des h'' racines appartenant à un même facteur, on aura deux équations, dont l'une exprimera qu'en retranchant la valeur de y, censée connue, de la somme des h'' racines exprimée en fonction d'une quelconque d'entre elles, on doit avoir zéro pour résultat, et l'autre sera la proposée en z elle-même.

La somme y a h'' valeurs différentes, car on a un pareil nombre de facteurs, et la première de ces deux equations, pour chaque valeur de y, doit être vérifiée par h' valeurs de l'inconnue; ces équations admettent donc un commun diviseur du degré h' déterminé à l'aide d'une équation en y du degré h''.

13. Par ce qui précède, l'équation en z se décomposera en h'' facteurs de la forme

$$(A) \qquad z^{h'} - yz^{h'-1} + az^{h'-2} + bz^{h'-3} + cz^{h'-4} + \ldots$$

$a, b, c, \ldots$ étant des fonctions rationnelles de y, susceptibles de h'' valeurs différentes.

Si h' et h'' sont des nombres premiers, la décomposition de l'équation en z s'arrête là; mais si h' est lui-même le produit de deux facteurs i', i'', on peut décomposer à son tour le polynôme (A). Quant au nombre h'', il convient de le supposer premier, afin de parvenir par une méthode simple et uniforme aux décompositions successives, jusqu'à la dernière : il en est de même à l'égard de i'', et en général de tous les nombres qui désignent en combien de facteurs semblables on décompose chaque polynôme en z, qu'on obtient successivement.

Prenant ici pour m une solution de $\frac{m^{i'} \pm 1}{p} =$ entier qui ne satisfasse à aucune condition semblable dans laquelle l'exposant de m soit $< i'$, on peut, d'une manière déterminée et unique, décomposer (A) en i'' facteurs contenant chacun i' racines liées par une relation telle que, la première étant $2\cos\varphi$, les autres soient $2\cos m\varphi$, $2\cos m^2\varphi$, $2\cos m^3\varphi$....., $2\cos m^{i'-1}\varphi$. Par des opérations tout à fait semblables à celles qu'on vient d'indiquer, on trouvera un polynôme de la forme

$$(B) \qquad z^{i'} - Sz^{i'-1} + a'z^{i'-2} + b'z^{i'-3} + c'z^{i'-4} + \ldots\ldots,$$

qui divisera (A); S désigne la somme des i' racines, qui pour chaque valeur de y doit avoir i'' valeurs différentes, et dépendra par conséquent d'une équation du degré i''; $a', b', c', \ldots$ sont des fonctions rationnelles de S, et aussi de y, qu'il n'est pas nécessaire de déterminer dans les calculs relatifs à la dé-

composition de (A). Le facteur (B), au moyen des h'' valeurs de y, produit donc les facteurs du degré h', qui composent (A), et chacun de ceux-ci, au moyen des i'' valeurs de S, se décompose à son tour en facteurs du degré i'.

Par là, la résolution de l'équation $x^p - 1 = 0$ se trouve maintenant ramenée à celle des équations

$$x^2 - zx + 1 = 0 ;$$
$$z^{i'} - Sz^{i'-1} + a'z^{i'-2} + b'z^{i'-3} + c'z^{i'-4} + \ldots = 0,$$

de l'équation du degré i'' en S, et de l'équation du degré h'' en y.

On voit que tant que le degré des facteurs dans lesquels on aura décomposé l'équation en z, est un nombre composé, on peut opérer une nouvelle décomposition ; ainsi, si i' était le produit de deux facteurs l', l'', on décomposerait encore le facteur (B), qu'on regarderait comme le produit de l'' facteurs semblables du degré l', etc.

14. Avec le secours des propositions des nos 8, 9, 10 et 11, on peut, sans difficulté, se rendre raison de ce qu'on vient de dire touchant l'abaissement de l'équation $x^p - 1 = 0$, et en conclure que *si* p—1 *se décompose en un nombre* n *de facteurs premiers, y compris les facteurs égaux, la résolution de l'équation* $x^p - 1 = 0$ *pourra se ramener rationnellement à celle de* n *équations dont les degrés seront marqués par ces mêmes facteurs premiers.* Comme les nombres désignés ci-dessus par h'', i'', l'', ... peuvent représenter les facteurs premiers de $\frac{p-1}{2}$ dans un ordre quelconque, il s'ensuit qu'on peut généralement opérer l'abaissement de plusieurs manières différentes. On en a vu un exemple dans le cas de $p = 13$, traité aux nos 4 et 5.

15. Les racines de l'équation $x^p - 1 = 0$ peuvent se construire géométriquement, par la ligne droite et le cercle, quand les

équations d'où dépend sa résolution, ne dépassent pas le second degré. Cela arrive lorsque l'exposant p est un nombre premier de la forme $2^{\varepsilon}+1$, d'où il suit qu'avec la règle et le compas on peut effectuer la division du cercle en $2_{\varepsilon}+1$ parties égales.

J'observerai que $2^{\varepsilon}+1$ ne saurait être un nombre premier si l'exposant ε n'est pas une puissance de 2. En effet, si ε était impair, $2^{\varepsilon}+1$ serait divisible par $2+1$ ou 3, et si ε était de la forme $\varepsilon'\lambda$, λ étant un nombre impair, $2^{\varepsilon'\lambda}+1$ serait divisible par $2^{\varepsilon'}+1$.