Résoluble ?

François Dubois [1]

Une introduction aux découvertes d'Evariste Galois

"Kafemath"
"La Coulée Douce", 21 rue du Sahel, Paris 12 ième
jeudi 21 février 2013

[1] co-animateur de café mathématique à Paris...

Compter formellement avec racine de deux

Résoudre formellement l'équation $X^2 = 2$
et compter ensuite normalement avec "la" solution $\sqrt{2}$

On introduit une racine (formelle !) de l'équation $X^2 = 2$
On la note ρ. Donc $\rho^2 = 2$ et $\rho \notin \mathbb{Q}$.

Puis on s'intéresse aux nombres de la forme $a + b\,\rho$
pour a et b rationnels (quotients de deux entiers): corps $\mathbb{Q}(\sqrt{2})$

Point important : $\mathbb{Q}(\sqrt{2})$ est bien un corps...
tout élément non nul a un inverse $\dfrac{1}{a + b\,\rho} = \dfrac{a - b\,\rho}{a^2 - 2\,b^2}$

Dans $\mathbb{Q}(\sqrt{2})$, on a toutes les racines de l'équation $X^2 = 2$.
Et on n'a pas eu besoin de dire si $\rho = \sqrt{2}$ ou si $\rho = -\sqrt{2}$!

Compter formellement avec racine de deux (*ii*)

L'indétermination de ρ n'est pas un défaut mais une force !

Automorphisme de $\mathbb{Q}(\sqrt{2})$:

$$\tau \;=\; \big(\mathbb{Q}(\sqrt{2}) \ni a + b\rho \longmapsto a - b\rho \in \mathbb{Q}(\sqrt{2})\big)$$

On remarque que $\tau^2 \equiv \tau_\circ\tau = \mathrm{id}$.

Groupe de Galois $\Gamma(\mathbb{Q}(\sqrt{2}), \mathbb{Q})$

ensemble des automorphismes α de $\mathbb{Q}(\sqrt{2})$

qui laissent invariant le corps des rationnels $\mathbb{Q}$

$$\forall \alpha \in \Gamma(\mathbb{Q}(\sqrt{2}), \mathbb{Q}),\ \forall x, y \in \mathbb{Q}(\sqrt{2}),\ \ \alpha(x+y) = \alpha(x) + \alpha(y)$$
$$\forall \alpha \in \Gamma(\mathbb{Q}(\sqrt{2}), \mathbb{Q}),\ \forall x, y \in \mathbb{Q}(\sqrt{2}),\ \ \alpha(x\,y) = \alpha(x)\,\alpha(y)$$
$$\forall \alpha \in \Gamma(\mathbb{Q}(\sqrt{2}), \mathbb{Q}),\ \forall q \in \mathbb{Q},\ \ \alpha(q) = q.$$

Or $\alpha(\rho^2)$ peut se calculer de deux façons :

$$\alpha(\rho^2) = \alpha(2) = 2, \qquad \alpha(\rho^2) = \alpha(\rho)^2$$

Donc $\alpha(\rho) = \rho$ ou $\alpha(\rho) = -\rho$, c'est à dire $\alpha = \mathrm{id}$ ou $\alpha = \tau$

et $\Gamma(\mathbb{Q}(\sqrt{2}), \mathbb{Q}) = \{\mathrm{id}, \tau\} \simeq \mathcal{S}_2$.

Le drame de la racine cubique de deux

On recommence avec l'équation $X^3 = 2$
Cette fois, le plus simple est de ne considérer
que la racine cubique réelle $\gamma \equiv \sqrt[3]{2} \simeq 1.25992105$

De plus, $\gamma^2 = \sqrt[3]{4}$ appartient au corps $\mathbb{Q}(\sqrt[3]{2})$
qui est formé des nombres de la forme $a + b\,\gamma + c\,\gamma^2$
avec a, b, c rationnels.

