

À la recherche des racines

Cécile Armana

IREM de Franche-Comté, Laboratoire de Mathématiques de Besançon
Université de Franche-Comté

Lycée Jules Haag – 23 mai 2013

(Lm^B)



UFC
UNIVERSITÉ
DE FRANCHE-COMTÉ

Nos protagonistes

Un polynôme...

l'expression $a_n x^n + a_{n-1} x^{n-1} + \dots + a_2 x^2 + a_1 x + a_0$

$n \geq 1$, $a_n, \dots, a_0$ des fractions d'entiers

Nos protagonistes

Un polynôme...

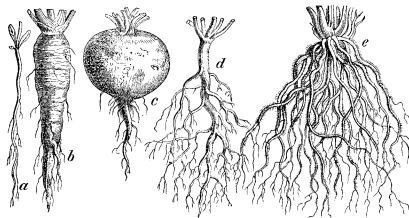
l'expression $a_n x^n + a_{n-1} x^{n-1} + \dots + a_2 x^2 + a_1 x + a_0$

$n \geq 1$, $a_n, \dots, a_0$ des fractions d'entiers

Ses racines...

les nombres réels x solutions de l'équation

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_2 x^2 + a_1 x + a_0 = 0$$



Des exemples !

$$x + 1, \quad 2x + 3, \quad x^2 - 1, \quad 5x^3 + x + 2/3, \dots$$

Des exemples !

$$x + 1, \quad 2x + 3, \quad x^2 - 1, \quad 5x^3 + x + 2/3, \dots$$

Le degré...

est le plus grand exposant qui apparaît dans le polynôme.

Des exemples !

$$x + 1, \quad 2x + 3, \quad x^2 - 1, \quad 5x^3 + x + 2/3, \dots$$

Le degré...

est le plus grand exposant qui apparaît dans le polynôme.

Un aquarium de 6 litres est 10 cm plus haut qu'il n'est large et 10 cm plus long qu'il n'est haut. Quelles sont ses dimensions ?

Longueur L , largeur ℓ , hauteur x (en dm)

$$x = \ell + 1, \quad L = x + 1, \quad L\ell x = 6$$

$$(x + 1)(x - 1)x = 6$$

$$x^3 - x - 6 = 0 \quad (\text{degré } 3)$$



©Citron / CC-BY-SA-3.0

Les racines ?

Théorème

Un polynôme de degré n admet au plus n racines réelles.

En existe-t-il ?

Les racines ?

Théorème

Un polynôme de degré n admet au plus n racines réelles.

En existe-t-il ?

Pas toujours : $x^2 + 1$ n'a pas de racines réelles.

Les racines ?

Théorème

Un polynôme de degré n admet au plus n racines réelles.

En existe-t-il ?

Pas toujours : $x^2 + 1$ n'a pas de racines réelles.

S'il en existe, comment les calculer ?

Les racines ?

Théorème

Un polynôme de degré n admet au plus n racines réelles.

En existe-t-il ?

Pas toujours : $x^2 + 1$ n'a pas de racines réelles.

S'il en existe, comment les calculer ?

- résolution exacte : les racines de $x^2 - 2$ sont $\sqrt{2}$ et $-\sqrt{2}$
- résolution approchée : une racine de $x^3 + x + 1$ a pour valeur approchée -0.6823278038 .
- **formules donnant les valeurs exactes des racines** en fonction des coefficients du polynôme

L'équation de degré 1

$$ax + b = 0$$

Elle a une seule racine : $-\frac{b}{a}$



Bilder ur Nordens Flora – source : Wikipedia

L'équation de degré 1

$$ax + b = 0$$

Elle a une seule racine : $-\frac{b}{a}$

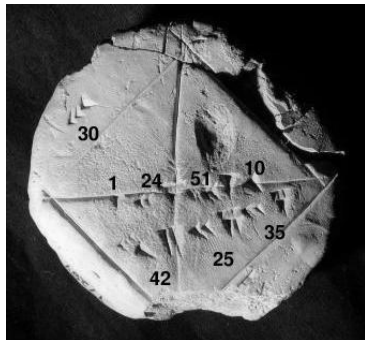


Bilder ur Nordens Flora – source : Wikipedia

Degré = complexité du calcul des racines

L'équation de degré 2

Babylone, 1800-1500 av. J.-C.



