

# BULLETIN DE LA S. M. F.

D. SELIVANOFF

## **Quelques remarques sur les équations du cinquième degré**

*Bulletin de la S. M. F.*, tome 21 (1893), p. 97-109

[http://www.numdam.org/item?id=BSMF\\_1893\\_\\_21\\_\\_97\\_0](http://www.numdam.org/item?id=BSMF_1893__21__97_0)

© Bulletin de la S. M. F., 1893, tous droits réservés.

L'accès aux archives de la revue « Bulletin de la S. M. F. » (<http://smf.emath.fr/Publications/Bulletin/Presentation.html>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/legal.php>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme  
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

*Quelques remarques sur les équations du cinquième degré;*  
par M. D. SÉLIVANOFF.

En 1889, j'ai publié un Travail, en langue russe, *Sur les équations du cinquième degré à coefficients entiers*, dont je vais reproduire ici quelques résultats.

Soit proposée une équation irréductible

$$x^5 + p_1 x^4 + p_2 x^3 + p_3 x^2 + p_4 x + p_5 = 0,$$

dont les coefficients sont des nombres entiers.

Dans la suite nous dirons simplement *fonction des racines* pour désigner une *fonction entière à coefficients rationnels des racines de l'équation proposée*.

Ainsi que Galois l'a démontré, il existe un groupe de substitutions jouissant des deux propriétés suivantes : 1° Une fonction des racines ayant une valeur rationnelle ne change pas de valeur numérique par les substitutions du groupe; 2° une fonction des racines dont la valeur numérique ne change pas par les substitutions du groupe a une valeur rationnelle. Ce groupe est nommé *groupe de l'équation*. Les substitutions contenues dans le groupe de l'équation, qui ne changent pas la valeur d'une fonction des racines, forment un groupe. Le groupe de l'équation irréductible est transitif. Désignons les racines de l'équation proposée par

$$x_0, x_1, x_2, x_3, x_4,$$

et supposons que  $x_a = x_b$ , si  $a \equiv b \pmod{5}$ .

En changeant chaque racine  $x_z$  en  $x_{z+1}$  on exécute une substitution circulaire ou *cyclique* ( $x_z, x_{z+1}$ ) que l'on désigne aussi par (0 1 2 3 4).

Le groupe d'une équation résoluble par radicaux est composé des substitutions de la forme ( $x_z, x_{az+b}$ ).

Soit G un groupe transitif donné

$$G = (s = 1, s_2, s_3, \dots, s_{5m}).$$

Ce groupe contient  $5m$  substitutions,  $m$  désignant le nombre des substitutions qui laissent une racine invariable. On forme les vingt-quatre substitutions circulaires (0 a b c d) en rempla-

çant  $a, b, c, d$  par les différents arrangements des quatre chiffres 1, 2, 3, 4.

Soit  $c_1$  l'une de ces substitutions qui ne soit pas contenue dans le groupe  $G$ . Les  $5m$  substitutions de la forme  $s^{-1}c_1s$  ne sont pas contenues dans  $G$ ,  $s$  étant une substitution du groupe  $G$ . Désignons ces substitutions par

$$(\alpha) \quad c_1, c_2, c_3, \dots, c_{5m}, \dots$$

Si la substitution circulaire  $c'_1$  n'est pas contenue dans  $G$  et dans la série  $(\alpha)$ , on forme de la même manière la série

$$(\beta) \quad c'_1, c'_2, c'_3, \dots, c'_{5m}, \dots$$

des substitutions circulaires qui ne sont contenues ni dans  $G$ , ni dans la série  $(\alpha)$ . En procédant de la même manière, on conclut que *le nombre des substitutions circulaires qui n'est pas contenu dans le groupe  $G$  est un multiple de 5.*

Soit maintenant  $c$  une substitution circulaire contenue dans  $G$ . Les substitutions

$$(\alpha) \quad c, c^2, c^3, c^4,$$

sont aussi contenues dans  $G$ . Si la substitution circulaire  $c'$  est contenue dans  $G$ , mais non dans la série  $(\alpha)$ , on forme la série

$$(b) \quad c', c'^2, c'^3, c'^4$$

contenue dans le groupe  $G$ . On démontre de cette manière que *le nombre des substitutions circulaires contenues dans le groupe  $G$  est un multiple de 4.*

