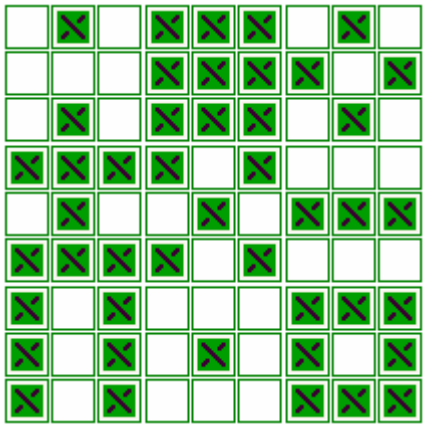
On Fermat's last theorem

By Méhdi Pascal
MehdiPascal38@gmail.com
March 3, 2025

Abstract

This paper is a correction of the last paper I published in viXra in 2021, "*On the signs of Lagrang*e " I had made some big mistakes, and since it's really very important, so I'm correcting it.
This paper contains a proof of Fermat's theorem for the first cases, a link between Fermat's theorem and a work by Lagrange, and a link between Fermat's theorem and Galois theory.

This paper was originally written in French, and is translated into English by DeepL, thank so much to DeepL.



Thank so much to viXra for allowing me to publish my essays.

Notation:

Let *E*=0 be a multivariate equation, and *S* a set, we denote the solubility of *E*=0 in the set *S* by *S*||*E*=0||*S*.

Example:

$$Z^*\left\|x^2+y^2=z^2\right\|Z^* \text{ is true}$$

$$Z^*\left\|x^3+y^3=z^3\right\|Z^* \text{ is false.}$$

Lemma :

$$Z^*\left\|x^n+y^n=z^n\right\|Z^* \text{ if and only if } Q^*\left\|x^n+y^n=z^n\right\|Q^* \quad .$$

Because on the one hand $Z^* \subset Q^*$ and on the other hand it is sufficient to multiply by the product of the denominators.

By virtue of the fact that in Q^* under the hypothesis that $x^n+y^n=z^n$ is solvable I can give y a value of my choice, for example $r \in Q^*$, since (x,y,z) is a solution then $\left(\frac{xr}{y}, r, \frac{zr}{y}\right)$ is also a solution.

Fermat's last theorem, case n=2, "Lagrange's idea".

Everyone knows that the equation $x^2+y^2=z^2$ has non-zero integer solutions, for example : $9^2+12^2=15^2$.

If we change sign, the equation $x^2-y^2=z^2$ also has non-zero integer solutions, for example $13^2-12^2=5^2$.

The two equations form a soluble system of non-zero integers, which I call a permutation system of order 2, such that :

$$Sp_2 := \begin{cases} x_1^2+y^2=z_1^2 \\ x_2^2-y^2=z_2^2 \end{cases}$$

This system is soluble in *Z**, because we have :

$$\begin{cases} 9^2+12^2=15^2 \\ 13^2-12^2=5^2 \end{cases}$$

We can therefore assume that we have the following equivalence:

$$Z^*\left\|Sp_2\right\|Z^* \Leftrightarrow Z^*\left\|u^2+v^2=w^2\right\|Z^*$$

Fermat's last theorem, case n=3

Let $Sp_3 := \begin{cases} x_1^3+y^3=z_1^3 \\ x_2^3+jy^3=z_2^3 \\ x_3^3+j^2y^3=z_3^3 \end{cases}$ be with $j=\exp\left(\frac{2\pi i}{3}\right)$, and we have,

$$Q^*\left\|Sp_3\right\|Q^* \text{ iff } Q^*\left\|u^3+v^3=w^3\right\|Q^*$$

Proof:

First sense, assume that $Q^*\left\|Sp_3\right\|Q^*$ is true, then pose $u=x_1$, $v=y$ and $w=z_1$ so $Q^*\left\|u^3+v^3=w^3\right\|Q^*$ is true.

In the second sense, we assume that $Q*\left\|u^3+v^3=w^3\right\|Q*$ is true, note that the *Sp3* system contains 7 unknowns, so by the hypothesis that $Q*\left\|u^3+v^3=w^3\right\|Q*$ is true, we set $x_1=u$, $y=v$ and $z_1=w$, so all that remains is to prove that the 4 remaining unknowns can be non-zero rationals.

