GALOIS inverse

[TAUVEL, p 187-188]

ÉNONCÉ :

Théorème : Soit $P \in \mathbb{Q}[X]$ un polynôme irréductible de degré p, p premier, et soit $D \subset \mathbb{C}$ un corps de décomposition de P. On suppose que P possède exactement deux racines non réelles. Alors $Gal(D/\mathbb{Q})$ est isomorphe à $\mathfrak{S}_p$. En particulier, si $p \geq 5$, P n'est pas résoluble par radicaux.

DÉVELOPPEMENT :

LEMME : Soit $p \geq 5$ premier supérieur ou égal à 5. Il existe un polynôme irréductible $P \in \mathbb{Q}[X]$ possédant exactement $p-2$ racines réelles.

Démonstration. Soit $m \in \mathbb{N}^*$ un entier pair et soit

$$P(X) = Q(X) - 2, \quad \text{où } Q(X) = (X^2 + m) \prod_{i=1}^{p-2} (X - 2i)$$

En écrivant $P = \sum_{k=0}^{p} p_k X^k$, on a :

- $p_p = 1$.
- $\forall k \in \{0, \dots, p-1\}$, $2 \mid p_k$.
- $p_0 = m \prod_{i=1}^{p-2}(2i) - 2$, donc $2^2 \nmid p_0$.

En vertu du critère d'EINSENSTEIN, P est irréductible sur $\mathbb{Q}[X]$.

Soit $k \in \mathbb{N}^*$ un entier impair. On a alors :

$$k^2 + m > 2, \quad \left| \prod_{i=1}^{p-2} (k - 2i) \right| \geq 1$$

Par suite, $|Q(k)| > 2$.
Soit $r \in \{0, 1, \dots, p-2\}$, on a $Q(2r+1) \neq 0$. Par ailleurs, le signe de $Q(2r+1)$ est le même que celui de $(-1)^s$, où $s = Card(\{1 \leq i \leq p-2 \mid 2r+1 < 2i\})$. Or $2r+1 < 2i \iff 2r+1 \leq 2i-1 \iff r+1 \leq i$, d'où $s = p - 2 - r$. car s et $r+1$ ont même parité. Ainsi on a $Q(2r+1) < 0$ si r est pair, $Q(2r+1) > 0$ si r est impair.
Ainsi, pour $r \in \{0, 1, \dots, p-2\}$, $P(2r+1) < 0$ si r est pair et $P(2r+1) > 0$ si r est impair. Ainsi,P admet au moins une racine dans l'intervalle $]2r+1, 2r+3[$. Par suite, P possède $p-2$ racines réelles distinctes.
Voyons maintenant que, pour m assez grand, P a une racine α non réelle.
Soient $\alpha_1, \dots, \alpha_p$ (respectivement $\beta_1, \dots, \beta_p$) les racines de P (respectivement de Q) dans $\mathbb{C}$. Il vient :

$$\sum_{j=1}^{p} a_j = \sum_{j=1}^{p} \beta_j = 2 \sum_{j=1}^{p-2} j$$

et :

$$\sum_{1 \leq i < j \leq p} \alpha_i \alpha_j = \sum_{1 \leq i < j \leq p} \beta_i \beta_j = m + 4 \sum_{1 \leq i < j \leq p-2} ij$$

Par suite, on a :

$$\begin{aligned}\sum_{j=1}^{p}\alpha_j^2 &= \left(\sum_{j=1}^{p}\alpha_j\right)^2 - 2\sum_{1\leq i<j\leq p}\alpha_i\alpha_j \\ &= 4\left(\sum_{j=1}^{p-2} j\right)^2 - 2m - 8\sum_{1\leq i<j\leq p-2} ij \\ &= 4\sum_{j=1}^{p-2} j^2 - 2m\end{aligned}$$

En prenant m assez grand, on a donc $\sum_{j=1}^{p}\alpha_j^2 < 0$, ce qui prouve que P possède au moins une racine non réelle α. Comme $P \in \mathbb{Q}[X]$, $\overline{\alpha}$ est également une racine non réelle de P. □

Démonstration. (*théorème*) : Soit x une des deux racines complexes de P. On a $[D : \mathbb{Q}] = [D : \mathbb{Q}(x)][\mathbb{Q}(x) : \mathbb{Q}]$. P étant irréductible, unitaire et annulant x, il s'agit du polynôme minimal de x sur $\mathbb{Q}$ et donc $[\mathbb{Q}(x) : \mathbb{Q}] = \deg(P) = p$. Ainsi, $p \mid [D : \mathbb{Q}] = |Gal(D/\mathbb{Q})|$. En vertu du théorème de CAUCHY, il existe $\sigma \in Gal(D/\mathbb{Q})$ d'ordre p. P admettant deux racines complexes conjuguées, la conjugaison complexe est donc dans $Gal(D/\mathbb{Q})$: c'est une transposition. En faisant agir $Gal(D/\mathbb{Q})$ sur les racines de P, on peut voir $Gal(D/\mathbb{Q})$ comme sous-groupe de $\mathfrak{S}_p$ contenant un $p-$cycle et une transposition. Mais comme $\mathfrak{S}_p$ est engendré par ces deux éléments, on a bien $Gal(D/\mathbb{Q}) \simeq \mathfrak{S}_p$. □

Remarques

- On utilise le théorème de CAUCHY dont on doit avoir une idée de la preuve.
- Il faut être en mesure de justifier que $\mathfrak{S}_p$ est engendré par un p-cycle et une transposition, ceci n'étant valable que lorsque que p est premier !
- En notant $S := \{x_1, \ldots, x_r\}$ les racines de P deux à deux distinctes dans D, on a que S est σ-stable pour tout élément σ de $Gal(D/\mathbb{Q})$ et ainsi on a l'homomorphisme de groupes injectif suivant :

$$\begin{array}{rccc}\Theta : & Gal(D/\mathbb{Q}) & \hookrightarrow & \mathfrak{S}_S \\ & \sigma & \longmapsto & \left\{\begin{array}{rcl} S & \to & S \\ \theta_\sigma : \ x & \mapsto & \sigma(x)\end{array}\right.\end{array}$$

  d'où l'identification de $Gal(D/\mathbb{Q})$ à un sous-groupe de $\mathfrak{S}_S$.
- On admet l'égalité $[D : \mathbb{Q}] = |Gal(D/\mathbb{Q})|$ dû au fait que l'extension est galoisienne (*i.e.* normale et séparable).