Théorie de Galois : Introduction

Yves Laszlo

Laboratoire Laurent Schwartz (CMLS)

2 fevrier 2007

Nous allons esquisser deux succès historiquement importants de la théorie de Galois.

Nous allons esquisser deux succès historiquement importants de la théorie de Galois. Commençons par la construction à la règle et au compas des points du plan complexe.

Definition

On dira que $z \in \mathbf{C}$ est *constructible*

Definition

On dira que $z \in \mathbf{C}$ est *constructible* s'il existe une suite finie de points distincts

$$z_0, \cdots, z_N = z$$

tel que

Definition

On dira que $z \in \mathbf{C}$ est *constructible* s'il existe une suite finie de points distincts

$$z_0, \cdots, z_N = z$$

tel que $z_0 \in \{0, 1\}$ et

Definition

On dira que $z \in \mathbf{C}$ est *constructible* s'il existe une suite finie de points distincts

$$z_0, \cdots, z_N = z$$

tel que $z_0 \in \{0, 1\}$ et pour tout $n < N$ le point z_{n+1} est un des points d'une intersection finie de deux « droite ou cercle » de type

Definition

On dira que $z \in \mathbf{C}$ est *constructible* s'il existe une suite finie de points distincts

$$z_0, \cdots, z_N = z$$

tel que $z_0 \in \{0, 1\}$ et pour tout $n < N$ le point z_{n+1} est un des points d'une intersection finie de deux « droite ou cercle » de type

$$\langle z_\alpha, z_\beta \rangle, 0 \leq \alpha < \beta \leq n$$

Definition

On dira que $z \in \mathbf{C}$ est *constructible* s'il existe une suite finie de points distincts

$$z_0, \cdots, z_N = z$$

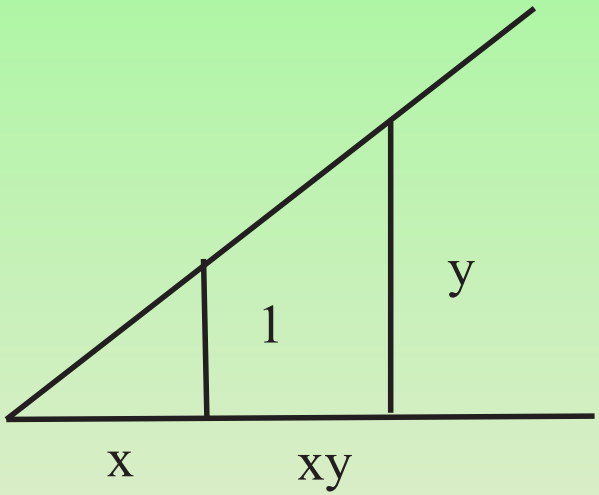
tel que $z_0 \in \{0, 1\}$ et pour tout $n < N$ le point z_{n+1} est un des points d'une intersection finie de deux « droite ou cercle » de type

$$\langle z_\alpha, z_\beta \rangle, 0 \leq \alpha < \beta \leq n$$

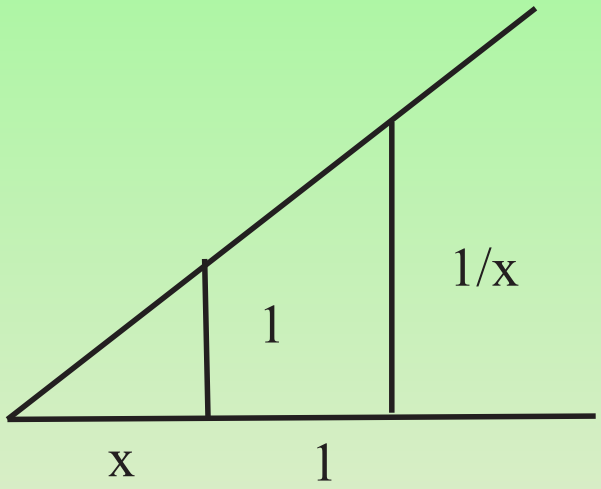
ou

$$C(z_\gamma, |z_\alpha - z_\beta|), \rangle, 0 \leq \alpha < \beta \leq n, \gamma \leq n.$$