Tablette YBC 7289, collection babylonienne de Yale – source : Wikipedia

Diophante (grec, 3^e siècle)

Al-Khwarizmi (perse, 9^e siècle)

L'équation de degré 2

$$ax^2 + bx + c = 0$$

$$\Delta = b^2 - 4ac \quad (\text{discriminant})$$

L'équation de degré 2

$$ax^2 + bx + c = 0$$

$$\Delta = b^2 - 4ac \quad (\text{discriminant})$$

- Si $\Delta > 0$, deux racines :

$$\frac{-b - \sqrt{\Delta}}{2a}, \frac{-b + \sqrt{\Delta}}{2a}$$

- Si $\Delta = 0$, une seule racine :

$$\frac{-b}{2a}$$

- Si $\Delta < 0$, aucune racine.



Ginseng Panax

L'équation de degré 3

L'école italienne de la Renaissance et les confrontations mathématiques



source : Wikipedia

Scipio del Ferro (1465-1525)

Niccolò Fontana, dit Tartaglia (1499-1557)

Girolamo Cardano (1501-1576)

L'équation de degré 3

$$ax^3 + bx^2 + cx + d = 0 \quad \xrightarrow{y=x-\frac{b}{3}} \quad \boxed{y^3 + py + q = 0}$$

$$\Delta = q^2 + \frac{4p^3}{27} \quad (\text{discriminant})$$

L'équation de degré 3

$$ax^3 + bx^2 + cx + d = 0 \quad y = x - \frac{b}{3} \longrightarrow$$

$$y^3 + py + q = 0$$

$$\Delta = q^2 + \frac{4p^3}{27} \quad (\text{discriminant})$$

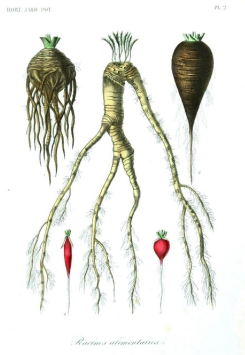
- Si $\Delta > 0$ alors **une racine** :

$$\sqrt[3]{\frac{-q + \sqrt{\Delta}}{2}} + \sqrt[3]{\frac{-q - \sqrt{\Delta}}{2}}$$

- Si $\Delta = 0$ alors **deux racines** :

$$\frac{3q}{p}, \frac{-3q}{2p}$$

- Si $\Delta < 0$: ...



L'équation de degré 3, cas $\Delta < 0$

L'exemple de Rafael Bombelli (1526-1572)

L'ALGEBRA OPERA

DI RAFAEL BOMBELLI da Bologna
Divisa in tre Libri.

*Con la quale ciascuno da se potrà venire in perfetta
cognitione della teorica dell' Arimetica.*

Con vna Tavola copiosa delle materie, che
in essa si contengono.

*Posta hora in luce à beneficio della studio di
detta professione.*



IN BOLOGNA,

Per Giovanni Rossi. MDLXXIX.

Con licenza de' Superiori

source : Wikipedia

L'équation de degré 3, cas $\Delta < 0$

$$x^3 - 15x - 4 = 0$$

$$\Delta = q^2 + \frac{4p^3}{27} = -484 = -22^2 < 0$$

L'équation de degré 3, cas $\Delta < 0$

$$x^3 - 15x - 4 = 0$$

$$\Delta = q^2 + \frac{4p^3}{27} = -484 = -22^2 < 0$$

- Imaginons qu'il existe un nombre i vérifiant $i^2 = -1$.

$$\Delta = (22i)^2 \quad \text{donc} \quad \ll \sqrt{\Delta} = 22i \gg$$

L'équation de degré 3, cas $\Delta < 0$

$$x^3 - 15x - 4 = 0$$

$$\Delta = q^2 + \frac{4p^3}{27} = -484 = -22^2 < 0$$

- Imaginons qu'il existe un nombre i vérifiant $i^2 = -1$.

