Le corps de décomposition du polynôme $X^3 - 3X + 1$

On déduit de l'égalité trigonométrique :

$$2\cos(3x) = (2\cos x)^3 - 3.(2\cos x)$$

que :

$$-1 = (2\cos(2\pi/9))^3 - 3.(2\cos(2\pi/9)) \ .$$

Donc $x_1 := 2\cos(2\pi/9)$ est une racine de :

$$P(X) = X^3 - 3X + 1 \ .$$

De même, $x_2 := 2\cos(4\pi/9)$, $x_3 := 2\cos(8\pi/9)$ sont racines de $P(X)$.

Comme x_1, x_2, x_3 sont 3 réels distincts, on a :

$$P(X) = X^3 - 3X + 1 = (X - x_1)(X - x_))(X - x_3) \ .$$

Le polynôme $P(X)$ n'a pas de racine sur $\mathbb{Z}$. En effet, sinon une telle racine serait un entier qui divise le coefficient constant : 1. Or ± 1 ne sont pas racines de $P(X)$.

On en déduit que $P(X)$ est irréductible sur $\mathbb{Q}$ (car $\mathbb{Z}$ est factoriel).

Donc $[\mathbb{Q}(x_1) : \mathbb{Q}] = 3$.

Posons : $L := \mathbb{Q}(j)(x_1, x_2, x_3)$ (où $j = -1/2 + i\sqrt{3}/2$).

C'est le corps de décomposition de $X^3 - 3X + 1$ sur $\mathbb{Q}(j)$.

Comme $x_2 = x_1^2 - 2$ et $x_3 = x_2^2 - 2$ (car $2\cos(2x) = (2\cos x)^2 - 2$), on a :

$$L = \mathbb{Q}(j)(x_1) \ .$$

Puisque x_1 est une racine de $P(X)$, $[L : \mathbb{Q}(j)] \leq 3$.

On a : $[L : \mathbb{Q}] = [L : \mathbb{Q}(j)][\mathbb{Q}(j) : \mathbb{Q}] = 2[L : \mathbb{Q}(j)]$. Or, on a aussi : $[L : \mathbb{Q}] = [L : \mathbb{Q}(x_1)][\mathbb{Q}(x_1) : \mathbb{Q}] = 3[L : \mathbb{Q}(x_1)]$.

Donc $3 | [L : \mathbb{Q}(j)]$ et $[L : \mathbb{Q}(j)] = 3$.

Comme on est en caractéristique nulle, comme L est un corps de décomposition, L est une extension galoisienne de $\mathbb{Q}(j)$. L'extension L de $\mathbb{Q}(j)$ est donc galoisienne cyclique de degré 3.

Comme x_1 est de degré 3 sur $\mathbb{Q}(j)$, $1, x_1, x_1^2$ est une base de L comme $\mathbb{Q}(j)-$espace vectoriel.

Puisque $x_2 = x_1^2 - 2$, $1, x_1, x_2$ est aussi une base de L.

Soit $\sigma : L \to \mathbb{C}$ le $\mathbb{Q}(j)-$plongement tel que : $\sigma(x_1) = x_2$. Comme l'extension $L/\mathbb{Q}(j)$ est galoisienne, $\sigma(L) \subseteq L$ et $\sigma \in G := \mathrm{Gal}(L/\mathbb{Q}(j))$. Comme $\mathrm{Gal}(L/\mathbb{Q}(j))$ est cyclique d'ordre 3, comme $\sigma \neq \mathrm{Id}$, σ engendre $\mathrm{Gal}(L/\mathbb{Q}(j))$.

Puisque $\sigma(x_1)$ est une racine de $P(X)$, $\sigma(x_2) = x_1$ ou x_3. Si $\sigma(x_2) = x_1$, σ serait d'ordre 2 ce qui est impossible. Donc $\sigma(x_2) = x_3 = -x_1 - x_2$. La matrice de σ dans la base $1, x_1, x_2$ est donc :

$$A := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & -1 \end{pmatrix} \ .$$

On remarque que j est une valeur propre de A et que le vecteur $\begin{pmatrix} 0 \\ 1 \\ -j \end{pmatrix} =$ $x_1 - jx_2$ est un vecteur propre associé à j.

Posons $x := x_1 - jx_2$. On a :

$$\sigma(x^3) = \sigma(x)^3 = j^3 x^3 = x^3$$

donc x^3 est dans $\mathbb{Q}(j) = L^G = L^{\langle \sigma \rangle}$. De plus, comme $\sigma(x) = jx \neq x$, $x \notin \mathbb{Q}(j)$ et $L = \mathbb{Q}(j)(x)$.

On peut calculer explicitement x^3 :

$$\begin{aligned} x^3 = (x_1 - jx_2)^3 &= x_1^3 - x_2^3 - 3jx_1x_2(x_1 - jx_2) \\ &= 3x_1 - 3x_2 - 3jx_1x_2(x_1 - jx_2) \end{aligned}$$

car $x_i^3 - 3x_i + 1 = 0$. Or $x_2 = x_1^2 - 2$ donc :

$$\begin{aligned} x^3 &= 3x_1 - 3(x_1^2 - 2) - 3jx_1(x_1^2 - 2)(x_1 - j(x_1^2 - 2)) \\ &= 3j^2x_1^5 - 3jx_1^4 - 12j^2x_1^3 + (6j - 3)x_1^2 + (12j^2 + 3)x_1 + 6 \ . \end{aligned}$$

Mais $x_1^4 = 3x_1^2 - x_1$ et $x_1^5 = 3x_1^3 - x_1^2 = -x_1^2 + 9x_1 - 3$. D'où :

$$\begin{aligned} x^3 &= (-3j^2 - 3j - 3)x_1^2 + (3j^2 + 3j + 3)x_1 + (3j^2 + 6) \\ &= 3(1 - j) \end{aligned}$$

car $1 + j + j^2 = 0$.

Donc : $L = \mathbb{Q}(j)(\sqrt[3]{3(1-j)})$.

Remarque : En revanche bien que l'extension $M := \mathbb{Q}(x_1, x_2, x_3) = \mathbb{Q}(x_1)$ soit galoisienne cyclique de degré 3, on ne peut pas trouver de $a \in \mathbb{Q}$ tel que $M = \mathbb{Q}(\sqrt[3]{a})$. En effet, sinon, l'extension M étant galoisienne, on aurait $\sqrt[3]{a}$ et ses conjugués $j\sqrt[3]{a}$, $j^2\sqrt[3]{a}$ dans M. Mais alors : $j = \frac{j\sqrt[3]{a}}{\sqrt[3]{a}}$ serait dans M. Or $M = \mathbb{Q}(x_1, x_2, x_3) \subseteq \mathbb{R}$ *d'où la contradiction.*