En utilisant les théorèmes de Thales et Pythagore (cf. figure)



Produit



Inverse (0<x<1)

on obtient que l'ensemble des complexes constructibles est un sous-corps de $\mathbf{C}$.

on obtient que l'ensemble des complexes constructibles est un sous-corps de $\mathbf{C}$.
Par exemple, $\sqrt{2}$ est constructible, mais pas $\sqrt[3]{2}$: pourquoi ?

on obtient que l'ensemble des complexes constructibles est un sous-corps de $\mathbf{C}$.
Par exemple, $\sqrt{2}$ est constructible, mais pas $\sqrt[3]{2}$: pourquoi ?

Soit L_n le sous-corps de $\mathbf{C}$ engendré par $\sqrt{-1}$ et les coordonnées des $z_\alpha, \alpha \leq n$.

on obtient que l'ensemble des complexes constructibles est un sous-corps de $\mathbf{C}$.
Par exemple, $\sqrt{2}$ est constructible, mais pas $\sqrt[3]{2}$: pourquoi ?

Soit L_n le sous-corps de $\mathbf{C}$ engendré par $\sqrt{-1}$ et les coordonnées des $z_\alpha, \alpha \leq n$.
Mais (facile) z_{n+1} est solutions d'une équation de degré 2 à coefficients dans L_n.

on obtient que l'ensemble des complexes constructibles est un sous-corps de $\mathbf{C}$.
Par exemple, $\sqrt{2}$ est constructible, mais pas $\sqrt[3]{2}$: pourquoi ?

Soit L_n le sous-corps de $\mathbf{C}$ engendré par $\sqrt{-1}$ et les coordonnées des $z_\alpha, \alpha \leq n$.
Mais (facile) z_{n+1} est solutions d'une équation de degré 2 à coefficients dans L_n.Ainsi,

$$L_n[z_{n+1}] = \{a + bz_{n+1}, a, b \in L_n\}$$

est un *corps* de degré ≤ 2 sur L_n.

on obtient que l'ensemble des complexes constructibles est un sous-corps de $\mathbf{C}$.
Par exemple, $\sqrt{2}$ est constructible, mais pas $\sqrt[3]{2}$: pourquoi ?

Soit L_n le sous-corps de $\mathbf{C}$ engendré par $\sqrt{-1}$ et les coordonnées des $z_\alpha, \alpha \leq n$.
Mais (facile) z_{n+1} est solutions d'une équation de degré 2 à coefficients dans L_n.Ainsi,

$$L_n[z_{n+1}] = \{a + bz_{n+1}, a, b \in L_n\}$$

est un *corps* de degré ≤ 2 sur L_n.
La réciproque est facile et laissée au lecteur en devoir. On obtient

Theorem (Wantzel,1814-1848, Chargé de cours à Polytechnique.)

Le complexe z est constructible si et seulement si il existe une suite finie de corps $L_0 = \mathbf{Q} \subset L_1 \cdots \subset L_n$ et $[L_{i+1} : L_i] \leq 2$ avec $z \in L_n$.

Theorem (Wantzel,1814-1848, Chargé de cours à Polytechnique.)

Le complexe z est constructible si et seulement si il existe une suite finie de corps $L_0 = \mathbf{Q} \subset L_1 \cdots \subset L_n$ et $[L_{i+1} : L_i] \leq 2$ avec $z \in L_n$.

La réciproque fait naturellement intervenir la théorie de Galois.

Theorem (Wantzel,1814-1848, Chargé de cours à Polytechnique.)

Le complexe z est constructible si et seulement si il existe une suite finie de corps $L_0 = \mathbf{Q} \subset L_1 \cdots \subset L_n$ et $[L_{i+1} : L_i] \leq 2$ avec $z \in L_n$.