$$\Delta = (22i)^2 \quad \text{donc} \quad \ll \sqrt{\Delta} = 22i \gg$$

- On applique la formule du cas $\Delta > 0$:

$$\sqrt[3]{\frac{4 + 22i}{2}} + \sqrt[3]{\frac{4 - 22i}{2}} =$$

L'équation de degré 3, cas $\Delta < 0$

$$x^3 - 15x - 4 = 0$$

$$\Delta = q^2 + \frac{4p^3}{27} = -484 = -22^2 < 0$$

- Imaginons qu'il existe un nombre i vérifiant $i^2 = -1$.

$$\Delta = (22i)^2 \quad \text{donc} \quad \ll \sqrt{\Delta} = 22i \gg$$

- On applique la formule du cas $\Delta > 0$:

$$\sqrt[3]{\frac{4+22i}{2}} + \sqrt[3]{\frac{4-22i}{2}} = \sqrt[3]{2+11i} + \sqrt[3]{2-11i} =$$

L'équation de degré 3, cas $\Delta < 0$

$$x^3 - 15x - 4 = 0$$

$$\Delta = q^2 + \frac{4p^3}{27} = -484 = -22^2 < 0$$

- Imaginons qu'il existe un nombre i vérifiant $i^2 = -1$.

$$\Delta = (22i)^2 \quad \text{donc} \quad \ll \sqrt{\Delta} = 22i \gg$$

- On applique la formule du cas $\Delta > 0$:

$$\sqrt[3]{\frac{4+22i}{2}} + \sqrt[3]{\frac{4-22i}{2}} = \sqrt[3]{2+11i} + \sqrt[3]{2-11i} = (2+i) + (2-i) = 4$$

On « devine » que 4 est une racine.

L'équation de degré 3, cas $\Delta < 0$

$$x^3 - 15x - 4 = 0$$

$$\Delta = q^2 + \frac{4p^3}{27} = -484 = -22^2 < 0$$

- Imaginons qu'il existe un nombre i vérifiant $i^2 = -1$.

$$\Delta = (22i)^2 \quad \text{donc} \quad \ll \sqrt{\Delta} = 22i \gg$$

- On applique la formule du cas $\Delta > 0$:

$$\sqrt[3]{\frac{4+22i}{2}} + \sqrt[3]{\frac{4-22i}{2}} = \sqrt[3]{2+11i} + \sqrt[3]{2-11i} = (2+i) + (2-i) = 4$$

On « devine » que 4 est une racine.

Invention des nombres complexes !

L'équation de degré 3, cas $\Delta < 0$

$$x^3 - 15x - 4 = 0$$

$$\Delta = q^2 + \frac{4p^3}{27} = -484 = -22^2 < 0$$

- Imaginons qu'il existe un nombre i vérifiant $i^2 = -1$.

$$\Delta = (22i)^2 \quad \text{donc} \quad \ll \sqrt{\Delta} = 22i \gg$$

- On applique la formule du cas $\Delta > 0$:

$$\sqrt[3]{\frac{4+22i}{2}} + \sqrt[3]{\frac{4-22i}{2}} = \sqrt[3]{2+11i} + \sqrt[3]{2-11i} = (2+i) + (2-i) = 4$$

On « devine » que 4 est une racine.

Invention des nombres complexes !

Détour obligatoire par les nombres complexes mais la racine est réelle
(*casus irreducibilis*)

L'équation de degré 3, cas $\Delta < 0$

Si $\Delta < 0$, on a **trois racines** décrites par la formule :

$$\sqrt[3]{\frac{-q + \sqrt{\Delta}}{2}} + \sqrt[3]{\frac{-q - \sqrt{\Delta}}{2}}$$

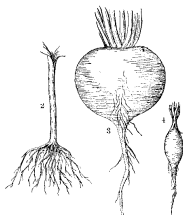
L'équation de degré 3, cas $\Delta < 0$

Si $\Delta < 0$, on a **trois racines** décrites par la formule :

$$\sqrt[3]{\frac{-q + \sqrt{\Delta}}{2}} + \sqrt[3]{\frac{-q - \sqrt{\Delta}}{2}}$$

- deux choix possibles pour chaque racine carrée complexe
- trois choix possibles pour chaque racine cubique complexe

Par symétrie on trouve en fait exactement **trois racines réelles**.



