Petite excursion dans le programme de Langlands

Anne-Marie Aubert

Institut de Mathématiques de Jussieu – Paris Rive Gauche
C.N.R.S., Sorbonne Université and Université Paris Cité

Mathématiques en Mouvement 2025: Théorie des nombres
15 Novembre 2025 à l'IHP

Robert Langlands, naissance en 1936 à New Westminster, Canada
Professeur émérite à l'Institute for Advanced Study, Princeton, États-Unis
Prix Abel 2018, Prix Wolf 1995

Un programme visionnaire qui s'élargit au fil du temps

Né d'une lettre (de 17 pages) envoyée en 1967 par Robert Langlands à André Weil, éminent professeur à l'Institute for Advanced Study, le programme de Langlands vise à établir un vaste réseau de conjectures reliant des domaines éloignés des mathématiques, principalement la théorie des nombres, l'analyse harmonique, la théorie des représentations et la géométrie algébrique.

Buste d'André Weil sculpté par Charlotte Langlands

Une idée surprenante

Des objets profonds de la théorie des nombres, liés aux groupes de Galois, lesquels encodent les symétries des systèmes de nombres, pourraient correspondre à des formes automorphes, des fonctions élégantes étudiées en analyse harmonique qui restent essentiellement inchangées lorsqu'on leur applique de vastes groupes de transformations.

Correspondance(s) et Fonctorialité

- Le programme postule une correspondance structurelle profonde entre les objets de deux mondes différents: le monde "analytique" (automorphe) et le monde "arithmétique" (galoisien).
- Il s'incarne en réalité dans plusieurs correspondances en jouant notamment sur les différents types de corps possibles.
- Au coeur du programme: ledit principe de fonctorialité.

Corps locaux (Notation F)

- archimédiens: $\mathbb{R}$ et $\mathbb{C}$.
- non archimédiens:
  - $\mathbb{Q}_p$ (le corps des nombres p-adiques) et ses extensions finies
  - $\mathbb{F}_p((t))$ (corps des séries de Laurent sur $\mathbb{F}_p$) et ses extensions finies

  avec p un nombre premier.

Valuation p-adique

La valuation p-adique d'un entier non nul n est l'exposant de la puissance la plus élevée du nombre premier p qui divise n: cet exposant est noté $v_p(n)$. De manière équivalente, c'est l'exposant auquel p apparaît dans la décomposition en facteurs premiers de n. On prolonge cette notation aux rationnels non nuls en posant $v_p(m/n) := v_p(m) - v_p(n)$.

Valeur absolue p-adique

C'est la fonction sur $\mathbb{Q}$ définie par

$$|x|_p := \begin{cases} 0 & \text{si } x = 0 \\ p^{-v_p(x)} & \text{si } x \neq 0. \end{cases}$$

Elle satisfait à l'inégalité ultramétrique:

$$|r + s|_p \leq \max\left(|r|_p, |s|_p\right).$$

Le corps $\mathbb{Q}_p$

La valeur absolue p-adique munit $\mathbb{Q}$ d'une structure d'espace métrique par la distance $d\colon \mathbb{Q} \times \mathbb{Q} \to \mathbb{R}$ définie par

$$d(r, s) := |r - s|_p.$$

La complétion de $\mathbb{Q}$ pour cette distance conduit au corps $\mathbb{Q}_p$ des nombres p-adiques.

Entiers p-adiques

Un entier p-adique est une série formelle infinie

$$a_0 + a_1 p + a_2 p^2 + \cdots$$

où $0 \leq a_i < p$ pour tout $i \in \mathbb{N}$. L'ensemble des entiers p-adiques est noté $\mathbb{Z}_p$.

Corps globaux (Notation K)

- corps de nombres: extensions finies de $\mathbb{Q}$
- corps de fonctions: extensions finies de $\mathbb{F}_p(t)$.

Clôture algébrique séparable d'un corps

Une extension séparable d'un corps commutatif E est une extension algébrique L de E t.q. le polynôme minimal de tout élément de L n'a que des racines simples (dans une clôture algébrique). Une clôture algébrique séparable $\overline{E}$ de E est une extension séparable et maximale pour cette propriété. E est dit algébriquement clos si $\overline{E} = E$.

Définition

Une représentation (à coefficients dans un corps C algébriquement clos) d'un groupe H est un morphisme de groupes de H dans $\mathrm{GL}(V)$, où V est un C-espace vectoriel.