La réciproque fait naturellement intervenir la théorie de Galois.On a alors (exercice)

$$[L : \mathbf{Q}] = \prod [L_{i+1} : L_i] = 2^m$$

avec $m \leq n$ et donc

Theorem (Wantzel,1814-1848, Chargé de cours à Polytechnique.)

Le complexe z est constructible si et seulement si il existe une suite finie de corps $L_0 = \mathbf{Q} \subset L_1 \cdots \subset L_n$ et $[L_{i+1} : L_i] \leq 2$ avec $z \in L_n$.

La réciproque fait naturellement intervenir la théorie de Galois.On a alors (exercice)

$$[L : \mathbf{Q}] = \prod [L_{i+1} : L_i] = 2^m$$

avec $m \leq n$ et donc $[\mathbf{Q}[z] : \mathbf{Q}]$ est une puissance de 2, car $\mathbf{Q}[z] \subset L_n$.

Theorem (Wantzel,1814-1848, Chargé de cours à Polytechnique.)

Le complexe z est constructible si et seulement si il existe une suite finie de corps $L_0 = \mathbf{Q} \subset L_1 \cdots \subset L_n$ et $[L_{i+1} : L_i] \leq 2$ avec $z \in L_n$.

La réciproque fait naturellement intervenir la théorie de Galois.On a alors (exercice)

$$[L : \mathbf{Q}] = \prod [L_{i+1} : L_i] = 2^m$$

avec $m \leq n$ et donc $[\mathbf{Q}[z] : \mathbf{Q}]$ est une puissance de 2, car $\mathbf{Q}[z] \subset L_n$.
Comme $[\mathbf{Q}[\sqrt[3]{2}] : \mathbf{Q}] = 3$, c'est donc que $\sqrt[3]{2}$ n'est pas constructible.

Simplement en observant que z constructible entraîne $[\mathbf{Q}[z] : \mathbf{Q}] < \infty$, c'est-à-dire (exercice) que z est annulé par $P \in Q[z] - 0$ on obtient

l'impossibilté de la quadrature du cercle,

Simplement en observant que z constructible entraîne $[\mathbf{Q}[z] : \mathbf{Q}] < \infty$, c'est-à-dire (exercice) que z est annulé par $P \in Q[z] - 0$ on obtient

l'impossibilté de la quadrature du cercle, (construire un carré de même aire que le disque unité)

Simplement en observant que z constructible entraîne $[\mathbf{Q}[z] : \mathbf{Q}] < \infty$, c'est-à-dire (exercice) que z est annulé par $P \in Q[z] - 0$ on obtient
l'impossibilté de la quadrature du cercle, (construire un carré de même aire que le disque unité) si on sait (Lindemann, 1852-1939) que π est **transcendant** !

Simplement en observant que z constructible entraîne $[\mathbf{Q}[z] : \mathbf{Q}] < \infty$, c'est-à-dire (exercice) que z est annulé par $P \in Q[z] - 0$ on obtient
l'impossibilté de la quadrature du cercle, (construire un carré de même aire que le disque unité) si on sait (Lindemann, 1852-1939) que π est **transcendant** !

On peut en déduire par exemple que l'on ne peut pas construire à la règle et au compas un heptagone régulier.

Simplement en observant que z constructible entraîne $[\mathbf{Q}[z] : \mathbf{Q}] < \infty$, c'est-à-dire (exercice) que z est annulé par $P \in Q[z] - 0$ on obtient
l'impossibilté de la quadrature du cercle, (construire un carré de même aire que le disque unité) si on sait (Lindemann, 1852-1939) que π est **transcendant** !

On peut en déduire par exemple que l'on ne peut pas construire à la règle et au compas un heptagone régulier.
En effet, sinon, la dimension de $\mathbf{Q}[\exp \frac{2i\pi}{7}]$ sur $\mathbf{Q}$ serait une puissance de 2.

