Galois inverse

Théorème. *Soit p un nombre premier. Il existe un polynôme $P \in \mathbb{Q}[X]$, irréductible sur $\mathbb{Q}$, dont on note K le corps de décomposition, tel que $\mathbf{Aut}(K) \cong \mathfrak{S}_p$. Autrement dit, $\mathfrak{S}_p$ est le groupe de Galois de K sur $\mathbb{Q}$.*

Lemme 1 (admis)**.** *Si P est un polynôme irréductible, le groupe de Galois de son corps de décomposition agit transitivement sur ses racines.*

Démonstration : Soit m un entier naturel pair. On pose

$$Q(X) = (X^2 + m) \prod_{k=1}^{p-2} (X - 2k)$$

et $P(X) = Q(X) - 2$. D'après le critère d'Eisenstein avec l'élément premier 2 de $\mathbb{Z}$, le polynôme P est irréductible sur $\mathbb{Q}$.

Si a est un entier naturel impair, on a $a^2 + m > 2$ et

$$\prod_{k=1}^{p-2} |a^2 - 2m| \geqslant 1,$$

donc $|Q(a)| > 2$. Soit $r \in [\![1, p-2]\!]$, alors $Q(2r+1)$ est non nul et du signe de $(-1)^s$, où

$$s = |\{k \in [\![1, p-2]\!], 2r + 1 \leqslant 2k - 1\}| = p - 2 - r\,;$$

ainsi, s a même parité que $s+1$. Donc si r est impair, $Q(2r+1) > 0$, et en vertu de $|Q(2r+1)| > 2$, on a $P(2r+1) > 0$. De même, si r est pair, on a $P(2r+1) < 0$. Ceci étant valable pour tout $r \in [\![0, p-2]\!]$, le théorème des valeurs intermédiaires implique que P possède au moins $p-2$ racines distinctes.

Notons $\alpha_1, \ldots, \alpha_p$ les racines de P dans $\mathbb{C}$. Comme P et Q ont mêmes coefficients devant X^{p-1} et devant X^{p-2}, les relations coefficients-racines impliquent que

$$\sum_{k=1}^{p} \alpha_i = \sum_{k=1}^{p-2} 2k \text{ et } \sum_{1 \leqslant i < j \leqslant p} \alpha_i \alpha_j = \sum_{1 \leqslant i < j \leqslant p-2} 2i2j + m.$$

Ainsi,

$$\begin{aligned}
\sum_{k=1}^{p} \alpha_k^2 &= \left(\sum_{k=1}^{p} \alpha_k \right)^2 - 2 \sum_{1 \leqslant i < j \leqslant p} \alpha_i \alpha_j \\
&= \left(\sum_{k=1}^{p-2} 2k \right)^2 - 2 \sum_{1 \leqslant i < j \leqslant p-2} 2i2j - 2m \\
&= \sum_{k=1}^{p-2} (2k)^2 - 2m
\end{aligned}$$

Choisissant m suffisamment grand, cette quantité est strictement négative, donc nécessairement, les α_k ne sont pas tous réels. Comme on sait déjà que $p-2$ d'entre eux sont réels, cela entraîne que les deux derniers sont des complexes conjugués, puisque que ce sont les racines de P, qui est à coefficients réels.

Soit K le corps de décomposition de P sur $\mathbb{Q}$. Alors tout automorphisme de K permute les racines de P, et un automorphisme de K qui fixe chaque racine est nécessairement l'identité, car $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$. Ainsi, $\mathbf{Aut}(K)$ est isomorphe à un sous-groupe de $\mathfrak{S}_p$, disons G.

La conjugaison complexe, restreinte à K, en est un automorphisme qui permute les deux racines complexes de P et laisse fixe les autres, donc G contient une transposition, notée τ.

D'après le lemme admis, l'action de $\mathbf{Aut}(K)$ sur l'ensemble des racines de P est transitive, donc p, qui est le cardinal de l'unique orbite de cette action, divise $|G|$. D'après le théorème de Cauchy, il existe dans G un élément d'ordre p, c'est-à-dire un p-cycle, noté c. Pour tout $j \in [\![1, p-1]\!]$, c^j est un élément de G, et c'est encore un p-cycle car p est premier.

Quitte à renuméroter, on peut supposer que $\tau = (1 \quad 2)$. Il existe alors $j \in [\![1, p-1]\!]$ tel que $c^j(1) = 2$, et quitte à renuméroter les éléments $3, \ldots, p$, on peut supposer que $c^j = (1 \quad 2 \quad 3 \quad \ldots \quad p)$. Ces deux éléments engendrant $\mathfrak{S}_p$, on en conclut que $G = \mathfrak{S}_p$, autrement dit que $\mathbf{Aut}(K) \cong \mathfrak{S}_p$.

■