Exemples

- C: $\mathbb{C}$, $\overline{\mathbb{Q}}_\ell$, ou $\overline{\mathbb{F}}_\ell$, avec ℓ un nombre premier.
- H: $\underbrace{\mathrm{GL}_n(F), \mathrm{SL}_n(F), \mathrm{GL}_n(\mathbb{A}_K)}_{\text{représentations “automorphes”}}$, $\underbrace{\mathrm{Gal}(\overline{F}/F), \mathrm{Gal}(\overline{K}/K)}_{\text{représentations galoisiennes}}$.

Définition

Une représentation galoisienne est un morphisme continu

$$\rho\colon \mathrm{Gal}(\overline{E}/E) \longrightarrow \mathrm{GL}_n(C).$$

Ici $V = C^n$ est de dimension finie. Dans la suite, nous supposerons $C = \mathbb{C}$.

Remarque

A contrario, les représentations des groupe de Lie $\mathrm{GL}_n(F)$ ou $\mathrm{SL}_n(F)$ sont en général de dimension infinie.

Deux nouveaux acteurs

F corps local non archimédien.

1. Le groupe de Weil W_F: un sous-groupe dense de $\mathrm{Gal}(\overline{F}/F)$, doté d'une topologie différente et plus fine.
2. Le L-groupe ${}^LG = G^\vee \rtimes W_F$: produit semi-direct d'un groupe dual complexe $G^\vee$ (déterminé par la structure algébrique de G)) et de W_F. Exemples: $(\mathrm{GL}_n(F))^\vee = \mathrm{GL}_n(\mathbb{C})$, $(\mathrm{SL}_n(F))^\vee = \mathrm{PGL}_n(\mathbb{C})$, $(\mathrm{Sp}_{2n}(F))^\vee = \mathrm{SO}_{2n+1}(\mathbb{C})$.

Correspondance de Langlands locale

Application surjective (conjecturale en général), satisfaisant plusieurs properties,

$$\left\{\begin{array}{c}\text{repres. irréd. de } G\\ \pi\colon G\to \mathrm{GL}(V)\end{array}\right\}/\text{iso.} \xrightarrow{\mathcal{L}} \left\{\begin{array}{c}L\text{-paramètres}\\ \text{i.e., morphisms continus}\\ \varphi_\pi\colon W_F\times \mathrm{SL}_2(\mathbb{C})\to {}^L G\end{array}\right\}/G^\vee\text{-conj.}$$

à fibres finies, appelées L-paquets.

La correspondance de Langlands locale pour GL_n

C'est l'unique bijection

$$\left\{\begin{array}{c}\text{repres. irréd. de } G\\ \pi\colon G\to \mathrm{GL}(V)\end{array}\right\}/\text{iso.} \xrightarrow{\mathcal{L}} \left\{\begin{array}{c}\text{représentations}\\ \varphi_\pi\colon W_F\times \mathrm{SL}_2(\mathbb{C})\to \mathrm{GL}_n(\mathbb{C})\end{array}\right\}/\text{iso.}$$

satisfaisant une liste prétablie de propriétés, dont la préservation des fonctions L.

Remarques

- Preuves indépendantes de Harris-Taylor, Henniart, et Scholze.
- Les L-paquets sont des singletons.
- Les représentations irréductibles supercuspidales de $\mathrm{GL}_n(F)$ correspondent aux représentations irréductibles de W_F.
- Une version pour les corps finis:
  [A., "On the Macdonald correspondence", Macdonald memorial volume at the Quarterly Journal of Mathematics, 2025].

Structure

Le programme se décompose en conjectures "locales" (examinant les propriétés autour d'un nombre premier p donné) et "globales" (concernant l'ensemble des nombres rationnels ou d'autres corps globaux).

Un dictionnaire entre deux univers

Le programme de Langlands global propose lui aussi un dictionnaire profond entre deux univers:

Côté automorphe:
Groupes de Lie
Représentations automorphes
Symétries des fonctions sur les groupes de Lie
Analyse harmonique sur les adèles
Fonctions L

Côté arithmétique:
Groupes de Galois
Représentations galoisiennes
Symétries des nombres algébriques
Courbes elliptiques, Géométrie algébrique
Fonctions L

Fonctions L de Dirichlet: On associe à un caractère de Dirichlet $\chi\colon (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$ la fonction L définie par

$$L(s,\chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \quad \text{pour } s \in \mathbb{C} \text{ t.q. } \Re(s) > 1.$$

Adèles

L'idée est d'étudier les questions de théorie des nombres concernant un corps de nombres en étudiant d'abord les congruences.

