Théorie de Galois

Grégory Berhuy
Université Grenoble Alpes

5 septembre 2022

Origine historique : Résoudre des équations polynômiales

Si $P = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Q}[X]$, peut-on résoudre $P(x) = 0$ de manière exacte, en écrivant x en fonction des coefficients ?

On peut supposer $a_n = 1$ et $a_{n-1} = 0$ (On remplace P par $P(X - a_n/n)$)

Si $P = X^2 + aX + b$, les racines de P sont :

Si $P = X^2 + aX + b$, les racines de P sont :

$$\frac{-b + \pm\sqrt{b^2 - 4ac}}{2}$$

Si $P = X^3 + pX + q$, les racines de P sont :

Si $P = X^3 + pX + q$, les racines de P sont (Cardan) :

$$j^k \sqrt[3]{\frac{1}{2}\left(-q+\sqrt{\frac{4p^3+27q^2}{27}}\right)} + j^{-k} \sqrt[3]{\frac{1}{2}\left(-q-\sqrt{\frac{4p^3+27q^2}{27}}\right)}$$

avec $j = 0, 1, 2$

Si $P = X^4 + aX^2 + bX + c$, c'est moins connu, mais il y a des formules (méthode de Ferrari)

Si $n \geq 5$, a-t-on des formules similaires ? i.e. les racines de P sont elles exprimables à l'aide des coefficients et de radicaux successifs ?

Si $n \geq 5$, a-t-on des formules similaires ? i.e. les racines de P sont elles exprimables à l'aide des coefficients et de radicaux successifs ?

En général, NON !

Pour le montrer, on utilise la théorie des corps.

Pour le montrer, on utilise la théorie des corps.

On introduit :

* $Dec(P)$: le $+$ petit sous-corps de $\mathbb{C}$ contenant toutes les racines de P.

Pour le montrer, on utilise la théorie des corps.

On introduit :

* $Dec(P)$: le + petit sous-corps de $\mathbb{C}$ contenant toutes les racines de P

* $Gal(P)$: le groupe des automorphismes d'anneaux de $Dec(P)$

On peut démontrer (pas très difficile) qu'un élément de $Gal(P)$ permute les racines de P et est entièrement déterminé par l'image de ces racines.

On peut démontrer (pas très difficile) qu'un élément de $Gal(P)$ permute les racines de P et est entièrement déterminé par l'image de ces racines.

Attention ! toute permutation n'est pas nécessairement possible.

Exemple : $P = X^4 - 2$

Exemple : $P = X^4 - 2$

Les racines sont $\alpha_1 = \sqrt[4]{2}, \alpha_2 = i\sqrt[4]{2}, \alpha_3 = -\sqrt[4]{2}, \alpha_4 = -i\sqrt[4]{2}$.

Exemple : $P = X^4 - 2$

Les racines sont $\alpha_1 = \sqrt[4]{2}, \alpha_2 = i\sqrt[4]{2}, \alpha_3 = -\sqrt[4]{2}, \alpha_4 = -i\sqrt[4]{2}$.

Si $\sigma \in Gal(P)$ vérifie $\sigma(\alpha_1) = \alpha_2$, alors on ne peut avoir $\sigma(\alpha_2) = \alpha_4 = -\alpha_2$

Exemple : $P = X^4 - 2$

Les racines sont $\alpha_1 = \sqrt[4]{2}, \alpha_2 = i\sqrt[4]{2}, \alpha_3 = -\sqrt[4]{2}, \alpha_4 = -i\sqrt[4]{2}$.

Si $\sigma \in Gal(P)$ vérifie $\sigma(\alpha_1) = \alpha_2$, alors on ne peut avoir $\sigma(\alpha_2) = \alpha_4 = -\alpha_2$

Sinon $\sigma(\alpha_1 + \alpha_2) = \sigma(\alpha_1) + \sigma(\alpha_2) = 0$, puis $\alpha_1 + \alpha_2 = 0$, contradiction.

Ainsi, $Gal(P)$ est un sous-groupe de $\mathfrak{S}_n$, parfois strict.