En désignant par  $4y$  le nombre des substitutions cycliques qui sont contenues dans le groupe  $G$  et par  $5z$  le nombre de celles qui ne sont pas contenues dans  $G$ , on obtient

$$4y + 5z = 24.$$

Les seules solutions de cette équation en nombres entiers et positifs sont

$$y = 1, \quad z = 4 \quad \text{et} \quad y = 6, \quad z = 0.$$

Dans le premier cas, le groupe  $G$  contient une substitution cyclique  $c$  avec ses puissances

$$c, c^2, c^3, c^4.$$

Dans le second cas, le groupe  $G$  contient toutes les vingt-quatre substitutions cycliques.

Supposons que le groupe de l'équation  $G$  contienne un seul groupe cyclique

$$\Gamma = (1, s, s^2, s^3, s^4).$$

Les racines  $x_0, x_1, x_2, x_3, x_4$  peuvent être disposées dans un ordre tel qu'on ait

$$s = (x_z, x_{z+1}).$$

Il est possible que  $G = \Gamma$ . Dans le cas contraire, il existe une substitution

$$t = (x_z, x_{\varphi(z)}),$$

qui est contenue dans  $G$ , mais non dans  $\Gamma$ . La substitution transformée  $t^{-1}st$  est cyclique et par conséquent contenue dans  $\Gamma$ . On a donc l'équation

$$t^{-1}st = s^a,$$

$a$  étant un des nombres, 2, 3, 4. En multipliant les deux membres de cette équation à gauche par  $t$ , on trouve

$$st = ts^a,$$

ou, en d'autres termes,

$$\varphi(z+1) = \varphi(z) + a.$$

En employant la notation du calcul des différences finies, on a

$$\Delta\varphi(z) = a.$$

Il en résulte

$$\varphi(z) = az + b;$$

par conséquent, *l'équation proposée est résoluble par radicaux.*

Les substitutions de la forme  $(x_z, x_{az+b})$  peuvent former les groupes suivants :

1° *Le groupe cyclique* composé des substitutions

$$1, s, s^2, s^3, s^4,$$

où  $s = (x_z, x_{z+1})$ ;

2° *Le groupe demi-métacyclique :*

$$1, s, s^2, s^3, s^4,$$

$$t, st, s^2t, s^3t, s^4t,$$

où  $t = (x_z, x_{4z})$ ;

3° Le groupe métacyclique :

$$\begin{aligned} & 1, \quad s, \quad s^2, \quad s^3, \quad s^4, \\ & u, \quad su, \quad s^2u, \quad s^3u, \quad s^4u, \\ & u^2, \quad su^2, \quad s^2u^2, \quad s^3u^2, \quad s^4u^2, \\ & u^3, \quad su^3, \quad s^2u^3, \quad s^3u^3, \quad s^4u^3, \\ & u^4, \quad su^4, \quad s^2u^4, \quad s^3u^4, \quad s^4u^4, \end{aligned}$$

où  $u = (x_z, x_{2z})$ .

Ces dénominations sont dues à Kronecker.

Supposons maintenant que le groupe transitif G contienne toutes les substitutions cycliques. Le groupe G contient aussi la substitution

$$(0 \ 1 \ 2 \ 3 \ 4)(0 \ 1 \ 4 \ 3 \ 2) = (0 \ 4 \ 1).$$

En transformant cette équation par les substitutions

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 2 & 4 & 3 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 3 & 4 & 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 4 & 3 & 2 & 1 \end{pmatrix},$$

on trouve

$$\begin{aligned} & (0 \ 2 \ 4 \ 3 \ 1)(0 \ 2 \ 1 \ 3 \ 4) = (0 \ 1 \ 2), \\ & (0 \ 3 \ 4 \ 2 \ 1)(0 \ 3 \ 1 \ 2 \ 4) = (0 \ 1 \ 3), \\ & (0 \ 4 \ 3 \ 2 \ 1)(0 \ 4 \ 1 \ 2 \ 3) = (0 \ 1 \ 4). \end{aligned}$$

Le groupe G contenant les substitutions  $(0 \ 1 \ 2)$ ,  $(0 \ 1 \ 3)$  et  $(0 \ 1 \ 4)$  est donc *alterné*, ou bien contient le groupe alterné. Dans le dernier cas, G est l'ensemble des cent vingt substitutions que l'on peut former avec cinq lettres. Ce groupe peut être nommé *symétrique*.