- Par exemple, pour étudier la factorisation d'un polynôme unitaire à coefficients entiers, on étudie d'abord la factorisation modulo chaque nombre premier. De plus, nous considérons les limitations imposées par le traitement du polynôme comme ayant des coefficients réels.
- Ainsi, dans le cas de $\mathbb{Q}$, on utilise une structure qui incorpore les congruences modulo chaque nombre premier (ainsi que les puissances du nombre premier), ainsi que des informations sur $\mathbb{R}$.
- L'anneau d'adèles $\mathbb{A}_\mathbb{Q}$ est la structure en question: $\mathbb{A}_\mathbb{Q} = \mathbb{R} \times \mathbb{A}_\mathbb{Q}^\infty := \mathbb{R} \times \prod'_p \mathbb{Q}_p =$, où tous les facteurs du produit, sauf un nombre fini, sont dans $\mathbb{Z}_p$:

$$\mathbb{A}_\mathbb{Q} := \left\{ (x_\infty, x_2, x_3, \ldots) : \begin{cases} x_v \in \mathbb{Q}_v & \text{pour tout } v \leq \infty \\ x_p \in \mathbb{Z}_p & \text{pour presque tout } p \end{cases} \right\}.$$

Définition

Soit $\mathrm{GL}_n(\mathbb{A}_\mathbb{Q})$ le groupe des matrices $n \times n$ inversibles sur $\mathbb{A}_\mathbb{Q}$.

Remarque: Le groupe $\mathrm{GL}_2(\mathbb{Q})$ se plonge diagonalement dans $\mathrm{GL}_2(\mathbb{A}_\mathbb{Q})$.

Plus généralement, si $\mathbf{G}$ est un groupe algébrique réductif (par exemple, $\mathbf{G} = \mathrm{SL}_n$), on notera $\mathbf{G}(\mathbb{A}_\mathbb{Q})$ le groupe adélique associé.

Définition

Une forme automorphe est une fonction sur $\mathbf{G}(\mathbb{A}_\mathbb{Q})$ à valeurs complexes satisfaisant certaines conditions d'invariance, de régularité et de croissance. Notons $\mathcal{A}(\mathbf{G})$ l'espace des formes automorphes sur $\mathbf{G}(\mathbb{A}_\mathbb{Q})$.
Une représentation automorphe est une représentation de $\mathbf{G}(\mathbb{A}_\mathbb{Q})$ qui est un sous-quotient de $\mathcal{A}(\mathbf{G})$.

Remarque

Nous allons voir que l'on peut associer une forme automorphe sur $\mathrm{GL}_2(\mathbb{A}_\mathbb{Q})$ à toute forme modulaire. Mais toutes les formes automorphes sur $\mathrm{GL}_2(\mathbb{A}_\mathbb{Q})$ ne sont pas obtenues à partir de formes modulaires.

Notations

Soient N un entier positif et $\widehat{\mathbb{Z}} := \prod_p \mathbb{Z}_p$. Posons

$$\widetilde{K}_0(N) := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\widehat{\mathbb{Z}}) \ : \ N \text{ divise } c \right\}$$

$$\widetilde{K}_1(N) := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\widehat{\mathbb{Z}}) \ : \ N \text{ divise } c \text{ et } d-1 \right\} \triangleleft \widetilde{K}_0(N)$$

et $K_i(N) := \widetilde{K}_i(N) \cap \mathrm{GL}_2(\mathbb{R})^+$ pour $i = 0, 1$, où

$$\mathrm{GL}_2(\mathbb{R})^+ := \{ g \in \mathrm{GL}_2(\mathbb{R}) \ : \ \det(g) > 0 \}.$$

L'application $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto d$ définit un isomorphisme

$$\kappa \colon \widetilde{K}_0(N)/\widetilde{K}_1(N) \longrightarrow \prod_{p|N} \mathbb{Z}_p^\times/(1+p\mathbb{Z}_p) = (\mathbb{Z}/N\mathbb{Z})^\times.$$

Remarque

On a

$$\widetilde{\Gamma}_0(N) := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}) \ : \ N \text{ divise } c \right\} = \widetilde{K}_0(N) \cap \mathrm{GL}_2(\mathbb{Z}).$$

Notons I_2 l'identité de $\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}}^{\infty})$.
L'application $\widetilde{\Gamma}_0(N)g \mapsto \mathrm{GL}_2(\mathbb{Q})(g, \mathrm{I}_2)K_0(N)$ définit un homeomorphism

$$\widetilde{\Gamma}_0(N)\backslash \mathrm{GL}_2(\mathbb{R})^+ \to \mathrm{GL}_2(\mathbb{Q})\backslash \mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}})/K_0(N).$$