In the *Sp3* system, we add the three equations, so that,

$$x_1^3+x_2^3+x_3^3=z_1^3+z_2^3+z_3^3$$

Because $j^2+j+1=0$

Therefore

$$x_2^3+x_3^3=y^3+z_2^3+z_3^3$$

The lemma allows me to put *y*=1, and so,

$$x_2^3+x_3^3=1+z_2^3+z_3^3$$

And $Q*\,||\,x_2^3+x_3^3=1+z_2^3+z_3^3\,||\,Q*$ is true, for example $7^3+8^3=1^3+5^3+9^3$, it even admits an infinite number of solutions, for example,

$$\left(2N+1\right)^3+\left(2N+2\right)^3=1^3+\left(2N+1+\sqrt{N+1}\right)^3+\left(2N+1-\sqrt{N+1}\right)^3$$

So the 4 remaining unknowns can be non-zero rationals, which proves equivalence.
The *Sp3* system cannot be soluble because of the complex number *j*, so Fermat's equation cannot be soluble either.
QFD

Fermat's last theorem case n≥4

Let $\zeta=\exp\left(\frac{2\pi i}{n}\right)$, the permutation system of order *n* be written as follows,

$$Sp_n:=\begin{cases}x_1^n+y^n=z_1^n\\x_2^n+\zeta y^n=z_2^n\\x_3^n+\zeta^2 y^n=z_3^n\\..[]..\\x_n^n+\zeta^{n-1}y^n=z_n^n\end{cases}$$

And we have,

$$Q*\left\|Sp_n\right\|Q*\Leftrightarrow Q*\left\|u^n+v^n=w^n\right\|Q*$$

Proof:

The same reasoning as for the case *n*=3 leads us to the following resolvent:

$$S_n:=\left(\sum_{j=2}^{n}x_j^n=1^n+\sum_{j=2}^{n}z_j^n\right)$$

This resolvent is at least solvable in *Q**, for cases 4, 5, 6 and 7, because we have,

$$12^4+13^4+21^4=1^4+4^4+17^4+20^4$$
$$5^5+8^5+13^5+14^5=1^5+6^5+7^5+11^5+15^5$$
$$2^6+5^6+20^6+26^6+27^6=1^6+6^6+8^6+18^6+25^6+28^6$$
$$3^7+6^7+16^7+18^7+22^7+28^7=1^7+2^7+7^7+11^7+21^7+24^7+27^7$$

For these 4 cases, $Q*\|Sp_n\|Q*$ is false, because of the complex number ζ, and so by equivalence we have, $Q*\|u^n+v^n=w^n\|Q*$ is also false, which proves Fermat's theorem for these first cases.

The link with Lagrange's work

Consider the following two equations,

$$(S_n) := \left(\sum_{j=1}^{n-1} x_j^n = \sum_{j=1}^{n} z_j^n\right)$$

$$(S_{n,d}) := \left(\sum_{j=1}^{d-1} x_j^n = \sum_{j=1}^{d} z_j^n\right)$$

With *d* a proper divisor of *n*, "$d \neq n \ \& \ d \neq 1$".
The problem with these two equations is that the first is always solvable, while the second is not, and we write,

$$Z*\|S_n\|Z* \text{ is true}$$

$$Z*\|S_{n,d}\|Z* \text{ is false.}$$

Don't try to prove that, because it's very complicated, what I'm proposing is to understand it, and to understand it I'm proposing to use a computer to look for the solutions to these two equations.
On the other hand, it is possible to demonstrate them case by case, so for the first equation (S_n), and as we've already seen solutions of the following type,

$$7^3+8^3=1^3+5^3+9^3$$
$$12^4+13^4+21^4=1^4+4^4+17^4+20^4$$
$$5^5+8^5+13^5+14^5=1^5+6^5+7^5+11^5+15^5$$
$$2^6+5^6+20^6+26^6+27^6=1^6+6^6+8^6+18^6+25^6+28^6$$
$$3^7+6^7+16^7+18^7+22^7+28^7=1^7+2^7+7^7+11^7+21^7+24^7+27^7$$