Simplement en observant que z constructible entraîne $[\mathbf{Q}[z] : \mathbf{Q}] < \infty$, c'est-à-dire (exercice) que z est annulé par $P \in Q[z] - 0$ on obtient
l'impossibilté de la quadrature du cercle, (construire un carré de même aire que le disque unité) si on sait (Lindemann, 1852-1939) que π est **transcendant** !

On peut en déduire par exemple que l'on ne peut pas construire à la règle et au compas un heptagone régulier.
En effet, sinon, la dimension de $\mathbf{Q}[\exp \frac{2i\pi}{7}]$ sur $\mathbf{Q}$ serait une puissance de 2.
Or, on a

Theorem (Gauss,1777-1855)

Soit $\mathbf{Q}[\exp \frac{2i\pi}{n}]$ *le corps engendré par* $\exp \frac{2i\pi}{n}$ *(qui est aussi l'ensemble des polynômes à coefficients rationnels en* $\exp \frac{2i\pi}{n}$*). On a* $[\mathbf{Q}[\exp \frac{2i\pi}{n}], \mathbf{Q}] = \varphi(n)$ *où* φ *est l'indicateur d'Euler et* $\mathbf{Q}[\exp \frac{2i\pi}{n}]$ *est*

Theorem (Gauss,1777-1855)

Soit $\mathbf{Q}[\exp \frac{2i\pi}{n}]$ *le corps engendré par* $\exp \frac{2i\pi}{n}$ *(qui est aussi l'ensemble des polynômes à coefficients rationnels en* $\exp \frac{2i\pi}{n}$*). On a* $[\mathbf{Q}[\exp \frac{2i\pi}{n}], \mathbf{Q}] = \varphi(n)$ *où* φ *est l'indicateur d'Euler et* $\mathbf{Q}[\exp \frac{2i\pi}{n}]$ *est*

Comme $\varphi(7) = 7 - 1 = 6$...

Theorem (Gauss,1777-1855)

Soit $\mathbf{Q}[\exp \frac{2i\pi}{n}]$ *le corps engendré par* $\exp \frac{2i\pi}{n}$ *(qui est aussi l'ensemble des polynômes à coefficients rationnels en* $\exp \frac{2i\pi}{n}$*). On a* $[\mathbf{Q}[\exp \frac{2i\pi}{n}], \mathbf{Q}] = \varphi(n)$ *où* φ *est l'indicateur d'Euler et* $\mathbf{Q}[\exp \frac{2i\pi}{n}]$ *est*

Comme $\varphi(7) = 7 - 1 = 6$... En particulier, si le polygone régulier à n côtés est constructible, $\varphi(n)$ est une puissance de 2, ce qui impose (exercice) que n est un produit d'une puissance de 2 et d'un nombre de Fermat $F_m = 2^{2^m} + 1$ qui est *premier*.

Theorem (Gauss,1777-1855)

Soit $\mathbf{Q}[\exp \frac{2i\pi}{n}]$ *le corps engendré par* $\exp \frac{2i\pi}{n}$ *(qui est aussi l'ensemble des polynômes à coefficients rationnels en* $\exp \frac{2i\pi}{n}$*). On a* $[\mathbf{Q}[\exp \frac{2i\pi}{n}], \mathbf{Q}] = \varphi(n)$ *où* φ *est l'indicateur d'Euler et* $\mathbf{Q}[\exp \frac{2i\pi}{n}]$ *est*

Comme $\varphi(7) = 7 - 1 = 6$... En particulier, si le polygone régulier à n côtés est constructible, $\varphi(n)$ est une puissance de 2, ce qui impose (exercice) que n est un produit d'une puissance de 2 et d'un nombre de Fermat $F_m = 2^{2^m} + 1$ qui est *premier*.

La réciproque était conjecturée semble-t-il par Gauss (comme toujours, il avait deviné juste) :

La réciproque était conjecturée semble-t-il par Gauss (comme toujours, il avait deviné juste) :

Theorem (Gauss-Wantzel)

La réciproque est vraie : si n est un produit d'une puissance de 2 et d'un nombre de Fermat $F_m = 2^{2^m} + 1$ qui est premier, alors le polygone régulier à n côtés est constructible.