Jacobi a indiqué (*Gesammelte Werke*, Band III, p. 276-278) la fonction demi-métacyclique de cinq lettres

$$\begin{aligned} z_1 = & \quad x_0 x_1 + x_1 x_2 + x_2 x_3 + x_3 x_4 + x_4 x_0 \\ & - x_0 x_2 - x_1 x_3 - x_2 x_4 - x_3 x_0 - x_4 x_1, \end{aligned}$$

dont la forme reste invariable par les substitutions du groupe demi-métacyclique.

Par les substitutions

$$(\gamma) \quad (0 \ 1 \ 2), \quad (1 \ 2 \ 3), \quad (2 \ 3 \ 4), \quad (3 \ 4 \ 0), \quad (4 \ 0 \ 1).$$

contenues dans le groupe alterné la valeur  $z_1$  se change en  $z_2, z_3, z_4, z_5, z_6$ .

La substitution (1 2 3 4) ne faisant pas partie du groupe alterné change  $z_1, z_2, z_3, z_4, z_5, z_6$  en  $-z_1, -z_2, -z_3, -z_4, -z_5, -z_6$ .

Telles sont les douze valeurs de la fonction  $z_1$ . La fonction  $z^2 = \sigma_1$ , ayant six valeurs différentes, est donc une fonction métacyclique.

La fonction

$$F(z) = (z - z_1)(z - z_2)(z - z_3)(z - z_4)(z - z_5)(z - z_6) \\ = z^6 + a_1 z^5 + a_2 z^4 + a_3 z^3 + a_4 z^2 + a_5 z + a_6$$

ne change pas par les substitutions du groupe alterné.

Les substitutions qui ne sont pas contenues dans le groupe alterné changent  $a_1, a_3, a_5$  en  $-a_1, -a_3, -a_5$ .

Ce sont donc les fonctions alternées et elles ont, par conséquent, la forme

$$a_1 = m_1 \sqrt{\Delta}, \quad a_3 = m_3 \sqrt{\Delta}, \quad a_5 = m_5 \sqrt{\Delta},$$

$\Delta$  étant le discriminant.

Les dimensions des fonctions  $a_1, a_3, a_5, \Delta$  sont respectivement égales à 2, 6, 10, 20; par conséquent,  $a_1$  et  $a_3$  sont nuls et  $m_5$  est un entier que nous désignerons par  $m$ .

Il résulte de cette analyse que

$$F(z) = z^6 + a_2 z^4 + a_4 z^2 + a_6 + mz \sqrt{\Delta}.$$

Les coefficients  $a_2, a_4, a_6$  sont des fonctions entières à coefficients entiers des fonctions symétriques élémentaires

$$\Sigma x_0 = -p_1, \quad \Sigma x_0 x_1 = p_2, \quad \Sigma x_0 x_1 x_2 = -p_3, \\ \Sigma x_0 x_1 x_2 x_3 = p_4, \quad x_0 x_1 x_2 x_3 x_4 = -p_5.$$

Ainsi l'équation  $F(z) = 0$ , dont les racines sont  $z_1, z_2, z_3, z_4, z_5, z_6$ , a ses coefficients entiers. En remplaçant  $z^2$  par  $\sigma$  dans l'expression  $F(z)F(-z)$ , on obtient l'équation

$$\varphi(\sigma) = (\sigma^3 + a_2 \sigma^2 + a_4 \sigma + a_6)^2 - m^2 \Delta \sigma = 0,$$

dont les racines sont

$$\sigma_1 = z_1^2, \quad \sigma_2 = z_2^2, \quad \sigma_3 = z_3^2, \quad \sigma_4 = z_4^2, \quad \sigma_5 = z_5^2, \quad \sigma_6 = z_6^2.$$