For the second equation we use the same reasoning, for example we take the case of *n*=6 with *d*=3, and we have,

$$(S_{6,3}) := (x_2^6+x_3^6=z_1^6+z_2^6+z_3^6)$$

In fact, let's have the following system,

$$(Sys) := \begin{cases} u_1^6+v_1^6+w^6=s_1^6+t_1^6 \\ u_2^6+v_2^6+jw^6=s_2^6+t_2^6 \\ u_3^6+v_3^6+j^2w^6=s_3^6+t_3^6 \end{cases}$$

With $j^2+j+1=0$.
We have,

$$Q*\|Sys\|Q* \text{ if and only if } Q*\|x_2^6+x_3^6=z_1^6+z_2^6+z_3^6\|Q*$$

The first meaning is obvious, because the equation ($S_{6,3}$) is a member of (*Sys*). For the second meaning, we add the three equations of the system (*Sys*), which gives,

$$u_1^6+v_1^6+u_2^6+v_2^6+u_3^6+v_3^6=s_1^6+t_1^6+s_2^6+t_2^6+s_3^6+t_3^6$$

Therefore,

$$u_2^6+v_2^6+u_3^6+v_3^6=w^6+s_2^6+t_2^6+s_3^6+t_3^6$$

And we have, $Q^* \left\| u_2^6 + v_2^6 + u_3^6 + v_3^6 = w^6 + s_2^6 + t_2^6 + s_3^6 + t_3^6 \right\| Q^*$ is true, for example,

$$13^6 + 23^6 + 24^6 + 34^6 = 1^6 + 8^6 + 21^6 + 30^6 + 32^6 \ .$$

This proves the equivalence, as the solubility of (*Sys*) is impossible, because of the complex number *j*, then by equivalence the equation ($S_{6,3}$) is also non-soluble.

Link with Galois theory

Fermat's equation is an equation with several unknowns, also called a diophantine equation, "*we restrict ourselves to the case of polynomial equations with several unknowns and rational coefficients*", when we ask the following question, can Galois' theory justify this kind of equation? Most mathematicians answer in the negative, but I think that any diophantine equation has a Galois justification. It's true that it's not an easy job, but I can give examples.
Let's say,

$$x^5 - 10yx - 5y^5 = 0$$

With,

$$xy \neq 0$$

This Diophantine equation is unsolvable, and it can be justified by Galois theory.

Proof

According to a criterion of Richard Dedekind, any transitive subgroup of S_n containing a transposition, and an (n-1)-cycle, is necessarily equal to S_n as a whole .
So for a fifth-degree equation that satisfies the following two conditions,
- A pair of complex solutions, and three real solutions.
- Irreducible.

Then certainly its Galois group verifies Dedekind's criterion, and so it is worth at S_5 that it is unsolvable, for example $x^5 - 10x - 5 = 0$.
Let y be any non-zero complex number, if I multiple each solution of the equation $x^5 - 10x - 5 = 0$ by y, I obtain the equation $x^5 - 10yx - 5y^5 = 0$, as $x^5 - 10x - 5 = 0$ is not solvable by radicals, so it is the same for the equation $x^5 - 10yx - 5y^5 = 0$.
This means that not only is there no non-zero rational pair that satisfies this equation, but there is also no pair of radicals that can be obtained by this equation.
QFD

Normally, when we talk about the solubility of a Diophantine equation, we talk about its solubility by integers. This notion must be completely abandoned, at least for the following reason: if an equation admits solutions by integers, then its solution field is quite simply Q, otherwise there are two cases, either it does not have a solution field as in the previous example, or it has a solution field, which is a finite and minimal extension of Q, for example $x^2 + xy + y^2 = 0$ with $xy \neq 0$, its solution field is $Q(i\sqrt{3})$, it is minimal because no solution in Q is possible.
For Fermat's equation $x^n + y^n = z^n$ with $xyz \neq 0$, the first thing to remember is that it is always solvable by radicals, because $z = \sqrt[n]{x^n + y^n}$ is a radical. An important consequence of this is that the Fermat equation has a field of solutions.

Lemma

Let a and b be two complex numbers, and $n \geq 2$ an integer.

