Équations (non) résolubles par radicaux

Antoine, Corentin, Valentin

December 7, 2016

1 Définitions

Définition 1.1. [Corps de décomposition] Soient K un corps parfait (fini ou de caractéristique nulle) et $P \in K[X]$ un polynôme non nul. Le corps de décomposition de P est le plus petit corps contenant K et toutes les racines de P.

Note : dans ce qui suit, K est toujours un corps parfait.

Définition 1.2. [Groupe de Galois] Soient $P \in K[X]$ et L son corps de décomposition. On définit le groupe de Galois de P noté $G_K(P)$ comme :

$$G_K(P) = \mathrm{Gal}(L/K) = \{\varphi \in \mathrm{Aut}(L) \mid \forall k \in K, \varphi(k) = k\}$$

Exemple 1.3. Soit $\mathbb{F}_{p^r}$ un corps à p^r éléments. On pose $\mathrm{Frob} : \mathbb{F}_{p^r} \to \mathbb{F}_{p^r},\ x \mapsto x^p$.

- Frob est un morphisme car $(x+y)^p = x^p + y^p$ puisque le corps est de caractéristique p.
- Frob est bijectif car $\mathrm{Frob}^r = \mathrm{id}$

Donc $\mathrm{Frob} \in \mathrm{Aut}(\mathbb{F}_{p^r})$ et $\mathrm{Frob}_{|\mathbb{F}_p} = \mathrm{id}$ donc $\mathrm{Frob} \in \mathrm{Gal}(\mathbb{F}_{p^r}/\mathbb{F}_p)$. On admet l'inclusion réciproque. Ainsi :

$$\langle \mathrm{Frob} \rangle = |\mathrm{Gal}(\mathbb{F}_{p^r}/\mathbb{F}_p)|$$

Exemple 1.4. $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$ où $\mathbb{Q}(\sqrt{2})$ est le plus petit corps contenant 1 et $\sqrt{2}$.
En effet, $\varphi \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ est entièrement déterminé par $\varphi(\sqrt{2})$.
Or $2 = \varphi(2) = \varphi(\sqrt{2}^2) = \varphi(\sqrt{2})^2 \Rightarrow \varphi(\sqrt{2}) = \pm\sqrt{2}$. Ainsi $|\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})| = 2$.
Ce corps est le corps de décomposition du polynôme $X^2 - 2$.

Définition 1.5. [Résolubilité par radicaux] Soit $P \in K[X]$. P est résoluble par radicaux si toutes ses racines s'obtiennent en utilisant que les coefficients de P, les éléments de K, les quatre opérations et l'extraction des racines n-ièmes. Plus précisément, cela signifie que l'on dispose d'une tour d'extension de K représentée comme suit :

$$\begin{aligned} L = & K_n = K(b_1, ..., b_n) \\ & | \\ & \vdots \\ & | \\ & K_1 = K(b_1) \\ & | \\ K = & K_0 \end{aligned}$$

où L est le corps de décomposition de P et $\forall i \in 1, n,\ \exists n_i \in \mathbb{N}^* : b_i^{n_i} \in K_{i-1}$

Exemple 1.6. Si P est de degré 2,

$$\{b_1, b_2\} = \left\{ \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \right\}$$

Si $P = X^3 + pX + q$,

$$\{b_1, b_2, b_3\} = \left\{ e^{2ik\pi/3} \sqrt[3]{\frac{1}{2}\left(-q + \sqrt{\frac{-\Delta}{27}} \right)} + e^{-2ik\pi/3} \sqrt[3]{\frac{1}{2}\left(-q - \sqrt{\frac{-\Delta}{27}} \right)} \mid k \in 0, 2 \right\}$$

avec $\Delta = -4p^3 - 27q^2$.

2 Théorème d'Abel

Historique

Les premières méthodes de résolution d'équations polynomiales de degré 2 datent du VIIIe-IXe siècles (l'indien Sridhar Acharya et l'arabe Al-Khwarizmi). Ce n'est qu'au XVIe siècle que l'italien Tartaglia donne une formule générale pour la résolution des équations du troisième degré (appelée méthode de Cardan). Quelques années plus tard, Ferrari fait de même pour les équations du quatrième degré. Il faudra attendre le début du XIXe siècle pour qu'Abel démontre qu'il n'existe pas de formule pour générale pour la résolution des équations de degré supérieur ou égal à cinq. Peu après, Galois clôt définitivement le problème en explicitant un critère de résolubilité des équations polynomiales de degré quelconque.