Supposons que l'équation  $\varphi(\sigma) = 0$  ait une racine  $\alpha$  rationnelle

et, par conséquent, entière. En rangeant les racines  $x_0, x_1, x_2, x_3, x_4$  dans un ordre convenable, nous aurons  $\sigma_1 = a$ . Les substitutions qui changent la valeur numérique de  $\sigma_1$ , ne sont pas contenues dans le groupe de l'équation

$$f(x) = x^5 + p_1 x^4 + p_2 x^3 + p_3 x^2 + p_4 x + p_5 = 0.$$

Si l'équation  $\varphi(\sigma) = 0$  n'a pas de racines égales, les substitutions

$$(\gamma) \quad (0 \ 1 \ 2), \quad (1 \ 2 \ 3), \quad (2 \ 3 \ 4), \quad (3 \ 4 \ 0), \quad (4 \ 0 \ 1)$$

du groupe alterné changent la valeur  $\sigma_1$ . Le groupe de l'équation proposée, ne contenant pas les substitutions  $(\gamma)$ , est donc métacyclique ou bien fait partie du groupe métacyclique. Dans ce cas, l'équation proposée est résoluble par radicaux.

Si l'équation  $\varphi(\sigma) = 0$  a des racines égales, il est possible que la valeur numérique  $\sigma_1$ , reste invariable pour certaines des substitutions  $(\gamma)$ . Supposons que le groupe de l'équation  $f(x) = 0$  contienne le groupe alterné. La valeur  $\sigma_1$  doit rester invariable pour toutes les substitutions du groupe alterné, car il n'existe pas de groupe transitif faisant partie du groupe alterné et contenant le groupe métacyclique. Il en résulte que

$$\varphi(\sigma) = (\sigma - a)^6.$$

Nous obtenons l'identité suivante

$$(\sigma^3 + a_2 \sigma^2 + a_4 \sigma + a_6)^2 - m^2 \Delta \sigma = (\sigma - a)^6,$$

qui peut être mise sous la forme

$$(\sigma^3 + a_2 \sigma^2 + a_4 \sigma + a_6)^2 - (\sigma^3 - 3a \sigma^2 + 3a^2 \sigma - a^3)^2 = m^2 \Delta \sigma$$

ou

$$(2\sigma^3 + p\sigma^2 + q\sigma + r)(t\sigma^2 + u\sigma + v) = m^2 \Delta \sigma.$$

En égalant les coefficients de  $\sigma^5$ ,  $\sigma^4$  et  $\sigma^3$  dans les deux membres de cette équation, on trouve

$$t = 0, \quad u = 0, \quad v = 0,$$

et, par conséquent,  $\Delta$  serait nul; or l'équation  $f(x) = 0$  est supposée irréductible et son discriminant ne peut pas être nul. Il est

donc démontré que le groupe de l'équation  $f(x) = 0$  ne peut pas contenir le groupe alterné et l'équation proposée est aussi résoluble par radicaux dans le cas considéré.

Si l'équation  $\varphi(\sigma) = 0$  n'a pas de racines rationnelles, les fonctions métacycliques n'étant pas rationnelles, le groupe de l'équation  $f(x) = 0$  contient le groupe alterné et l'équation  $f(x) = 0$  n'est pas résoluble par radicaux.

On a donc ce théorème :

*Pour que l'équation irréductible*

$$f(x) = x^5 + p_1 x^4 + p_2 x^3 + p_3 x^2 + p_4 x + p_5 = 0,$$

*à coefficients entiers, soit résoluble par radicaux, il faut et il suffit que l'équation*

$$\varphi(\sigma) = (\sigma^3 + a_2 \sigma^2 + a_4 \sigma + a_6)^2 - m^2 \Delta \sigma = 0$$