Let $E = \left\{ (a+b), (a^2+b^2), (a^3+b^3) \ ..[]..\ (a^n+b^n) \right\}$

$E \subset Q$ if and only if, *a* and *b* are radicals of second degree, "*a* and *b* are conjugates in $Q(\sqrt{\delta})$, $a = r + s\sqrt{\delta}$ & $b = r - s\sqrt{\delta}$ "

The proof is easy, this lemma is very important, unfortunately it is not sufficient, but at least it allows us to understand the nature of the solutions of Fermat's equation.

Parametric form of the equation

Under the assumption that the equation $x^n + y^n = z^n$ is solvable in *Q**, then there exist two non-zero rationals *a* and *b* such that, $x = z - a$ and $y = z - b$, so

$$(z-a)^n + (z-b)^n - z^n = 0$$

Expand and obtain,

$$z^n + \sum_{j=1}^{n} (-1)^j \binom{n}{j} (a^j + b^j) z^{n-j} = 0$$

We pose $H_n(z) = z^n + \sum_{j=1}^{n} (-1)^j \binom{n}{j} (a^j + b^j) z^{n-j} = (z-a)^n + (z-b)^n - z^n$, so Fermat's equation becomes,

$$H_n(z) = 0$$

And we have the following theorem:

Theorem

$H_n(z) \in Q[X]$ if and only if the two parameters a and b are radicals of second degree.

Proof

This is an immediate consequence of the previous lemma.

Examples:

For n=3

$$\left(18 + 17\sqrt{2}\right)^3 + \left(18 - 17\sqrt{2}\right)^3 = 42^3$$

$$\left(9 + \sqrt{5}\right)^3 + \left(9 - \sqrt{5}\right)^3 = 12^3$$

$$\left(6 + 5\sqrt{6}\right)^3 + \left(6 - 5\sqrt{6}\right)^3 = 18^3$$

..[]..

We even have a double solution,

A double solution means that it is a solution of both $x^3 + y^3 = z^3$ and $x^2 + y^2 = z^2$, because in general we have $dH_n(z)/dz = nH_{n-1}(z)$.

Calculating the discriminant of $H_3(z)$ gives,

$$disc\left(H_3(z)\right) = -27a^2b^2\left(9(a^2+b^2) - 14ab\right)$$

In *Q*, $disc\left(H_3(z)\right) = 0$ leads to trivial solutions, in particular the term $9(a^2+b^2) - 14ab$ is always positive, and only cancels out at $a = b = 0$.

In the case of a quadratic extension $Q(\sqrt{\delta})$, put $a = r + s\sqrt{\delta}$ and $b = r - s\sqrt{\delta}$ so $9(a^2+b^2) - 14ab = 0$ leads to $r^2 = -8s^2\delta$, so we necessarily have $\delta = -2$, and so $r = 4s$ we find that $a = s\left(4 + i\sqrt{2}\right)$ and $b = s\left(4 - i\sqrt{2}\right)$, so $H_3(z) = (z - 2s)^2(z - 20s)$ so we have,

$$(-2 + \mathrm{i}\sqrt{2})^3 + (-2 - i\sqrt{2})^3 = 8$$

&

$$(-2+\mathrm{i}\sqrt{2})^2+(-2-i\sqrt{2})^2=4$$

And this is the only double solution with one common factor. "*The little s*".

For n≥4

For higher orders solutions are becoming increasingly very rare, so to find some you have to be crafty,

$$(1+i\sqrt{7})^4+(1-i\sqrt{7})^4=2^4$$
$$(1+i\sqrt{3})^5+(1-i\sqrt{3})^5=2^5$$
$$(1+i\sqrt{3})^7+(1-i\sqrt{3})^7=2^7$$

Even if it doesn't prove that the solutions can't be rationals, but I think that the field of solutions to Fermat's equation is always a quadratic field $Q(\sqrt{\delta})$, and what do you think?