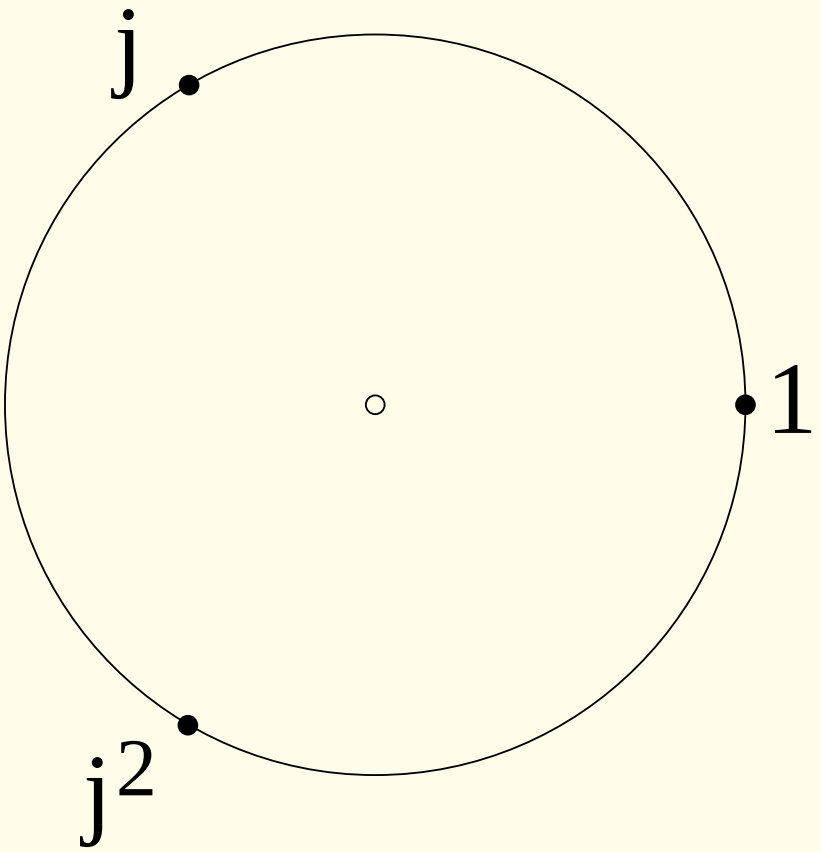
On a même une belle factorisation :

$$X^3 - 2 = (X - \gamma)(X^2 + \gamma X + \gamma^2)$$

Trop belle car le corps $\mathbb{Q}(\sqrt[3]{2})$ inclus dans $\mathbb{R}$
ne contient **pas** les trois racines cubiques de 2...

C'est à dire $\sqrt[3]{2}$, $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$
avec $j = -\frac{1}{2} + \frac{\sqrt{3}}{2}\,i$, $1 + j + j^2 = 0$

Le drame de la racine cubique de deux (*ii*)



Les racines cubiques de l'unité. On a $1 + j + j^2 = 0$.

Le drame de la racine cubique de deux (*iii*)

On peut se rendre compte que

$$\Gamma(\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}) = \{\mathrm{id}\} \text{ est pauvre !}$$

Bonne façon de faire : considérer d'abord le corps $\mathbb{Q}(j)$
des complexes de la forme $a + d\,j$ avec a et d rationnels
et la (une !) racine cubique j définie plus haut

Alors on a quatre corps : $\mathbb{Q}$, $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(j)$ et $\mathbb{Q}(j, \sqrt[3]{2})$.

- le corps $\mathbb{Q}$ des nombres rationnels
- le corps $\mathbb{Q}(\sqrt[3]{2})$ des nombres complexes de la forme $a + b\,\gamma + c\,\gamma^2$
- le corps $\mathbb{Q}(j)$ des nombres complexes de la forme $a + d\,j$
- le corps $\mathbb{Q}(j, \sqrt[3]{2})$ composé des nombres complexes de la forme $a + d\,j + b\,\gamma + e\,j\gamma + c\,\gamma^2 + f\,j\gamma^2$

Le drame de la racine cubique de deux (*iv*)

Groupes de Galois intermédiaires :

$\Gamma(\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}) = \{\mathrm{id}\}$

$\Gamma(\mathbb{Q}(j), \mathbb{Q}) \simeq \mathcal{S}_2$ groupe des permutations de deux racines

$\Gamma(\mathbb{Q}(j, \sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2})) \simeq \mathcal{S}_2$
groupe des permutations de deux racines

$\Gamma(\mathbb{Q}(j, \sqrt[3]{2}), \mathbb{Q}(j)) \simeq \mathcal{A}_3$
groupe des permutations circulaires de trois racines