*ait au moins une racine entière.*

Pour les équations de la forme

$$f(x) = x^5 + ux + v = 0,$$

les valeurs de  $a_2, a_4, a_6, m$  et  $\Delta$  peuvent être obtenues presque sans calcul, comme l'a démontré M. Runge dans un article inséré au Tome VII des *Acta mathematica* (p. 173-186). On y trouve le résultat suivant :

$$\varphi(\sigma) = (\sigma^3 - 5u\sigma^2 + 15u^2\sigma + 5u^3)^2 - \Delta\sigma.$$

M. Runge met encore cette fonction sous la forme

$$\varphi(\sigma) = (\sigma - u)^4 (\sigma^2 - 6u\sigma + 25u^2) - 5^5 v^4 \sigma.$$

Faisons  $u = \pm 1$ . La racine entière de l'équation

$$5^5 v^4 \sigma = (\sigma \mp 1)^4 (\sigma^2 \mp 6\sigma + 25)$$

doit être positive, car

$$\sigma^2 \mp 6\sigma + 25 = (\sigma \mp 3)^2 + 16.$$

Le nombre  $\sigma$  est diviseur de 25 et, par conséquent, les seules valeurs à examiner sont  $\sigma = 1, 5, 25$ .



Comme ces valeurs ne vérifient pas l'équation, on a le théorème suivant :

*Les équations de la forme*

$$x^5 + ux + v = 0 \quad (u = \pm 1)$$

*ne sont pas résolubles par radicaux, quand elles sont irréductibles.*

Ce théorème a été démontré par M. Runge dans le cas où  $u = 1$ .

La recherche des diviseurs linéaires de la fonction

$$f(x) = x^5 + ux + v$$

ne présente aucune difficulté. Pour trouver les diviseurs quadratiques, on divise  $f(x)$  par  $x^2 + a_1x + a_2$  et l'on égale à zéro le reste de la division. On a ainsi deux équations

$$(1) \quad a_2^2 - 3a_1^2a_2 + a_1^4 + u = 0,$$

$$(2) \quad a_1a_2(2a_2 - a_1^2) - v = 0,$$

qui servent à déterminer les nombres entiers  $a_1$  et  $a_2$ . Ces nombres doivent encore satisfaire aux conditions

$$|a_1| < 2\rho, \quad |a_2| < \rho^2,$$

$\rho$  étant la limite supérieure des modules des racines de l'équation  $f(x) = 0$ . La recherche des diviseurs quadratiques est ainsi réduite à un nombre fini d'opérations.

L'impossibilité des équations (1) et (2) devient quelquefois manifeste, si les premiers membres de ces équations ne sont pas divisibles par un nombre premier. Soit l'équation

$$f(x) = x^5 + x - v, \quad v > 0.$$

Si l'on avait  $v < 0$ , il suffirait de remplacer  $f(x)$  par  $-f(-x)$ .

En supposant, par exemple,  $\rho = 6$ , on a

$$v < 6^5 - 6 \quad \text{ou} \quad v < 7770.$$

La fonction  $f(x)$  a des diviseurs linéaires pour

$$v = 1^5 + 1, \quad 2^5 + 2, \quad 3^5 + 3, \quad 4^5 + 4, \quad 5^5 + 5$$

ou

$$\nu = 2, \quad 34, \quad 246, \quad 1028, \quad 3130.$$

Cette fonction est divisible par  $x^2 + a_1 x + a_2$ , si les nombres entiers  $a_1$  et  $a_2$  satisfont aux équations

$$a_2^2 - 3a_1^2 a_2 + a_1^3 + 1 = 0, \quad a_1 a_2 (2a_2 - a_1^2) + \nu = 0.$$

En résolvant la première par rapport à  $a_2$ , on obtient

$$2a_2 = 3a_1^2 + s,$$

où  $s^2 = 5a_1^3 - 4$ .

La seconde équation prend la forme

$$a_1(2a_1^2 + s)(3a_1^2 + s) = -2\nu.$$

Ayant trouvé les nombres entiers  $a_1$  et  $s$  qui vérifient les conditions

$$5a_1^3 - s^2 = 4, \quad -12 < a_1 < 12,$$

on détermine les valeurs correspondantes de  $a_2$  et  $\nu$  par les formules obtenues.