Thank you for reading this paper
Sincerely
Méhdi Pascal
MehdiPascal38@gmail.com

Notation :
Soit E=0 une équation à plusieurs variables, et S un ensemble, on note la solubilité de E=0 dans l'ensemble S par $S||E=0||S$.
Exemple :

$$Z^*\left\|x^2+y^2=z^2\right\|Z^* \text{ est vraie}$$
$$Z^*\left\|x^3+y^3=z^3\right\|Z^* \text{ est fausse.}$$

Lemme :

$$Z^*\left\|x^n+y^n=z^n\right\|Z^* \textit{ Si et seulement si } Q^*\left\|x^n+y^n=z^n\right\|Q^*.$$

Car d'un part $Z^*\subset Q^*$ et d'autre part il suffit de multiplier par le produit des dénominateurs.
En vertu, dans Q^* sous l'hypothèse que $x^n+y^n=z^n$ est soluble je peux donner à y une valeur de mon choix, soit par exemple $r\in Q^*$, comme (x,y,z) est une solution alors $\left(\frac{xr}{y},r,\frac{zr}{y}\right)$ est aussi une solution.

Le grand théorème de Fermat, cas n=2, « l'idée de Lagrange »

Tout le monde sait que l'équation $x^2+y^2=z^2$ admet des solutions par entières non nulles, par exemple on a : $9^2+12^2=15^2$.
Faisons un changement de signe, là aussi l'équation $x^2-y^2=z^2$ admet aussi des solutions par entières non nulles, par exemple on a :$13^2-12^2=5^2$.
Les deux équations forment un système soluble par entiers non nuls, que j'appels système de permutation d'ordre 2, tel que :

$$Sp_2 := \begin{cases} x_1^2 + y^2 = z_1^2 \\ x_2^2 - y^2 = z_2^2 \end{cases}$$

Ce système est soluble dans *Z**, car on a :

$$\begin{cases} 9^2 + 12^2 = 15^2 \\ 13^2 - 12^2 = 5^2 \end{cases}$$

On peut donc supposé qu'on a l'équivalence suivant :

$$Z^* \| Sp_2 \| Z^* \Leftrightarrow Z^* \| u^2 + v^2 = w^2 \| Z^*$$

<u>*Le grand théorème de Fermat, cas n*=3</u>

Soit $Sp_3 := \begin{cases} x_1^3 + y^3 = z_1^3 \\ x_2^3 + jy^3 = z_2^3 \\ x_3^3 + j^2 y^3 = z_3^3 \end{cases}$ avec $j = \exp\left(\frac{2\pi i}{3}\right)$, et on a,

$$Q^* \| Sp_3 \| Q^* \text{ si et selement si } Q^* \| u^3 + v^3 = w^3 \| Q^*$$

<u>*Preuve* :</u>

Premier sens, on suppose que $Q^* \| Sp_3 \| Q^*$ est vraie, puis on pose $u = x_1$, $v = y$ et $w = z_1$ donc $Q^* \| u^3 + v^3 = w^3 \| Q^*$ est vraie.

Second sens, on suppose que $Q^* \| u^3 + v^3 = w^3 \| Q^*$ est vraie, notons que le système Sp_3 contient 7 inconnus, donc par hypothèse que $Q^* \| u^3 + v^3 = w^3 \| Q^*$ est vraie, on pose $x_1 = u$, $y = v$ et $z_1 = w$, donc il ne reste que de prouver que les 4 inconnus restantes peuvent êtres des rationnels non nuls.

Dans le système Sp_3 on fait l'addition des trois équations, tel que,

$$x_1^3 + x_2^3 + x_3^3 = z_1^3 + z_2^3 + z_3^3$$

$$\text{Car } j^2 + j + 1 = 0$$

$$\text{Donc,}$$

$$x_2^3 + x_3^3 = y^3 + z_2^3 + z_3^3$$

Le lemme me permet de poser y=1, et donc,

$$x_2^3 + x_3^3 = 1 + z_2^3 + z_3^3$$

Et on a $Q^* \| x_2^3 + x_3^3 = 1 + z_2^3 + z_3^3 \| Q^*$ est vrais, par exemple $7^3 + 8^3 = 1^3 + 5^3 + 9^3$, elle admet même une infinité des solution, par exemple,

$$(2N+1)^3 + (2N+2)^3 = 1^3 + \left(2N + 1 + \sqrt{N+1}\right)^3 + \left(2N + 1 - \sqrt{N+1}\right)^3$$

Donc les 4 inconnus restantes peuvent êtres des rationnels non nuls, cela prouve l'équivalence.

Le système Sp_3 ne peut pas être soluble à cause du nombre complexe j, en vertu l'équation de Fermat ne peut pas être aussi soluble.