La réciproque était conjecturée semble-t-il par Gauss (comme toujours, il avait deviné juste) :

Theorem (Gauss-Wantzel)

La réciproque est vraie : si n est un produit d'une puissance de 2 et d'un nombre de Fermat $F_m = 2^{2^m} + 1$ qui est premier, alors le polygone régulier à n côtés est constructible.

Notons qu'on a $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$ et sont tous premiers.

La réciproque était conjecturée semble-t-il par Gauss (comme toujours, il avait deviné juste) :

Theorem (Gauss-Wantzel)

La réciproque est vraie : si n est un produit d'une puissance de 2 et d'un nombre de Fermat $F_m = 2^{2^m} + 1$ qui est premier, alors le polygone régulier à n côtés est constructible.

Notons qu'on a $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$ et sont tous premiers.
Si les constructions des triangles équilatéraux, carrés, et pentagones réguliers sont élémentaires, celle du polygone régulier à 17 côté est moins évidente...

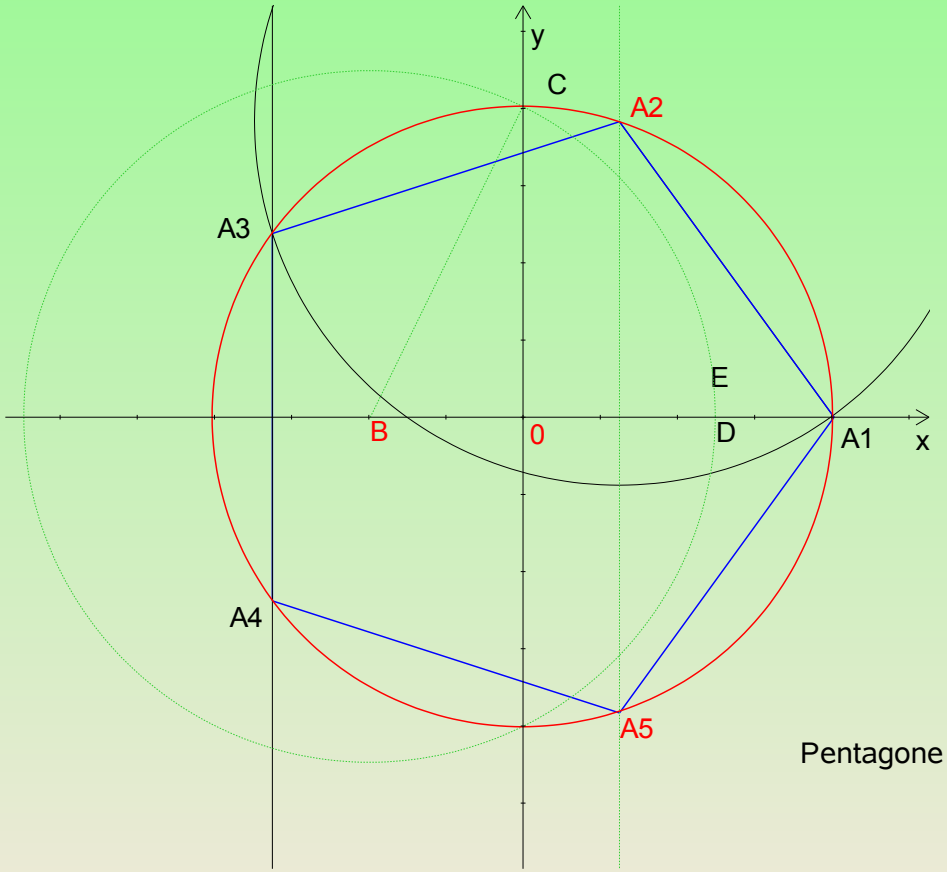
La réciproque était conjecturée semble-t-il par Gauss (comme toujours, il avait deviné juste) :

Theorem (Gauss-Wantzel)

La réciproque est vraie : si n est un produit d'une puissance de 2 et d'un nombre de Fermat $F_m = 2^{2^m} + 1$ qui est premier, alors le polygone régulier à n côtés est constructible.