Le demi-plan de Poincaré

$$\mathfrak{H} := \{z = x + iy \ : \ y > 0\} \subset \mathbb{C}.$$

Forme automorphe associée à une forme modulaire

Soit $f\colon \mathfrak{H} \to \mathbb{C}$ une forme modulaire f de poids k, de niveau N et de nebentypus χ (un caractère $(\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$)

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k \chi(d)\, f(z) \quad \text{pour tout } \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)^+.$$

On associe à f la fonction $\phi_f\colon \mathrm{GL}_2(\mathbb{R})^+ \times \widetilde{K}_0(N)$ définie par

$$\phi_f(g,h) := j(g,i)^{-k} f(gi)\, \chi^{-1}(\kappa(h)) \quad \text{pour } g \in \mathrm{GL}_2(\mathbb{R})^+ \text{ et } h \in \widetilde{K}_0(N).$$

La fonction ϕ_f satisfait

$$\phi_f(\gamma g, \gamma h) = \phi_f(g,h), \quad \text{pour tout } \gamma \in \widetilde{\Gamma}_0(N).$$

Elle s'étend de manière unique sur $\mathrm{GL}_2(\mathbb{Q})\backslash\mathrm{GL}_2(\mathbb{A}_\mathbb{Q})/K_0(N)$, et définit une forme automorphe sur $\mathrm{GL}_2(\mathbb{A}_\mathbb{Q})$.

La courbe modulaire

Pour un entier $N \geq 1$, la courbe modulaire $X_1(N)$ est une variété algébrique définie sur $\mathbb{Q}$.

- Elle compactifie l'espace modulaire $\Gamma_1(N)\backslash\mathfrak{H}$ en ajoutant les pointes (cusps).
- Elle possède une action naturelle de l'algèbre de Hecke (opérateurs T_p) et du groupe de Galois $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sur sa cohomologie.

Représentation galoisienne associée à une forme modulaire [Deligne, 1969–1971]

On réalise f à l'intérieur de la cohomologie de la courbe modulaire $X_1(N)$. Pour tout nombre premier ℓ, il existe une représentation ℓ-adique

$$\rho_{f,\ell} \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$$

qui encode les données arithmétiques de f: valeurs de Hecke, caractères, poids.

Correspondance de Langlands globale

Une représentation automorphe cuspidale π de $\mathrm{GL}_n(\mathbb{A}_\mathbb{Q})$ correspond conjecturalement à un "système compatible" de représentations ℓ-adiques $\rho_{\pi,\ell}\colon \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$, $\ell \neq p$; telles que leurs fonctions L coïncident.

Le principe de fonctorialité

S'il existe un homomorphisme ${}^L H \to {}^L G$ entre les L-groupes, alors il devrait y exister un transfert correspondant des représentations automorphes de H vers celles de G.

Exemple

Changement de base: si E/F est une extension finie, il existe un homomorphisme ${}^L\mathrm{GL}_n/F \to {}^L\mathrm{GL}_n/E$. La fonctoralité prédit que les représentations automorphes de $\mathrm{GL}_n(\mathbb{A}_F)$ se relèvent en des représentations automorphes de $\mathrm{GL}_n(\mathbb{A}_E)$.

Remarques

- La fonctorialité est un principe directeur fondamental plutôt qu'un théorème unique. Sa démonstration requiert des outils extrêmement sophistiqués (formule des traces de Selberg, méthodes des paquets d'Arthur, théorie des variétés de Shimura).
- Ce principe a des conséquences majeures. Par exemple, il a été un point de départ clé dans les travaux qui ont mené à la démonstration du dernier théorème de Fermat.

Un cadre unifié

Le programme de Langlands propose un cadre unifié qui englobe toutes ces fonctions L (celles de Riemann, de Dirichlet, de Hecke, les formes modulaires, d'Artin, etc.) comme provenant d'une source unique: les représentations automorphes.
La fonctorialité (le cœur du programme) nous dit comment ces fonctions L se transforment lorsque nous nous déplaçons entre différents groupes ou représentations.

Conclusion

- Les coefficients des formes modulaires (et plus généralement des représentations automorphes) contiennent des données qui reflètent la distribution des nombres premiers.
- Le programme de Langlands ne compte pas directement les nombres premiers.
- Il explique plutôt l'existence d'objets analytiques qui contrôlent la distribution des nombres premiers (les fonctions L), leurs relations et comment leurs symétries peuvent être comprises en termes de théorie des représentations.
- La distribution des nombres premiers est la surface visible d'une symétrie conjecturale beaucoup plus profonde capturée par la fonctorialité de Langlands.

Merci pour votre attention!