$\Gamma(\mathbb{Q}(j, \sqrt[3]{2}), \mathbb{Q}) \simeq \mathcal{S}_3$ groupe des arbitraires de trois racines

Joseph-Louis Lagrange (1736-1813)

source : www.galois.ihp.fr

1770 : Mémoire sur la résolution algébrique des équations

Louis Augustin Cauchy (1789-1857)

source : www.uh.edu/engines

1815 : notion de groupe de permutations

Paolo Ruffini (1765-1822)

source : fermatslasttheorem.blogspot.fr

1799 : contribution de 516 pages sur l'impossibilité de résoudre avec des radicaux une équation polynomiale générale

1980 : "Paolo Ruffini's contributions to the quintic"
Raymond Ayoub (1923-2013)

Niels Abel (1802-1829)

source : www.galois.ihp.fr

1826 : l'équation du cinquième degré

ne peut être résolue par radicaux

Evariste Galois (1811-1832)

source : images.math.cnrs.fr

Johann Carl Friedrich Gauss (1777-1855) et Charles Gustave Jacob Jacobi (1804-1851)

sources : rare-earth-magnets.com et eurinsa.insa-lyon.fr

les références de Galois à la fin de sa lettre à Auguste Chevalier

Joseph Liouville (1809-1882)

source : phys.psu.edu

1846 : publie les œuvres scientifiques de Galois

Premier extrait de la lettre de Galois à Chevalier

Paris, le 29 mai 1832
Mon cher Ami,
J'ai fait en analyse plusieurs choses nouvelles. [...]
[...] on voit une grande différence entre adjoindre à une équation une des racines d'une équation auxiliaire, ou les adjoindre toutes.

En langage moderne :

si on a une racine dans l'extension K du corps k,
on a toutes les racines de l'équation
l'extension de corps $K : k$ est galoisienne (normale en anglais)

Relations entre groupes de Galois

Groupes de Galois intermédiaires pour la racine cubique de deux

Quatre corps

$$\begin{array}{ccccc} k \equiv \mathbb{Q} & \subset & M \equiv \mathbb{Q}(\sqrt[3]{2}) & \subset & \mathbb{Q}(j, \sqrt[3]{2}) \equiv L \\ k & \subset & K \equiv \mathbb{Q}(j) & \subset & L \end{array}$$

Cinq groupes de Galois

$$\begin{array}{ccc} \Gamma(L, M) = \mathcal{S}_2 & \subset & \Gamma(L, k) = \mathcal{S}_3 \\ \Gamma(L, K) = \mathcal{A}_3 & \subset & \Gamma(L, k) = \mathcal{S}_3 \\ \Gamma(M, k) = \{\mathrm{id}\}, & & \Gamma(K, k) = \mathcal{S}_2 \end{array}$$

On ne peut **pas** calculer le groupe quotient $\Gamma(L, k) / \Gamma(L, M)$
On peut calculer le "groupe quotient" $\Gamma(L, k) / \Gamma(L, K)$
et on a la relation $\Gamma(L, k) / \Gamma(L, K) \simeq \Gamma(K, k)$

Second extrait de la lettre de Galois à Chevalier

En d'autres termes, quand un groupe G en contient un autre H le groupe G peut se partager en groupes que l'on obtient chacun en opérant sur les permutations de H une même substitution, en sorte $G = H + HS + HS' + \ldots$ et aussi il peut se décomposer en groupes qui ont tous les mêmes substitutions en sorte que $G = H + TH + T'H + \ldots$
Ces deux genres de décomposition ne coïncident pas ordinairement. Quand elles coïncident, la décomposition est dite propre.

En langage moderne :

le sous-groupe H de G est distingué (normal en anglais)
on note $H \triangleleft G$
les classes "à gauche" Hx et "à droite" xH
coïncident pour tout $x \in G$

Groupe quotient

H sous-groupe de G distingué : $H \triangleleft G$
pour tout $x \in G$, $x\,H = H\,x$
$\forall\, x \in G,\ \forall\, h \in H,\ \exists\, \eta \in H$ tel que $\eta\, x = x\, h$
$\forall\, x \in G,\ \forall\, h \in H,\ x\, h\, x^{-1} \in H$

Alors le produit de deux classes $x\,H$ et $y\,H$
peut être défini modulo H :

$$(x\,h)\,(y\,\eta) = x\,y\,(y^{-1}\,h\,y)\,\eta$$

L'ensemble des classes $x\,H$ est noté $G\,/\,H$
Le produit des classes défini plus haut donne à $G\,/\,H$
une struture de groupe : c'est le groupe quotient.