On démontre :

On démontre :

* Les racines de P sont exprimables en fonction des coeffs de P et de radicaux $\iff$ il existe $G_0 = \{\mathrm{Id}\} \triangleleft G_1 \triangleleft \cdots \triangleleft G_{r-1} \triangleleft G_r = Gal(P)$ avec G_i/G_{i-1} abélien pour tout i.

On démontre :

* Les racines de P sont exprimables en fonction des coeffs de P et de radicaux $\iff$ il existe $G_0 = \{\mathrm{Id}\} \triangleleft G_1 \triangleleft \cdots \triangleleft G_{r-1} \triangleleft G_r = Gal(P)$ avec G_i/G_{i-1} abélien pour tout i.

* Il existe des exemples pour lesquels $Gal(P) = \mathfrak{S}_n$

On démontre :

* Les racines de P sont exprimables en fonction des coeffs de P et de radicaux $\Longleftrightarrow$ il existe $G_0 = \{\mathrm{Id}\} \triangleleft G_1 \triangleleft \cdots \triangleleft G_{r-1} \triangleleft G_r = Gal(P)$ avec G_i/G_{i-1} abélien pour tout i.

* Il existe des exemples pour lesquels $Gal(P) = \mathfrak{S}_n$

* Si $n \geq 5$, les sous-groupes distingués de $\mathfrak{S}_n$ sont $\{\mathrm{Id}\}, \mathfrak{A}_n, \mathfrak{S}_n$.

En particulier, la propriété précédente n'est pas vérifiée.

Conclusion : pas de formule générale exprimable à l'aide de radicaux pour les équations polynômiales de degré ≥ 5.

Conclusion : pas de formule générale exprimable à l'aide de radicaux pour les équations polynômiales de degré ≥ 5.

Un des buts de l'UE est de formaliser et démontrer tout ceci.

Autres problèmes : constructions à la règle et au compas

A l'aide uniquement d'une règle et d'un compas :

peut-on trissecter un angle ? dupliquer un cube (i.e. construire $\sqrt[3]{2}$) ? quarrer un cercle (i.e. construire $\sqrt{\pi}$) ?

construire un n-gone régulier (i.e. construire $\cos(2\pi/n)$) ?

De manière générale, peut-on construire une longueur α à la règle et au compas ?

On démontre :

α est constructible $\iff$ il existe $L_0 = \mathbb{Q} \subset L_1 \subset \cdots \subset L_{r-1} \subset L_r$ tels que $\alpha \in L_r$ et $L_i = L_{i-1}(\sqrt{d_i})$ pour tout i

On démontre :

α est constructible $\iff$ il existe $L_0 = \mathbb{Q} \subset L_1 \subset \cdots \subset L_{r-1} \subset L_r$ tels que $\alpha \in L_r$ et $L_i = L_{i-1}(\sqrt{d_i})$ pour tout i

Pas très pratique.

Conséquence intéressante néanmoins : si L est le $+$ petit sous-corps contenant α, alors $\dim_{\mathbb{Q}} L$ est une puissance de 2

Conséquence intéressante néanmoins : si L est le $+$ petit sous-corps contenant α, alors $\dim_{\mathbb{Q}} L$ est une puissance de 2.

Permet de régler le cas de $\sqrt[3]{2}, \sqrt{\pi}$, et très péniblement du n-gone, mais pas celui d'une racine réelle de $X^4 + 2X - 2$.

Soit μ_α l'unique générateur unitaire de l'idéal
$\{P \in \mathbb{Q}[X] \mid P(\alpha) = 0\}$

Soit μ_α l'unique générateur unitaire de l'idéal $\{P \in \mathbb{Q}[X] \mid P(\alpha) = 0\}$

On démontre :

α est constructible $\iff$ $\mathrm{Gal}(\mu_\alpha)$ est un 2-groupe.

Soit μ_α l'unique générateur unitaire de l'idéal $\{P \in \mathbb{Q}[X] \mid P(\alpha) = 0\}$

On démontre :

α est constructible $\iff \mathrm{Gal}(\mu_\alpha)$ est un 2-groupe.

Autre but de l'UE : développer la théorie des nombres constructibles et démontrer le résultat précédent.