Si  $a_1$  est pair,  $s$  est aussi pair. En posant

$$a_1 = 2z, \quad s = 4t \quad \text{ou} \quad 4t + 2,$$

on obtient les équations impossibles

$$20z^3 = 4t^2 + 1 \quad \text{ou} \quad 20z^3 = 4t^2 + 4t + 2;$$

d'où l'on conclut que  $a_1$  est un nombre impair.

Supposons que  $a_1$  soit divisible par un nombre premier  $p$ . Il suit de la congruence

$$s^2 \equiv -4 \pmod{p}$$

que le symbole de Legendre

$$\left(\frac{-4}{p}\right) = (-1)^{\frac{p-1}{2}}$$

doit être égal à 1. Donc  $p$  est de la forme  $4k + 1$ .

En excluant les valeurs paires de  $a_1$ , ou divisibles par les nombres premiers de la forme  $4k + 3$ , nous n'obtenons que les valeurs suivantes

$$a_1 = \pm 1, \quad a_1 = \pm 5.$$

Pour  $a_1 = \pm 1$ , on trouve les résultats suivants

$$\begin{aligned}x^5 + x - 1 &= (x^2 - x + 1)(x^3 + x^2 - 1), \\x^5 + x - 6 &= (x^2 - x + 2)(x^3 + x^2 - x - 3).\end{aligned}$$

La valeur  $a_1 = \pm 5$  ne convient pas, car le nombre

$$5^5 - 4 = 3121$$

n'est pas un carré parfait. On a donc ce théorème :

*Les équations de la forme*

$$x^5 + x - v = 0 \quad (0 < v < 7770)$$

*ne sont résolubles par radicaux que pour*

$$v = 1, 2, 6, 34, 246, 1028, 3130.$$

Passons maintenant à l'équation

$$f(x) = x^5 - x - v = 0 \quad (v > 0),$$

en supposant toujours  $\rho = 6$ . On a encore

$$v < 6^5 - 6 \quad \text{ou} \quad v < 7770.$$

La fonction  $f(x)$  a des diviseurs linéaires pour

$$v = 2^5 - 2, \quad 3^5 - 3, \quad 4^5 - 4, \quad 5^5 - 5$$

ou

$$v = 30, \quad 240, \quad 1020, \quad 3120.$$

La fonction  $f(x)$  est divisible par  $x^2 + a_1x + a_2$ , si les nombres  $a_1$  et  $a_2$  vérifient les conditions

$$a_2^2 - 3a_1^2a_2 + a_1^4 - 1 = 0, \quad a_1a_2(2a_2 - a_1^2) + v = 0.$$

En déterminant les entiers  $a_1$  et  $s$  de manière que

$$s^2 - 5a_1^2 = 4, \quad -12 < a_1 < 12,$$

on trouve les valeurs correspondantes de  $a_2$  et  $v$  par les formules suivantes

$$\begin{aligned}2a_2 &= 3a_1^2 + s, \\a_1(2a_1^2 + s)(3a_1^2 + s) &= -2v.\end{aligned}$$

Le nombre  $a_1$  est pair en même temps que  $s$ . En posant

$$a_1 = 2z, \quad s = 2t,$$

on trouve

$$20z^4 = (t+1)(t-1).$$

Le nombre  $t$  est impair, car le premier membre de cette équation est pair. Soit donc  $t = 2m + 1$ ; on a

$$5z^4 = m(m+1).$$

Les nombres  $m$  et  $m+1$  sont premiers entre eux.

L'équation obtenue est impossible, car le nombre  $5z^4$  n'est pas un produit de deux nombres consécutifs premiers entre eux. Il est donc démontré que  $a_1$  est un nombre impair.

