Galois Inverse

Théorème
Soit p un nombre premier, alors il existe un polynôme $P \in \mathbb{Q}[X]$ dont le corps de décomposition admet $\mathfrak{S}_p$ comme groupe de Galois.

Référence : Tauvel, *Corps commutatif et théorie de Galois*, pp 187-189.

Démonstration :

On considère un entier m pair positif et $Q(X) = (X^2+m)\prod_{i=1}^{p-2}(X-2i)$. On pose $P(X) = Q(X) - 2$.

On va montrer que P est irréductible sur $\mathbb{Q}[X]$ et a $p-2$ racines réelles distinctes et 2 racines complexes conjuguées. On conclura en montrant qu'un tel polynôme admet $\mathfrak{S}_p$ comme groupe de Galois.

Si on écrit $P = \sum_{k=0}^{p} p_k X^k$ on a :

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

Donc, par le critère d'Eisenstein, P est irréductible sur $\mathbb{Q}[X]$.

Soit k un entier impair positif. On a $|k^2 + m| > 2$ et $\prod_{i=1}^{p-2}|k-2i| \geq 1$, donc $|Q(k)| > 2$ et $|P(k)| > 0$.

On prend maintenant $r \in [\![0, p-2]\!]$, on a vu que $Q(2r+1) \neq 0$ et de plus $\mathrm{sg}(Q(2r+1)) = \mathrm{sg}((-1)^s)$ avec

$$s = \mathrm{Card}(\{i \in [\![1, p-2]\!], 2r+1-2i \leq 0\}) = p-2-r \equiv r+1 \mod (2).$$

Donc :

— Si r est pair, on a $Q(2r+1) < 0$ et $|Q(2r+1)| > 2$. Donc $P(2r+1) < 0$.
— Si r est impair, on a $Q(2r+1) > 0$ et $|Q(2r+1)| > 2$. Donc $p(2r+1) > 0$.

Par le théorème des valeurs intermédiaires, P admet au moins $p-2$ racines réelles distinctes sur $]0, p-2[$.

Si on note $\alpha_1, \cdots, \alpha_p$ les racines de P et $\beta_1, \cdots, \beta_p$ les racines de Q, par les relations coefficients racines on a :

$$\sum_{i=1}^{p}\alpha_i = \sum_{i=1}^{p}\beta_i = -\mathrm{coeff}(X^{p-1}) = 2\sum_{i=1}^{p-2} i$$

$$\sum_{1\leq i<j\leq p}\alpha_i\alpha_j = \sum_{1\leq i<j\leq p}\beta_i\beta_j = \mathrm{coeff}(X^{p-2}) = m + 4\sum_{1\leq i<j\leq p} ij.$$

Donc

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

Pour m assez grand $\sum_{i=1}^{p} \alpha_i^2 < 0$ et donc P admet deux racines complexes conjuguées.

Soit maintenant D le corps de décomposition de P sur $\mathbb{Q}$, on va montrer que $\mathrm{Gal}(D/\mathbb{Q}) \cong \mathfrak{S}_p$.

Soit x une des deux racine complexes de P. On a $[D : \mathbb{Q}] = [D : \mathbb{Q}(x)][\mathbb{Q}(x) : \mathbb{Q}]$. P irréductible et annule x, c'est donc le polynôme minimal de x sur $\mathbb{Q}$ et donc $[\mathbb{Q}(x) : \mathbb{Q}] = \deg(P) = p$. Donc $p \mid [D : \mathbb{Q}] = \mathrm{Card}(\mathrm{Gal}(D/\mathbb{Q}))$ et, par le théorème de Cauchy, il existe σ d'ordre p dans le groupe de Galois de D sur $\mathbb{Q}$. Ensuite, P admet deux racines complexes conjuguées, la conjugaison complexe est donc dans $\mathrm{Gal}(D/\mathbb{Q})$ et est une transposition.

En faisant agir $\mathrm{Gal}(D/\mathbb{Q})$ sur les racines de P, on peut voir $\mathrm{Gal}(D/\mathbb{Q})$ comme un sous-groupe de $\mathfrak{S}_p$ contenant un p-cycle et une transposition. Or $\mathfrak{S}_p$ est engendré par ces deux éléments, on a donc $\mathrm{Gal}(D/\mathbb{Q}) \cong \mathfrak{S}_p$ ■