La "correspondance de Galois"

On se donne une extension de corps $L : k$ galoisienne
(en caractéristique zéro...)

Une extension intermédiaire $k \subset K \subset L$
est une extension galoisienne (normal extension) de k
si et seulement si le groupe de Galois $\Gamma(L, K)$ est un
sous groupe distingué (normal sub-group) de $\Gamma(L, k)$.
De plus $\Gamma(L,\, k) \,/\, \Gamma(L,\, K) \simeq \Gamma(K,\, k)$

Avec l'exemple de la racine cubique de deux :
$\Gamma(L,\, M) = \mathcal{S}_2$ non distingué dans $\Gamma(L,\, k) = \mathcal{S}_3$
$\Gamma(L,\, K) = \mathcal{A}_3 \quad \triangleleft \quad \Gamma(L,\, k) = \mathcal{S}_3$
et $\mathcal{S}_3 \,/\, \mathcal{A}_3 = \Gamma(L,\, k) \,/\, \Gamma(L,\, K) \simeq \Gamma(K,\, k) = \mathcal{S}_2$

Où est la résolution des équations par radicaux ?

Introduire un radical : manipuler les racines p ièmes de l'unité
de la forme $\zeta_p = \exp(2\,i\,k\,\pi/p)$
où p est un nombre premier et $1 \leq k \leq p-1$

Ce qui revient à introduire un corps intermédiaire de la forme $\mathbb{Q}(\zeta)$

Or le groupe de Galois $\Gamma(\mathbb{Q}(\zeta), \mathbb{Q}) \simeq \mathcal{C}_p$
est le groupe cyclique d'ordre p.
Et ce groupe est abélien (commutatif) !

Avec la correspondance de Galois, ce groupe est un
groupe quotient $\Gamma(L, \mathbb{Q}) \,/\, \Gamma(L, \mathbb{Q}(\zeta)) \simeq \Gamma(\mathbb{Q}(\zeta), \mathbb{Q}) \simeq \mathcal{C}_p$

Et la résolubilité par radicaux impose des contraintes
sur le "dévissage" du groupe de Galois

Groupe résoluble

Le groupe fini G est résoluble

si il existe une suite de sous groupes distingués

$1 \equiv G_0 \lhd G_1 \lhd \ldots \lhd G_i \lhd G_{i+1} \lhd \ldots \lhd G_m \equiv G$

tels que tous les groupes quotients G_{i+1} / G_i sont abéliens

Théorème (Galois).

Une équation polynomiale $f(x) = 0$ est résoluble par radicaux si et seulement si le groupe de Galois associé est résoluble.

Les groupes $\mathcal{S}_2$, $\mathcal{S}_3$ et $\mathcal{S}_4$ sont résolubles

$1 \lhd \mathcal{S}_2$

$1 \lhd \mathcal{A}_3 \lhd \mathcal{S}_3$

$1 \lhd V_4 \lhd \mathcal{A}_4 \lhd \mathcal{S}_4$

donc les équations polynomiales de degrés 2, 3 et 4 sont résolubles par radicaux !

Groupe simple

A partir du degré $n \geq 5$, on a la suite "courte"

$$1 \triangleleft \mathcal{A}_n \triangleleft \mathcal{S}_n$$

car le groupe $\mathcal{A}_n$ des permutations paires est simple

(il n'a pas de sous groupe distingué non trivial).

Exemple d'équation du cinquième degré non résoluble par radicaux.

Il suffit d'être certain que le groupe de Galois de l'équation

est bien "tout" le groupe $\mathcal{S}_5$

C'est le cas si on a trois racines réelles

et deux complexes conjuguées.