Notons qu'on a $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$ et sont tous premiers.
Si les constructions des triangles équilatéraux, carrés, et pentagones réguliers sont élémentaires, celle du polygone régulier à 17 côté est moins évidente...
Rappelons la construction (connue de Ptolémée, premier siècle de notre ère) du pentagone régulier, simple conséquence de la formule élémentaire

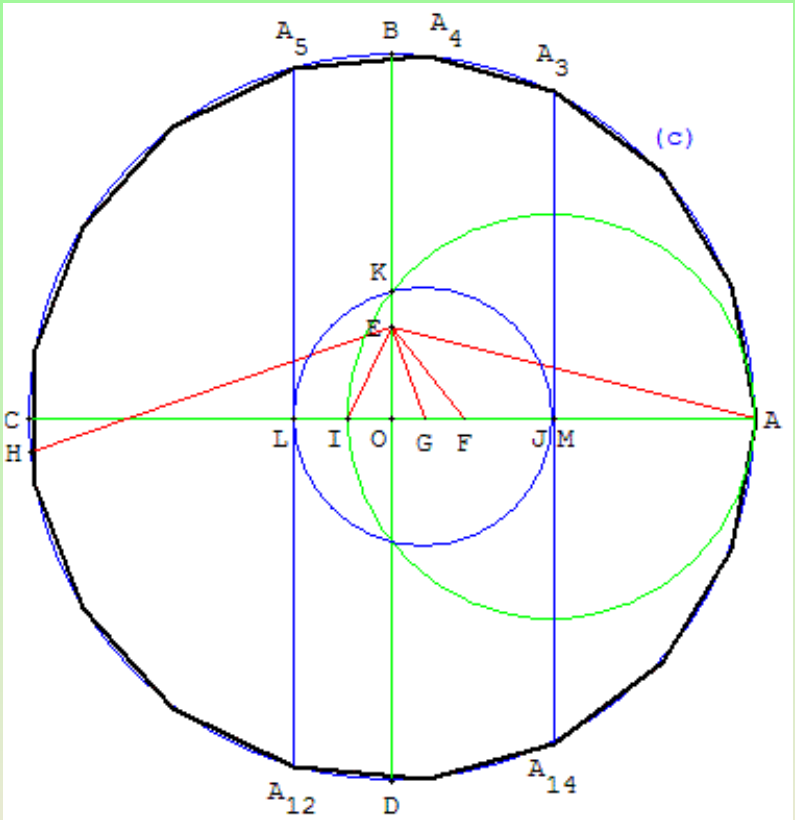
$$\cos(\frac{2\pi}{5}) = \frac{\sqrt{5}-1}{4}.$$



Pentagone

Gauss, encore lui, a donné une construction du polygone à 17 côtés ; voici une construction :

Gauss, encore lui, a donné une construction du polygone à 17 côtés ; voici une construction :



Heptadécagone

On a ici déjà

$$\begin{aligned} 16\cos(\frac{2\pi}{17}) &= -1+\sqrt{17}+\sqrt{34-2\sqrt{17}} \\ &+ \sqrt{68+12\sqrt{17}-4\sqrt{34-2\sqrt{17}}-8\sqrt{34+2\sqrt{17}}} \end{aligned}$$

formule qui se déduit d'ailleurs de la théorie de Galois.

On a ici déjà

$$\begin{aligned} 16\cos(\frac{2\pi}{17}) &= -1+\sqrt{17}+\sqrt{34-2\sqrt{17}} \\ &+ \sqrt{68+12\sqrt{17}-4\sqrt{34-2\sqrt{17}}-8\sqrt{34+2\sqrt{17}}} \end{aligned}$$

formule qui se déduit d'ailleurs de la théorie de Galois.
En revanche, F_6 est divisible par 641 (Euler).