Théorème 2.1 (Abel)**.** *Il n'existe pas de formule générale exprimant les solutions des équations du cinquième degré en fonction des coefficients littéraux du polynôme, à l'aide les quatre opérations et de l'extraction des racines n-ièmes.*

Corollaire 2.2. *Il n'existe pas de formule générale exprimant les solutions des équations de degré supérieur ou égal à cinq en fonction des coefficients littéraux du polynôme, à l'aide des quatre opérations et de l'extraction des racines n-ièmes.*

3 Théorème de Galois et applications

Dans ce rapport, nous admettons le théorème et le lemme suivants :

Théorème 3.1 (Galois)**.** *Une équation polynomiale à coefficients dans K est résoluble par radicaux si et seulement si son groupe de Galois est résoluble.*

Lemme 3.2. *Si $x \in L$ vérifie $\forall g \in G(L/K),\ g(x) = x$, alors $x \in K$.*

Remarque 3.3. Ce théorème est plus fort que celui d'Abel puisqu'il caractérise les polynômes résolubles par radicaux. En particulier, comme le plus petit groupe non-résoluble est $\mathfrak{A}_5$, tout groupe de cardinal strictement inférieur à 60 est résoluble, donc si $P \in K[X]$ est de degré $d \leq 4$, comme le groupe de Galois de P s'injecte dans $\mathfrak{S}_d$ (car $G_K(P)$ agit fidèlement sur l'ensemble de ses racines $n_1, ..., n_d$ par $\varphi \mapsto (n_i \mapsto \varphi(n_i))$), φ étant définie par son action sur une base du corps de décomposition de P), son cardinal est ≤ 24, donc il est résoluble et on conclut que P est résoluble par radicaux. De plus, même si les équations polynomiales à coefficients littéraux de degré ≥ 5 ne sont pas résolubles par radicaux, certains polynômes de degré ≥ 5 sont résolubles par radicaux. Par exemple, le groupe de Galois du polynôme $X^n - 1$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$, donc $X^n - 1$ est résoluble par radicaux.

Exemple de polynôme de degré 5 non-résoluble par radicaux

Soit

$$P(X) = X^5 - 5X - 1 \in \mathbb{Q}[X] \tag{1}$$

Montrons que P possède 3 racines réelles distinctes :

$$P'(X) = X^4 - 5 \leq 0 \Leftrightarrow X \in [-1, 1]$$

$$P(-1) = 3,\ P(1) = -5$$

Montrons que P est irréductible sur $\mathbb{Q}[X]$: l'irréductibilité sur $\mathbb{Q}[X]$ étant équivalente à l'irréductibilité sur $\mathbb{Z}[\mathbb{X}]$, on montre que P est irréductible sur $\mathbb{Z}[X]$
Supposons

$$P = (X^4 + aX^3 + bX^2 + cX + d)(X + e), \quad a, b, c, d, e \in \mathbb{Z}$$

Alors $de = -1$, donc $(d, e) \in \{(1, -1), (-1, 1)\}$, donc -1 ou 1 est racine de P ce qui est faux.
Supposons

$$P = (X^2 + aX + b)(X^3 + cX^2 + dX + e), \quad a, b, c, d, e \in \mathbb{Z}$$

On a $a + c = 0$, $eb = -1$, donc $c = -a$, $e = -b = \pm 1$. Aussi, $db - ab = -5$, donc $d - a = -5b$ (car $b^2 = 1$).

$$P = (X^2 + aX + b)(X^3 - aX^2 + (a - 5b)X - b), \quad a, b, c, d, e \in \mathbb{Z}$$

Donc $-b + a(a - 5b) - ab = 0$, i.e. $b = a(a - 6b)$, donc $a|b, i.e, a = \pm 1$. Cela donne $a - 6b \in \{-7, -5, 5, 7\}$, puis $b \in \{-7, -5, 5, 7\}$, ce qui est absurde.

Lemme 3.4. *Si $P \in K[X]$ est irréductible alors si a est une racine de P, $\mathcal{O}_a$ par l'action de $G_K(P)$ est l'ensemble des racines.*

Proof. Si $\mathcal{O}_a = \{a, g_1(a), ..., g_K(a)\}$, on pose $R = \Pi_{i=0}^{K}(X - g_i(a))$. $G_K(P)$ agit sur un polynôme par son action sur chacun des coefficients. Comme les relations coefficients-racines sont symétriques en les racines, on a $\forall g \in G_K(P)$, $g.R = R$. Donc $R \in K[X]$ et $R(a) = 0$ donc $P|R$ (car P polynôme minimal de a) et donc $\mathcal{O}_a$ est l'ensemble des racines. □

Montrons que $G_K(P) = \mathfrak{S}_5$:
Le groupe $G_K(P)$ agit fidèlement sur l'ensemble de ses racines. La conjugaison $f : L \to L, x \mapsto \bar{x} \in G_K(P)$ et laisse invariante les 3 racines réelles : c'est donc une transposition. Soit alors x une racine de P. Notons O_x l'orbite de x sous l'action de $G_K(P)$. On a $|O_x| \mid |G_K(P)|$. Or P est irréductible donc le lemme assure que O_x est l'ensemble des 5 racines. Par conséquent, $5||G_K(P)|$ et d'après le théorème de Cauchy, il existe $\varphi \in G_K(P)$ d'ordre 5 ; dans $\mathfrak{S}_5$, il s'agit d'un 5-cycle. Comme $G_K(P)$ contient une transposition et un 5-cycle,

$$G_K(P) = \mathfrak{S}_5 \qquad \text{qui n'est pas résoluble}$$

P n'est donc pas résoluble par radicaux.