L'équation de degré 4

Lodovico Ferrari (1522-1565)

Théorème

Les quatre racines (complexes) de $x^4 + ax^3 + bx^2 + cx + d$ sont :

$$\begin{aligned}
 x_1 &= -\frac{a}{4} + \sqrt{\frac{a^2}{16} - \frac{b}{4}} + \frac{\frac{a^3}{64} - \frac{ab}{8} + \frac{b^2}{16}}{\sqrt{\frac{a^2}{16} - \frac{b}{4}}} + \sqrt{\frac{a^2}{16} - \frac{b}{4} - \frac{\frac{a^3}{64} - \frac{ab}{8} + \frac{b^2}{16}}{\sqrt{\frac{a^2}{16} - \frac{b}{4}}}} \\
 x_2 &= -\frac{a}{4} + \sqrt{\frac{a^2}{16} - \frac{b}{4}} - \frac{\frac{a^3}{64} - \frac{ab}{8} + \frac{b^2}{16}}{\sqrt{\frac{a^2}{16} - \frac{b}{4}}} + \sqrt{\frac{a^2}{16} - \frac{b}{4} + \frac{\frac{a^3}{64} - \frac{ab}{8} + \frac{b^2}{16}}{\sqrt{\frac{a^2}{16} - \frac{b}{4}}}} \\
 x_3 &= -\frac{a}{4} + \sqrt{\frac{a^2}{16} - \frac{b}{4}} - \sqrt{\frac{a^2}{16} - \frac{b}{4} - \frac{\frac{a^3}{64} - \frac{ab}{8} + \frac{b^2}{16}}{\sqrt{\frac{a^2}{16} - \frac{b}{4}}}} + \frac{\frac{a^3}{64} - \frac{ab}{8} + \frac{b^2}{16}}{\sqrt{\frac{a^2}{16} - \frac{b}{4} - \frac{\frac{a^3}{64} - \frac{ab}{8} + \frac{b^2}{16}}{\sqrt{\frac{a^2}{16} - \frac{b}{4}}}}} \\
 x_4 &= -\frac{a}{4} + \sqrt{\frac{a^2}{16} - \frac{b}{4}} - \sqrt{\frac{a^2}{16} - \frac{b}{4} + \frac{\frac{a^3}{64} - \frac{ab}{8} + \frac{b^2}{16}}{\sqrt{\frac{a^2}{16} - \frac{b}{4}}}} - \frac{\frac{a^3}{64} - \frac{ab}{8} + \frac{b^2}{16}}{\sqrt{\frac{a^2}{16} - \frac{b}{4} + \frac{\frac{a^3}{64} - \frac{ab}{8} + \frac{b^2}{16}}{\sqrt{\frac{a^2}{16} - \frac{b}{4}}}}}
 \end{aligned}$$

L'équation de degré 4

$$r_1 = \frac{-a}{4} - \frac{1}{2} \sqrt{\frac{a^2}{4} - \frac{2b}{3} + \frac{2^{\frac{1}{3}}(b^2 - 3ac + 12d)}{3\left(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + \sqrt{-4(b^2 - 3ac + 12d)^3 + (2b^3 - 9abc + 27c^2 + 27a^2d - 72bd)^2}\right)}}$$

$$r_2 = \frac{-a}{4} - \frac{1}{2} \sqrt{\frac{a^2}{4} - \frac{2b}{3} + \frac{2^{\frac{1}{3}}(b^2 - 3ac + 12d)}{3\left(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + \sqrt{-4(b^2 - 3ac + 12d)^3 + (2b^3 - 9abc + 27c^2 + 27a^2d - 72bd)^2}\right)}}$$

$$r_3 = \frac{-a}{4} + \frac{1}{2} \sqrt{\frac{a^2}{4} - \frac{2b}{3} + \frac{2^{\frac{1}{3}}(b^2 - 3ac + 12d)}{3\left(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + \sqrt{-4(b^2 - 3ac + 12d)^3 + (2b^3 - 9abc + 27c^2 + 27a^2d - 72bd)^2}\right)}}$$

$$r_4 = \frac{-a}{4} + \frac{1}{2} \sqrt{\frac{a^2}{4} - \frac{2b}{3} + \frac{2^{\frac{1}{3}}(b^2 - 3ac + 12d)}{3\left(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + \sqrt{-4(b^2 - 3ac + 12d)^3 + (2b^3 - 9abc + 27c^2 + 27a^2d - 72bd)^2}\right)}}$$