CQFD

<u>*Le grand théorème de Fermat cas n*≥4</u>

Soit $\zeta = \exp\left(\frac{2\pi i}{n}\right)$, le système de permutation d'ordre *n* s'écrie comme suivant ,

$$Sp_n := \begin{cases} x_1^n + y^n = z_1^n \\ x_2^n + \zeta y^n = z_2^n \\ x_3^n + \zeta^2 y^n = z_3^n \\ ..[].. \\ x_n^n + \zeta^{n-1} y^n = z_n^n \end{cases}$$

Et on a,

$$Q^* \| Sp_n \| Q^* \Leftrightarrow Q^* \| u^n + v^n = w^n \| Q^*$$

Preuve :

Le même raisonnement comme pour le cas n=3 nous conduit à la résolvante suivante :

$$S_n := \left(\sum_{j=2}^{n} x_j^n = 1^n + \sum_{j=2}^{n} z_j^n \right)$$

Cette résolvante est au moins soluble dans Q^*, pour les cas 4, 5, 6 et 7, car on a,

$$12^4 + 13^4 + 21^4 = 1^4 + 4^4 + 17^4 + 20^4$$
$$5^5 + 8^5 + 13^5 + 14^5 = 1^5 + 6^5 + 7^5 + 11^5 + 15^5$$
$$2^6 + 5^6 + 20^6 + 26^6 + 27^6 = 1^6 + 6^6 + 8^6 + 18^6 + 25^6 + 28^6$$
$$3^7 + 6^7 + 16^7 + 18^7 + 22^7 + 28^7 = 1^7 + 2^7 + 7^7 + 11^7 + 21^7 + 24^7 + 27^7$$

Pour ces 4 cas, $Q^* \| Sp_n \| Q^*$ est fausse, à cause du nombre complexe ζ, et donc par équivalence on a, $Q^* \| u^n + v^n = w^n \| Q^*$ est aussi fausse, ce qui prouve le théorème de Fermat pour ces premiers cas.

Le lien avec le travail de Lagrange

Soient les deux équations suivantes,

$$(S_n) := \left(\sum_{j=1}^{n-1} x_j^n = \sum_{j=1}^{n} z_j^n \right)$$
$$(S_{n,d}) := \left(\sum_{j=1}^{d-1} x_j^n = \sum_{j=1}^{d} z_j^n \right)$$

Avec d un diviseur propre de n, « $d \neq n$ & $d \neq 1$ ».

Le problème qu'on a avec ces deux équations c'est que la première est toujours soluble, alors que la seconde ne l'est pas, et on écrie,

$Z^* \| S_n \| Z^*$ est vrai

$Z^* \| S_{n,d} \| Z^*$ est faux.

N'essaient pas de prouver ça, car c'est très compliqué, ce que je propose c'est de le comprendre, et pour le comprendre je propose de chercher par ordinateur les solutions de ces deux équations.

En revanche il est possible de les démontrer cas par cas, donc pour la première équation (S_n), et comme on a vue déjà des solutions de type suivant,

$$7^3 + 8^3 = 1^3 + 5^3 + 9^3$$
$$12^4 + 13^4 + 21^4 = 1^4 + 4^4 + 17^4 + 20^4$$
$$5^5 + 8^5 + 13^5 + 14^5 = 1^5 + 6^5 + 7^5 + 11^5 + 15^5$$
$$2^6 + 5^6 + 20^6 + 26^6 + 27^6 = 1^6 + 6^6 + 8^6 + 18^6 + 25^6 + 28^6$$

$$3^7+6^7+16^7+18^7+22^7+28^7=1^7+2^7+7^7+11^7+21^7+24^7+27^7$$

Pour la seconde équation on fait le même raisonnement, par exemple on prend le cas n=6 avec d=3, et on a,

$$(S_{6,3}) := (x_2^6+x_3^6=z_1^6+z_2^6+z_3^6)$$

En effet, soit le système suivant,

$$(Sys) := \begin{cases} u_1^6+v_1^6+w^6=s_1^6+t_1^6 \\ u_2^6+v_2^6+jw^6=s_2^6+t_2^6 \\ u_3^6+v_3^6+j^2w^6=s_3^6+t_3^6 \end{cases}$$

Avec $j^2+j+1=0$.

