Arithmétique statistique des groupes de Galois

Résumé : Le domaine de l'arithmétique statistique concerne le comportement asymptotique, probabiliste, et statistique des objets en théorie de nombre en familles. Des exemples de familles sont des familles de variétés, de polynômes (irreducibles avec groupe de Galois donné) ou de sommes de caractères. Un exemple classique est le groupe généralisé de Sato–Tate : soit A une variété abélienne, $T_\ell(A)$ son module de Tate — ou groupe de cohomologie étale $H^1_{et}(A, \mathbb{Z}_\ell)$ — et posons $V_\ell(A) = T_\ell(A) \otimes \mathbb{Q}$. Alors le groupe de Sato–Tate est un groupe compacte de Lie minimal qui contient l'image de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$:

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}(V_\ell(A)) \subset \mathrm{GL}(V_\ell(A) \otimes \mathbb{C}),$$

déterminée par un plongement de $\mathbb{Q}_\ell \to \mathbb{C}$.

L'objet derrière ces statistiques est le groupe de Galois absolu $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, qui est un groupe profini — déterminé comme limite de ses quotients finis. Ici, on s'intéresse précisement aux représentations de ces quotients finis. Precisement, on part du problème suivant : Soit donnée un polynôme irreductible $f(x)$ de degré n dans $\mathbb{Z}[x]$. On associe, pour presque tout premier p, une partition $(d_1, \ldots, d_t)$, où $d_1 + \cdots + d_t = n$, de les degrés d_i des polynômes dans la factorization de $f(x)$ mod p dans $\mathbb{F}_p[x]$.

On interprète les propriétés de cette fonction $p \mapsto (d_1, \ldots, d_t)$ comme étude des représentations du groupe $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. En partant des représentations orthogonales, et passant par sa restriction aux groupes finis, on détermine des parametrisations des anneaux de caractères associés à ces représentations. On exprime les relations d'orthogonalité provenant du mésure de Haar, en termes de l'arithmétique statistique. Finalement, on en déduit des algorithmes pour caracteriser le groupe de Galois et on détermine l'équivalence des représentations finies du groupe $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Cette étude est motivée par du travail commun avec Gilles Lachaud et Yih-Dar Shieh sur les groupes orthogonaux, et une question de Fernando Villegas–Rodriguez sur l'application au cas des groupes finis.