L'équation de degré 4

$$-a^3 + 4ab - 8c$$

$$\frac{2^{\frac{1}{3}}(b^2 - 3ac + 12d)}{c + 27c^2 + 27a^2d - 72bd + \sqrt{-4(b^2 - 3ac + 12d)^3 + (2b^3 - 9abc + 27c^2 + 27a^2d - 72bd)^2}}^{\frac{1}{3}} + \left(\frac{2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + \sqrt{-4(b^2 - 3ac + 12d)^3 + (2b^3 - 9abc + 27c^2 + 27a^2d - 72bd)^2}}{54} \right)^{\frac{1}{3}}$$

$$-a^3 + 4ab - 8c$$

$$\frac{2^{\frac{1}{3}}(b^2 - 3ac + 12d)}{c + 27c^2 + 27a^2d - 72bd + \sqrt{-4(b^2 - 3ac + 12d)^3 + (2b^3 - 9abc + 27c^2 + 27a^2d - 72bd)^2}}^{\frac{1}{3}} + \left(\frac{2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + \sqrt{-4(b^2 - 3ac + 12d)^3 + (2b^3 - 9abc + 27c^2 + 27a^2d - 72bd)^2}}{54} \right)^{\frac{1}{3}}$$

$$-a^3 + 4ab - 8c$$

$$\frac{2^{\frac{1}{3}}(b^2 - 3ac + 12d)}{c + 27c^2 + 27a^2d - 72bd + \sqrt{-4(b^2 - 3ac + 12d)^3 + (2b^3 - 9abc + 27c^2 + 27a^2d - 72bd)^2}}^{\frac{1}{3}} + \left(\frac{2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + \sqrt{-4(b^2 - 3ac + 12d)^3 + (2b^3 - 9abc + 27c^2 + 27a^2d - 72bd)^2}}{54} \right)^{\frac{1}{3}}$$

$$-a^3 + 4ab - 8c$$

Un bilan

Formules pour les degrés 1 à 4

- ... de plus en plus compliquées !

Un bilan

Formules pour les degrés 1 à 4

- ... de plus en plus compliquées !
- elles donnent les racines en fonction des **coefficients** du polynôme et des **opérations** : $+$, $-$, $\times$, $\div$ et $\sqrt{}$, $\sqrt[3]{}$, ... (radicaux)

Un bilan

Formules pour les degrés 1 à 4

- ... de plus en plus compliquées !
- elles donnent les racines en fonction des **coefficients** du polynôme et des **opérations** : $+$, $-$, $\times$, $\div$ et $\sqrt{}$, $\sqrt[3]{}$, ... (radicaux)

Question (résolubilité par radicaux)

Pour $n \geq 5$, existe-t-il des formules donnant les racines de n'importe quel polynôme de degré n sous forme de radicaux ?

Vers le degré 5

Des avancées

- Leonhard Euler (1764) : $x^5 - 2625x - 61500$ admet pour racine

$$\sqrt[5]{75(5 + 4\sqrt{10})} + \sqrt[5]{225(35 + 11\sqrt{10})} + \sqrt[5]{225(35 - 11\sqrt{10})} + \sqrt[5]{75(5 - 4\sqrt{10})}$$

- Joseph-Louis Lagrange (1771) : synthèse

Vers le degré 5

Des avancées

- Leonhard Euler (1764) : $x^5 - 2625x - 61500$ admet pour racine

$$\sqrt[5]{75(5 + 4\sqrt{10})} + \sqrt[5]{225(35 + 11\sqrt{10})} + \sqrt[5]{225(35 - 11\sqrt{10})} + \sqrt[5]{75(5 - 4\sqrt{10})}$$

- Joseph-Louis Lagrange (1771) : synthèse

Puis le doute

[...] il semble donc qu'on pourrait conclure de là par induction que toute équation, de quelque degré qu'elle soit, sera aussi résoluble à l'aide d'une réduite dont les racines [...] Mais d'après ce que nous avons démontré on a, ce semble, lieu de se convaincre d'avance que cette conclusion se trouvera en défaut dès le cinquième degré. D'où il s'ensuit que, si la résolution algébrique des équations de degrés supérieurs au quatrième n'est pas impossible, elle doit dépendre de quelques fonctions des racines, différentes de la précédente.
(Lagrange)

Le degré 5 et au-delà

Théorème (Abel, 1826 – Galois, 1829)

Il n'existe aucune formule générale permettant d'exprimer les racines de n'importe quel polynôme de degré ≥ 5 par radicaux.

