Le théorème d'irréductibilité de Hilbert, entre géométrie et arithmétique

Master Class *Arithmétique et Géométrie Algébrique*

Antoine Chambert Loir

Lorsque K est un corps, la théorie de Galois associe à un polynôme $f \in K[T]$ le sous-groupe $Gal(f)$ du groupe des permutations de ses racines (supposées distinctes) dans une clôture algébrique qui préserve les relations polynomiales entre ces racines.

L'enseignement de la théorie de Galois est souvent présenté dans le contexte *arithmétique* des extensions finies du corps $\mathbf{Q}$ des nombres rationnels. C'est le le plus attirant, peut-être, mais certainement le plus mystérieux, comme en témoigne la difficulté du problème de Galois inverse : quels sont les groupes finis de la forme $Gal(f)$?

La théorie de Galois s'applique bien sûr aussi à des corps tels que $\mathbf{C}(z)$, le corps des fractions rationnelles en une indéterminée, où elle acquiert alors un parfum *géométrique* : ce corps étant celui des fonctions méromorphes sur la « sphère de Riemann » (droite projective complexe), la théorie de Galois apparaît alors comme une version algébrique de la théorie des revêtements des espaces topologiques.

Le théorème d'irréductibilité de Hilbert se place à l'interface de ces deux contextes. Étant donné un polynôme $f \in \mathbf{Q}[z, T]$, il compare le groupe de Galois de f — considéré comme élément de $\mathbf{C}(z)[T]$ — et le groupe de Galois des polynômes $f(a, T)$, pour $a \in \mathbf{Q}$: pour la « plupart » des a, ces deux groupes sont les mêmes !

La démonstration que nous exposerons est due à Dörge (1927) et est un prototype des méthodes utilisées aujourd'hui en théorie des nombres transcendants.