On a ici déjà

$$\begin{aligned} 16\cos(\frac{2\pi}{17}) &= -1+\sqrt{17}+\sqrt{34-2\sqrt{17}} \\ &+ \sqrt{68+12\sqrt{17}-4\sqrt{34-2\sqrt{17}}-8\sqrt{34+2\sqrt{17}}} \end{aligned}$$

formule qui se déduit d'ailleurs de la théorie de Galois.
En revanche, F_6 est divisible par 641 (Euler). On ne sait pas si F_{33} est premier,

On a ici déjà

$$\begin{aligned} 16\cos(\frac{2\pi}{17}) &= -1+\sqrt{17}+\sqrt{34-2\sqrt{17}} \\ &+ \sqrt{68+12\sqrt{17}-4\sqrt{34-2\sqrt{17}}-8\sqrt{34+2\sqrt{17}}} \end{aligned}$$

formule qui se déduit d'ailleurs de la théorie de Galois.
En revanche, F_6 est divisible par 641 (Euler). On ne sait pas si F_{33} est premier,alors qu'on sait que $F_{2478782}$ ne l'est pas :

On a ici déjà

$$\begin{aligned} 16\cos(\frac{2\pi}{17}) &= -1+\sqrt{17}+\sqrt{34-2\sqrt{17}} \\ &+ \sqrt{68+12\sqrt{17}-4\sqrt{34-2\sqrt{17}}-8\sqrt{34+2\sqrt{17}}} \end{aligned}$$

formule qui se déduit d'ailleurs de la théorie de Galois.
En revanche, F_6 est divisible par 641 (Euler). On ne sait pas si F_{33} est premier,alors qu'on sait que $F_{2478782}$ ne l'est pas : peu de choses sont connues sur la primalité des nombres de Fermat.

- Problème : étant donné un polynôme

$$P = X^n + a_{n-1}X^{n-1} + \cdots + a_0, a_i \in \mathbf{C},$$

« calculer » les n racines z_i de P.

- Problème : étant donné un polynôme

$$P = X^n + a_{n-1}X^{n-1} + \cdots + a_0, a_i \in \mathbf{C},$$

« calculer » les n racines z_i de P.

- Précisément, trouver des formules

$$z_i = F_i(a_0, \cdots, a_{n-1})$$

où $F_i's$ sont des fonctions construites à partir de racines m-ièmes et des fractions rationnelles.

- Á vrai dire, si n est grand des fonctions plus compliquées sont nécessaires.

- Á vrai dire, si n est grand des fonctions plus compliquées sont nécessaires.
- Première réduction : le changement de variable

$$X \mapsto X - \frac{a_{n-1}}{n},$$

permet de se ramener à

- Á vrai dire, si n est grand des fonctions plus compliquées sont nécessaires.
- Première réduction : le changement de variable

$$X \mapsto X - \frac{a_{n-1}}{n},$$

permet de se ramener à

$$a_{n-1} = 0.$$

Si $n = 2$, les racines z_i's de

$$X^2 + a_0$$

se calculent en utilisant des polynômes et la fonction :

Si $n = 2$, les racines z_i's de

$$X^2 + a_0$$

se calculent en utilisant des polynômes et la fonction : $x \mapsto \sqrt{x}$:

$$z_i = \pm\sqrt{a_0} \ ;$$

- Si $n = 3$, les z_i's se calculent à l'aide de polynômes et des fonctions $x \mapsto \sqrt[2]{x}$ et $x \mapsto \sqrt[3]{x}$ (Scipione del Ferro, ~ 1502) ;

- Si $n = 3$, les z_i's se calculent à l'aide de polynômes et des fonctions $x \mapsto \sqrt[2]{x}$ et $x \mapsto \sqrt[3]{x}$ (Scipione del Ferro, ~ 1502) ;
- Si $\rho = \exp(2\sqrt{-1}\pi/3)$, on a

$$z_i = \rho^i \sqrt[3]{-\frac{a_0}{2} + \sqrt{\frac{\Delta}{4.27}}} + \rho^{2i} \sqrt[3]{-\frac{a_0}{2} - \sqrt{\frac{\Delta}{4.27}}}.$$