Le degré 5 et au-delà

Théorème (Abel, 1826 – Galois, 1829)

Il n'existe aucune formule générale permettant d'exprimer les racines de n'importe quel polynôme de degré ≥ 5 par radicaux.

Paolo Ruffini (1765-1822)

Pour degré 5, plusieurs preuves antérieures, incomplètes et parfois incomprises



Le degré 5 et au-delà

Théorème (Abel, 1826 – Galois, 1829)

Il n'existe aucune formule générale permettant d'exprimer les racines de n'importe quel polynôme de degré ≥ 5 par radicaux.

Niels Henrik Abel (1802-1829)

Travaux incompris jusqu'en 1830
(reconnaissance posthume)



Le degré 5 et au-delà

Théorème (Abel, 1826 – Galois, 1829)

Il n'existe aucune formule générale permettant d'exprimer les racines de n'importe quel polynôme de degré ≥ 5 par radicaux.

Évariste Galois (1811-1832)

- Travaux indépendants de ceux d'Abel.
- Mémoire perdu. Travaux retrouvés et compris à partir de 1843 !
- *Galois, à l'âge de 19 ans, a déjà à son actif des résultats mathématiques d'une portée incomparable qui sont l'acte de naissance des mathématiques contemporaines. (Alain Connes)*



La portée du résultat

« Il n'existe pas de formule générale en degré ≥ 5 »



La portée du résultat

« Il n'existe pas de formule générale en degré ≥ 5 »



- Un des premiers résultats d'impossibilité en mathématiques !

La portée du résultat

« Il n'existe pas de formule générale en degré ≥ 5 »



- Un des premiers résultats d'impossibilité en mathématiques !
- Cela n'empêche pas certains polynômes de degré ≥ 5 d'avoir des racines exprimables par radicaux.

Exemple : $x^5 - 1$ a pour racine 1.

La portée du résultat

« Il n'existe pas de formule générale en degré ≥ 5 »



- Un des premiers résultats d'impossibilité en mathématiques !
- Cela n'empêche pas certains polynômes de degré ≥ 5 d'avoir des racines exprimables par radicaux.

Exemple : $x^5 - 1$ a pour racine 1.

- Théorème (d'Alembert-Gauss, fin 18^e-début 19^e siècle). Tout polynôme de degré n admet exactement n racines complexes.

La vie de Galois (1811-1832)



- Un élève rebelle et frondeur

C'est la fureur des Mathématiques qui le domine ; aussi je pense qu'il vaudrait mieux pour lui que ses parents consentent à ce qu'il ne s'occupe que de cette étude ; il perd son temps ici et n'y fait que tourmenter ses maîtres et se faire accabler de punitions.

Commentaire de son maître d'étude, 1827-1828.

La vie de Galois (1811-1832)



- Un élève rebelle et frondeur
- L'engagement politique



Prison Saint Pélagie

La vie de Galois (1811-1832)



- Un élève rebelle et frondeur
- L'engagement politique
- Un génie précoce et incompris

PURES ET APPLIQUÉES.

417

MÉMOIRE

Sur les conditions de résolubilité des équations par radicaux.

Le Mémoire ci-joint [*] est extrait d'un ouvrage que j'ai eu l'honneur de présenter à l'Académie il y a un an. Cet ouvrage n'ayant pas été compris, les propositions qu'il renferme ayant été révoquées en doute, j'ai dû me contenter de donner, sous forme synthétique, les principes généraux, et une *seule* application de ma théorie. Je supplie mes juges de lire du moins avec attention ce peu de pages.