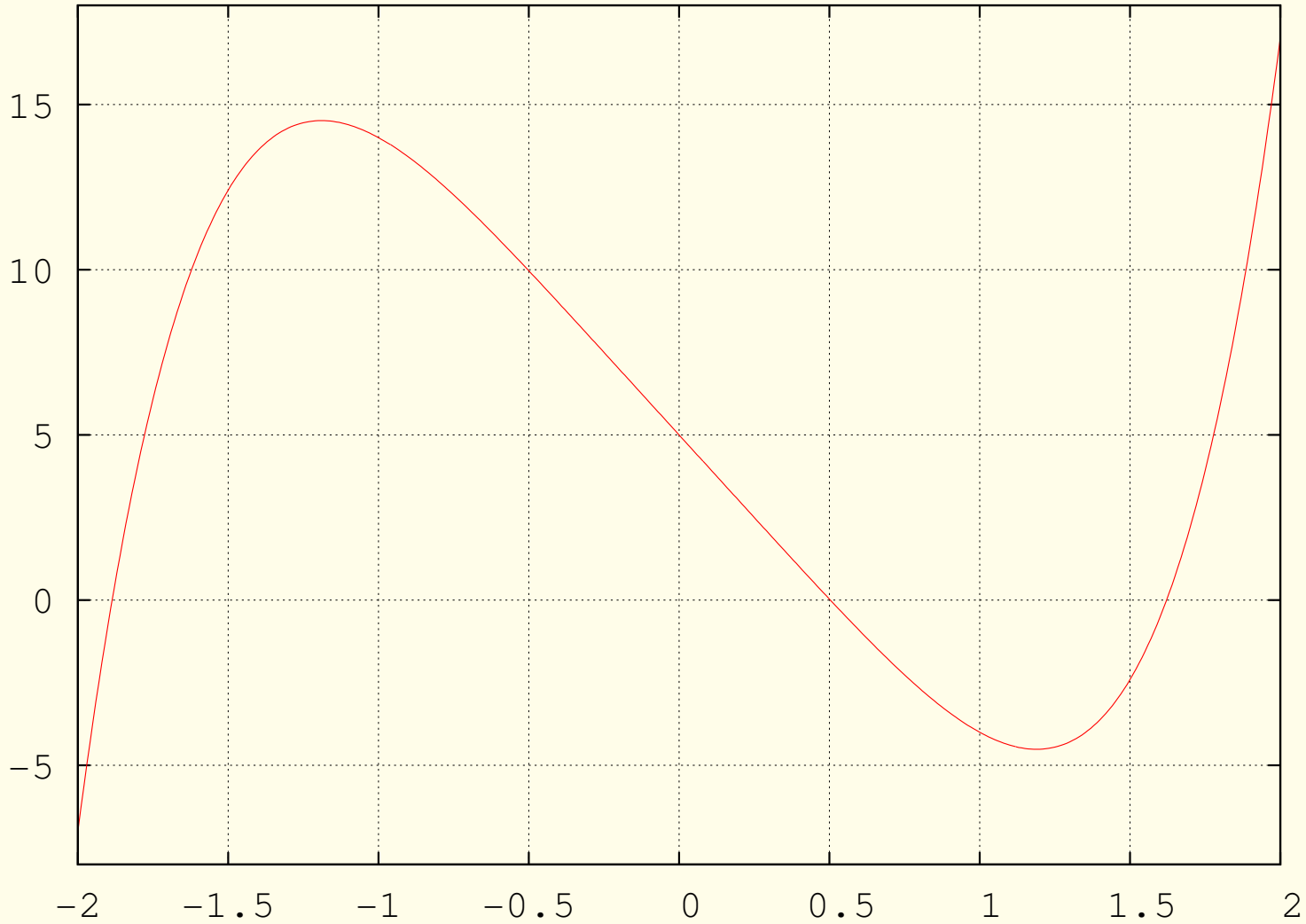
Il faut aussi partir d'un polynome irréductible

sur le corps des rationnels

pas de factorisation du type $(x^2+1)(x^3+x^2+x+1)$...

C'est le cas par exemple avec $f(x) = x^5 - 10x + 5$

Non résoluble !



Représentation dans le champ réel

du polynome $f(x) = x^5 - 10\,x + 5$

Lectures complémentaires

Ian Stewart, *Galois Theory*,
Chapman and Hall, Londres, New York, 1973.

Yves Laszlo, *Introduction à la théorie de Galois*
cours à l'ecole Polytechnique, 2006,
publié aussi chez Ellipses (David Hernandez et Yves Laszlo)

Adrien et Régine Douady, *Algèbre et théories galoisiennes*,
Cassini, 2005.