Supposons que  $a_1$  soit premier ou une puissance d'un nombre premier. Il suit de l'équation

$$5a_1^4 = (s+2)(s-2)$$

que  $5a_1^4$  doit être décomposable en deux facteurs dont la différence est 4. Ces facteurs ne peuvent donc pas avoir un diviseur commun autre que 2 ou 4. Il en résulte que

$$s+2 = 5a_1^4, \quad s-2 = 1,$$

ou bien

$$s+2 = -1, \quad s-2 = -5a_1^4$$

et, par conséquent,

$$s = \pm 3, \quad a_1 = \pm 1.$$

Si  $a_1$  n'est pas égal à 5 ou à une puissance de 5, on a encore la décomposition

$$s+2 = a_1^4, \quad s-2 = 5,$$

ou

$$s+2 = -5, \quad s-2 = -a_1^4,$$

en supposant  $a_1^2 > 1$ . De là résulte l'équation impossible

$$a_1^4 = 9.$$

En examinant les seuls cas qui restent,  $a_1 = \pm 1$ , on trouve le résultat suivant

$$x^5 - x - 15 = (x^2 - x + 3)(x^3 + x^2 - 2x - 5),$$

en supposant toujours  $x > 0$ .

On peut donc énoncer ce théorème :

*Les équations de la forme*

$$x^5 - x - \nu = 0 \quad (0 < \nu < 7770)$$

*ne sont résolubles par radicaux que pour*

$$\nu = 15, \quad 30, \quad 240, \quad 1020, \quad 3120.$$

Toutes ces valeurs de  $\nu$  sont divisibles par 15.

Nous allons démontrer que l'équation

$$f(x) = x^5 - x - \nu = 0$$

*n'est pas résoluble par radicaux, si  $\nu$  n'est pas multiple de 15.*

Il suffit de démontrer l'irréductibilité de cette équation. Prenons 3 pour module. L'équation  $f(x) = 0$  peut avoir une racine entière  $a$ , si une des congruences

$$f(0) \equiv 0, \quad f(1) \equiv 0, \quad f(-1) \equiv 0 \pmod{3}$$

a lieu.

En remarquant que pour l'équation considérée

$$f(0) \equiv -\nu, \quad f(1) \equiv -\nu, \quad f(-1) \equiv -\nu \pmod{3},$$

on conclut que l'équation proposée n'a pas de racines entières, si  $\nu$  n'est pas divisible par 3.

Supposons que  $f(x)$  soit divisible par  $x^2 + a_1x + a_2$ . Les équations (1) et (2) peuvent être remplacées par les congruences

$$a_1^2 + a_2^2 - 1 \equiv 0, \quad a_1a_2(a_1^2 + a_2) \equiv -\nu \pmod{3}.$$

Si  $a_1$  est divisible par 3,  $\nu$  l'est aussi. Si  $a_1$  n'est pas divisible par 3, on a

$$a_1^2 \equiv 1, \quad a_2 \equiv 0, \quad \nu \equiv 0 \pmod{3}.$$

Donc la fonction  $f(x)$  n'a pas de diviseurs quadratiques, si  $\nu$  n'est pas divisible par 3.

Passons au module 5. D'après le théorème de Fermat, pour tout entier  $a$ , on a

$$a^5 - a \equiv 0 \pmod{5},$$

et, par conséquent,

$$f(a) \equiv -\nu \pmod{5}.$$

Donc  $f(x)$  n'a pas de diviseurs linéaires, si  $\nu$  n'est pas multiple de 5.

En supposant que  $f(x)$  soit divisible par  $x^2 + a_1x + a_2$ , on

obtient les congruences

$$\begin{aligned} a_2(a_2 + 2a_1^2) + a_1^2 - 1 &\equiv 0 \pmod{5}, \\ a_1 a_2(2a_2 - a_1^2) + \nu &\equiv 0 \pmod{5}. \end{aligned}$$

Le nombre  $\nu$  est divisible par 5 en même temps que  $a_1$  ou  $a_2$ . En posant  $a_1 \equiv \pm 1 \pmod{5}$ , on trouve

$$a_2(a_2 + 2) \equiv 0, \quad \pm a_2(2a_2 - 1) + \nu \equiv 0 \pmod{5}.$$

Si  $a_2$  n'est pas divisible par 5, on a

$$a_2 \equiv -2, \quad 2a_2 - 1 \equiv 0, \quad \nu \equiv 0 \pmod{5}.$$

On démontre de la même manière qu'on a aussi  $\nu \equiv 0 \pmod{5}$ , quand  $a_1 \equiv \pm 2 \pmod{5}$ .

Le théorème énoncé est donc démontré.

---