On trouvera ici une *condition* générale à laquelle *satisfait toute équation soluble par radicaux*, et qui réciproquement assure leur résolubilité. On en fait l'application seulement aux équations dont le degré est un nombre premier. Voici le théorème donné par notre analyse :

« Pour qu'une équation de degré premier, qui n'a pas de diviseurs commensurables, soit soluble par radicaux, il *faut* et il *suffit* que toutes les racines soient des fonctions rationnelles de deux quelconques d'entre elles. »

Les autres applications de la théorie sont elles-mêmes autant de théories particulières. Elles nécessitent d'ailleurs l'emploi de la théorie des nombres, et d'un algorithme particulier : nous les réservons pour une autre occasion. Elles sont en partie relatives aux équations modulaires de la théorie des fonctions elliptiques, que nous démontrons ne pouvoir se résoudre par radicaux.

Ce 16 janvier 1831.

E. GALOIS.

[*] J'ai jugé convenable de placer en tête de ce Mémoire la préface qu'on va lire, bien que je l'aie trouvée biffée dans le manuscrit.

La vie de Galois (1811-1832)



- Un élève rebelle et frondeur
- L'engagement politique
- Un génie précocé et incompris
- Le destin tragique

Paris, le 29 mai 1832

Mon cher Ami,

J'ai fait en analyse plusieurs choses nouvelles. Les unes concernent la théorie des Équations, les autres les fonctions Intégrales. [...]

Tu prieras publiquement Jacobi ou Gauss de donner leur avis non sur la vérité, mais sur l'importance des théorèmes. Après cela il se trouvera, j'espère, des gens qui trouveront leur profit à déchiffrer tout ce gâchis.

Je t'embrasse avec effusion.

E. Galois

Les mathématiques de Galois

- Symétries des racines. Notion de groupe de permutations.

Les mathématiques de Galois

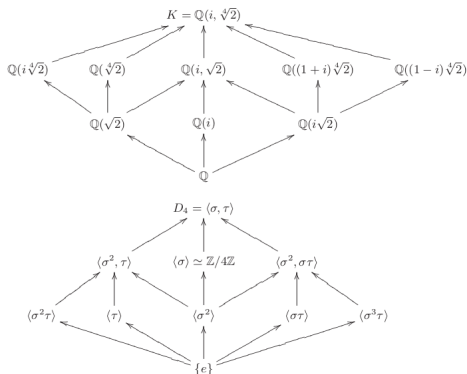
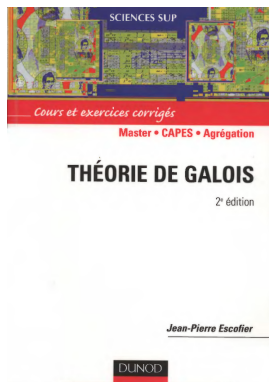
- Symétries des racines. Notion de groupe de permutations.
- Critère pour dire si un polynôme donné est résoluble par radicaux en termes du groupe des racines.
Exemple : $x^5 - 10x + 5$ n'a aucune racine exprimable par radicaux.

Les mathématiques de Galois

- **Symétries des racines.** Notion de **groupe de permutations**.
- **Critère** pour dire si un polynôme **donné** est résoluble par radicaux en termes du **groupe** des racines.
Exemple : $x^5 - 10x + 5$ n'a aucune racine exprimable par radicaux.
- **Obstruction** dans le cas général : « le groupe symétrique S_n n'est pas résoluble si $n \geq 5$ ».

Au-delà de Galois

- La théorie de Galois est enseignée en quatrième année à l'université



Au-delà de Galois

- La **théorie de Galois** est enseignée en quatrième année à l'université
- L'**algèbre moderne**

Au-delà de Galois

- La **théorie de Galois** est enseignée en quatrième année à l'université
- L'**algèbre moderne**
- **Théorie des corps finis** ; cryptographie, codes correcteurs d'erreurs

Au-delà de Galois

- La **théorie de Galois** est enseignée en quatrième année à l'université
- L'**algèbre moderne**
- Théorie des **corps finis** ; cryptographie, codes correcteurs d'erreurs
- Le **groupe de Galois** et ses prolongements sont des objets centraux des recherches actuelles algèbre, arithmétique, géométrie

Théorème (Fermat-Wiles, 1994)

Il n'existe pas de nombres entiers non nuls x , y et z tels que :

$$x^n + y^n = z^n$$

dès que $n \geq 3$.

Merci de votre attention !