- Si $n = 3$, les z_i's se calculent à l'aide de polynômes et des fonctions $x \mapsto \sqrt[2]{x}$ et $x \mapsto \sqrt[3]{x}$ (Scipione del Ferro, ~ 1502) ;
- Si $\rho = \exp(2\sqrt{-1}\pi/3)$, on a

$$z_i = \rho^i \sqrt[3]{-\frac{a_0}{2} + \sqrt{\frac{\Delta}{4.27}}} + \rho^{2i} \sqrt[3]{-\frac{a_0}{2} - \sqrt{\frac{\Delta}{4.27}}}.$$

- avec$\Delta = 4{a_1}^3 + {a_0}^2$ et la normalisation des racines cubiques de 1

$$\sqrt[3]{-\frac{a_0}{2} + \sqrt{\frac{\Delta}{4.27}}} \cdot \sqrt[3]{-\frac{a_0}{2} - \sqrt{\frac{\Delta}{4.27}}} = -\frac{a_1}{3}.$$

- Si $n = 4$, les z_i's se calculent avec des polynômes et les fonctions

$$x \mapsto \sqrt[2]{x}, \sqrt[3]{x}.$$

- Si $n = 4$, les z_i's se calculent avec des polynômes et les fonctions
$$x \mapsto \sqrt[2]{x}, \sqrt[3]{x}.$$
- L'astuce due to Ferrari (1540) est de se ramener à une équation de degré 3 :

- Si $n = 4$, les z_i's se calculent avec des polynômes et les fonctions
$$x \mapsto \sqrt[2]{x}, \sqrt[3]{x}.$$
- L'astuce due to Ferrari (1540) est de se ramener à une équation de degré 3 :
- On écrit d'abord
$$P(X) = X^4 + 2yX^2 + y^2 + [(a_2 - 2y)X^2 + a_1X + (a_0 - y^2)]$$

- Si $n = 4$, les z_i's se calculent avec des polynômes et les fonctions
$$x \mapsto \sqrt[2]{x}, \sqrt[3]{x}.$$
- L'astuce due to Ferrari (1540) est de se ramener à une équation de degré 3 :
- On écrit d'abord
$$P(X) = X^4 + 2yX^2 + y^2 + [(a_2 - 2y)X^2 + a_1X + (a_0 - y^2)]$$
- Puis, on cherche $y \in \mathbf{C}$ $y \in \mathbf{C}$ tel que
$$-[(a_2 - 2y)X^2 + a_1X + (a_0 - y^2)] = (aX + b)^2.$$

- Cette condition équivaut à l'annulation du discriminant

$$a_2 + 4(a_2 - 2y)(a_0 - y^2)$$

- Cette condition équivaut à l'annulation du discriminant

$$a_2 + 4(a_2 - 2y)(a_0 - y^2)$$

- qui est une équation de degré 3 en y.

- Cette condition équivaut à l'annulation du discriminant

$$a_2 + 4(a_2 - 2y)(a_0 - y^2)$$

- qui est une équation de degré 3 en y.
- Finalement, on écrit

$$P(X) = [(X^2 + y) + (aX + b)][(X^2 + y) - (aX + b)],$$

- Cette condition équivaut à l'annulation du discriminant

$$a_2 + 4(a_2 - 2y)(a_0 - y^2)$$

- qui est une équation de degré 3 en y.
- Finalement, on écrit

$$P(X) = [(X^2 + y) + (aX + b)][(X^2 + y) - (aX + b)],$$

- qui donne le résultat -(grâce aux formules de Cardan)-.

Si $n = 5$ (Abel, 1826) ou $n > 5$ (Galois, 1830) ont prouvé que les fractions rationnelles et que les fonction racines m-ièmes ne sont pas suffisantes en général.