On a,

$$Q^*\|Sys\|Q^* \text{ Si et seulement si } Q^*\left\|x_2^6+x_3^6=z_1^6+z_2^6+z_3^6\right\|Q^*$$

Le premier sens est évident, car l'équation ($S_{6,3}$) est membre du (*Sys*), pour le second sens on fait l'addition des trois équations du système (*Sys*), ce qui donne,

$$u_1^6+v_1^6+u_2^6+v_2^6+u_3^6+v_3^6=s_1^6+t_1^6+s_2^6+t_2^6+s_3^6+t_3^6$$

Donc,

$$u_2^6+v_2^6+u_3^6+v_3^6=w^6+s_2^6+t_2^6+s_3^6+t_3^6$$

Et on a, $Q^*\left\|u_2^6+v_2^6+u_3^6+v_3^6=w^6+s_2^6+t_2^6+s_3^6+t_3^6\right\|Q^*$ est vrai, exemple,

$$13^6+23^6+24^6+34^6=1^6+8^6+21^6+30^6+32^6.$$

Ceci prouve l'équivalence, comme la solubilité de (*Sys*) est impossible, à cause du nombre complexe *j*, alors par équivalence l'équation ($S_{6,3}$) est aussi non soluble.

Lien avec la théorie de Galois

L'équation de Fermat est une équation à plusieurs inconnus, dite aussi une équation diophantienne, « *on se limite au cas des équations polynomiaux à plusieurs inconnus et à coefficients rationnels* », lorsque on pose la question suivante, est ce que la théorie de Galois peut justifier ce genre d'équation ? La plupart des mathématiciennes répondent par la négation, moi je pense que toute équation diophantienne à une justification de Galois, c'est vrai que ce n'est pas un travail facile, mais je peux donner des exemples.

Soit,

$$x^5-10yx-5y^5=0$$

Avec,

$$xy\neq 0$$

Cette équation diophantienne est non résoluble, et elle peut être justifié par la théorie de Galois.

Preuve

D'après un critère de Richard Dedekind, tout sous groupe transitive de *Sn* contenant une transposition, et un (*n*-1)-cycle, est forcément égale à *Sn* tout entier[1].

Donc pour une équation de cinquième degré qui vérifie les deux conditions suivantes,

- Un couple des solutions complexe, et trois solutions réelles.
- Irréductible.

Alors certainement son groupe de Galois vérifie le critère de Dedekind, et donc il vaut à S_5 qu'est non résoluble, par exemple $x^5-10x-5=0$.

[1] Wikipidia

Soit *y* un nombre complexe quelconque non nul, si je multiple chaque solution de l'équation $x^5-10x-5=0$ par *y*, j'obtient l'équation $x^5-10yx-5y^5=0$, comme $x^5-10x-5=0$ est non résoluble par radicaux, alors il est de même pour l'équation $x^5-10yx-5y^5=0$.
Cela veut dire que non seulement il n'existe aucun couple rationnel non nul qui vérifie cette équation, mais il n'existe aucun couple des radicaux qui s'obtient par cette équation.
CQFD
Normalement lorsque on parle de la solubilité d'une équation diophantienne, on parle de sa solubilité par entier, cette notion doit être totalement abandonné, au moins pour la raisons suivante, si une équation admet des solutions par entiers, c'est que son corps de solution est tout simplement *Q*, sinon alors il y a deux cas, soit elle n'admet pas un corps de solution comme pour l'exemple précédent, ou soit elle admet un corps de solution, qu'est une extension finie et minimale de *Q*, exemple $x^2+xy+y^2=0$ avec $xy\neq 0$, son corps de solution est $Q(i\sqrt{3})$, il est minimale car aucune solution dans *Q* n'est possible.

Pour l'équation de Fermat $x^n+y^n=z^n$ avec $xyz\neq 0$, la première chose à retenir est le fait qu'elle toujours résoluble par radicaux, car $z=\sqrt[n]{x^n+y^n}$ est bien une radicale. Cela a une conséquence importante, c'est que l'équation de Fermat admet un corps de solution.
Lemme

Soient *a* et *b* deux nombres complexes, et *n*≥2 un entier.

Soit $E=\left\{(a+b),(a^2+b^2),(a^3+b^3)\ ..[]..\ (a^n+b^n)\right\}$

$E\subset Q$ si et seulement si, *a* et *b* sont des radicaux de seconde degré, « *a et b sont des conjugués dans* $Q(\sqrt{\delta})$, $a=r+s\sqrt{\delta}$ & $b=r-s\sqrt{\delta}$ »

La démonstration est facile, ce lemme est très important, malheureusement il n'est pas suffisant, mais au moins il nous permet de comprend la nature des solution de l'équation de Fermat.
Forme paramétrique de l'équation
Sous l'hypothèse que l'équation $x^n+y^n=z^n$ est soluble dans Q^*, alors ils existent deux rationnels non nuls *a* et *b* tel que, $x=z-a$ et $y=z-b$, donc,

$$(z-a)^n+(z-b)^n-z^n=0$$

On développe et on obtient,

$$z^n+\sum_{j=1}^{n}(-1)^j\binom{n}{j}(a^j+b^j)z^{n-j}=0$$

On pose $H_n(z)=z^n+\sum_{j=1}^{n}(-1)^j\binom{n}{j}(a^j+b^j)z^{n-j}=(z-a)^n+(z-b)^n-z^n$, ainsi l'équation de Fermat devient,

$$H_n(z)=0$$

Et on a le théorème suivant :

Théorème
$H_n(z)\in Q[X]$ si et seulement si les deux paramètres *a* et *b* sont des radicaux de second degré.
Preuve
C'est une conséquence immédiate du lemme précédent.

Exemples :
Pour n=3

$$\left(18+17\sqrt{2}\right)^3+\left(18-17\sqrt{2}\right)^3=42^3$$
$$\left(9+\sqrt{5}\right)^3+\left(9-\sqrt{5}\right)^3=12^3$$
$$\left(6+5\sqrt{6}\right)^3+\left(6-5\sqrt{6}\right)^3=18^3$$
..[]..

On a même une solution double,
Une solution double veut dire que c'est une solution à la fois de $x^3+y^3=z^3$ et de $x^2+y^2=z^2$, car en général on a $dH_n(z)/dz=nH_{n-1}(z)$.
Le calcule du discriminant de $H_3(z)$ donne,

$$disc\left(H_3(z)\right)=-27a^2b^2\left(9(a^2+b^2)-14ab\right)$$

Dans Q, $disc\left(H_3(z)\right)=0$ conduit aux solutions triviales, en particulier le terme $9(a^2+b^2)-14ab$ est toujours positive, et il s'annule seulement en $a=b=0$.
Dans le cas d'une extension quadratique $Q(\sqrt{\delta})$, on pose $a=r+s\sqrt{\delta}$ et $b=r-s\sqrt{\delta}$ donc $9(a^2+b^2)-14ab=0$ conduit à $r^2=-8s^2\delta$, forcément on a $\delta=-2$, et donc $r=4s$ on trouve que $a=s\left(4+i\sqrt{2}\right)$ et $b=s\left(4-i\sqrt{2}\right)$, donc $H_3(z)=(z-2s)^2(z-20s)$ ainsi on a,

$$(-2+\mathrm{i}\sqrt{2})^3+(-2-i\sqrt{2})^3=8$$
&
$$(-2+\mathrm{i}\sqrt{2})^2+(-2-i\sqrt{2})^2=4$$

Et c'est l'unique solution double à un facteur commun près. « *Le petit s* ».
Pour n≥4

Pour les ordres supérieurs les solutions deviennent de plus en plus très rares, donc pour trouver quelque unes il faut rusé,

$$(1+i\sqrt{7})^4+(1-i\sqrt{7})^4=2^4$$
$$(1+i\sqrt{3})^5+(1-i\sqrt{3})^5=2^5$$
$$(1+i\sqrt{3})^7+(1-i\sqrt{3})^7=2^7$$

Même si ça ne prouve pas que les solutions ne puissent pas êtres des rationnels, mais je pense que le corps des solutions de l'équation de Fermat est toujours un corps quadratique $Q(\sqrt{\delta})$, et vous que pensez vous ?

Merci pour la lecture de ce papier
Cordialement
Méhdi Pascal
MehdiPascal38@gmail.com