La théorie de Galois et l'arithmétique

A 20 ans, dans la nuit précédant le duel où il devait trouver la mort, Évariste Galois (1811-1832) écrivit un testament de ses réflexions des années passées. C'était une théorie des équations algébriques que l'on a appelée la théorie de Galois. Aujourd'hui plus que jamais elle est au cœur de l'arithmétique où elle fait se rencontrer l'algèbre, la géométrie, la topologie et l'analyse harmonique.

Une équation algébrique (à une inconnue X) s'écrit $a_d X^d + a_{d-1} X^{d-1} + \cdots + a_1 X + a_0 = 0$. Quand le degré d est 1, elle admet la solution $-a_0/a_1$ dès que les coefficients a_0, a_1 sont éléments d'un ensemble F où existent les quatre opérations $+$, $-$, $\times$ et $/$; un tel F est appelé un corps. Quand $d = 2$, les solutions sont $(-a_1 \pm \sqrt{a_1^2 - 4\,a_0\,a_2})/2\,a_2$. De même, pour $d = 3$ ou 4, les solutions s'expriment en termes des quatre opérations et du passage aux racines $\sqrt{a}$, $\sqrt[3]{a}$, $\sqrt[4]{a}$ des équations $X^2 = a$, $X^3 = a$, $X^4 = a$. Abel a montré que c'est impossible à partir de $d = 5$. La théorie de Galois répond à la question la plus générale de savoir déterminer toutes les relations entre équations algébriques à coefficients dans un corps F. On associe à chacune l'ensemble fini de ses solutions muni de l'action d'un groupe[1] G_F, le groupe de Galois de F. Alors les relations entre équations correspondent aux applications entre ensembles finis associés qui respectent l'action de G_F.

Entre 1958 et 1970, une vision nouvelle et deux généralisations considérables furent apportées à la théorie de Galois par le mathématicien français Alexander Grothendieck, dans le cadre de sa refonte de la géométrie algébrique en « théorie des schémas ». Il définit d'abord les revêtements d'un schéma S : ce sont les schémas S' fibrés sur S et qui localement (au sens de sa « topologie étale ») s'écrivent comme des empilements de copies de S (tels les étages d'un immeuble au-dessus du sol). Puis il montre que la catégorie[2] des revêtements de S équivaut à celle des ensembles finis munis de l'action d'un groupe π_S, le « groupe fondamental de S ». A tout corps F est associé un schéma de dimension 0, son « spectre » $S = \mathrm{Spec}\,F$, et les équations algébriques à une inconnue à coefficients dans F correspondent aux revêtements de S ; le groupe fondamental π_S n'est autre que le groupe de Galois G_F. On a donc une généralisation géométrique commune de la théorie de Galois et de celle du groupe fondamental topologique de Henri Poincaré (1854-1912).

Mais de même qu'il y a des schémas de toutes dimensions, il y a au-dessus d'un schéma S des fibrations de toutes dimensions relatives et non pas seulement de dimension relative 0 comme les revêtements ; quand $S = \mathrm{Spec}\,F$, ce sont les « variétés » définies par des équations algébriques à plusieurs inconnues. Dans cette direction verticale aussi, Grothendieck a donné une généralisation partielle de la théorie de Galois, la « cohomologie ℓ-adique » des fibrations. La cohomologie (ou plutôt l'homologie) d'un espace topologique avait été inventée par Poincaré et, dès les années 1940, André Weil montrait l'intérêt de la transposer en géométrie algébrique. Après des travaux pionniers de Jean-Pierre Serre, Grothendieck a réalisé cette transposition, associant à toute fibration sur un schéma S des espaces de cohomologie ℓ-adique qui sont des représentations[3] linéaires continues du groupe fondamental π_S ; on parle de représentations galoisiennes de S. On aurait une généralisation complète de la théorie de Galois si l'on savait remonter de celles-ci aux variétés algébriques ; c'est l'objet de la théorie des « motifs » de Grothendieck qui, aujourd'hui encore, reste conjecturale. En dehors de la dimension relative 0, on ne connaît guère que le cas particulier des variétés dites « abéliennes » qui avait été conjecturé par John Tate et fut démontré par Gerd Faltings en 1983 : quand deux variétés abéliennes ont même cohomologie ℓ-adique, elles se paramètrent l'une par l'autre. Mais s'il est vrai que la catégorie des fibrations (ou plutôt des motifs) sur un schéma de base S équivaut à celle des représentations galoisiennes de S, le problème de déterminer ces représentations et leurs relations mutuelles se pose de façon cruciale.

– Laurent Lafforgue, Institut des hautes études scientifiques (IHES), Le Bois-Marie, 35 route de Chartres, 91440 Bures-sur-Yvette.
laurent@ihes.fr

Encadré 1

ÉQUATIONS POLYNOMIALES ET THÉORIE DE GALOIS

L'équation générale du troisième degré, à coefficients complexes par exemple, se résout classiquement en deux étapes. Tout d'abord, on ramène cette équation à la forme

$$P(X) = X^3 - pX + q = 0,\ p, q \text{ réels}$$

(on élimine le terme en X^2),

puis on cherche une racine x de P sous la forme :

$$x = u + v \text{ avec la condition } 3uv = p.$$

En développant $P(u+v)$, on obtient le système :

$$\begin{cases} u^3 + v^3 = -q \\ u^3 v^3 = \dfrac{p^3}{27} \end{cases}$$

que l'on sait résoudre : u^3 et v^3 sont les racines du polynôme $X^2 + qX + \dfrac{p^3}{27}$. On aboutit finalement à la « formule de Cardan » :

$$x = \sqrt[3]{\frac{-q}{2} + \sqrt{\frac{q^2}{4} - \frac{p^3}{27}}} + \sqrt[3]{\frac{-q}{2} - \sqrt{\frac{q^2}{4} - \frac{p^3}{27}}} \qquad (1)$$

donnant bien toutes les racines de P. En effet, le choix de la première racine cubique impose celui de la seconde, du fait de la relation $3uv = p$. L'équation de degré 4 se ramène, par une méthode semblable, à celle de degré 3.
La théorie de Galois permet de montrer l'absence d'une formule semblable à (1) pour l'équation de degré 5 ou supérieur, c'est-à-dire de la forme

L'arithmétique est l'étude des variétés algébriques (et donc des représentations galoisiennes) sur le corps $\mathbb{Q}$ des fractions. Grothendieck lui associe le point Spec $\mathbb{Q}$ mais aussi un schéma de dimension 1, Spec $\mathbb{Z}$, dont les points sont les nombres premiers et sur lequel les fonctions sont les éléments de $\mathbb{Q}$. Cela fait ressembler $\mathbb{Q}$ aux corps de fonctions algébriques sur les courbes. De même qu'une fonction f sur une courbe a un ordre d'annulation (ou de pôle s'il est négatif) $v_p(f)$ en tout point p, de même pour f une fraction et p un nombre premier il y a un unique entier $v_p(f)$ tel que $f/p^{v_p(f)}$ soit sans facteur p. Le corps $\mathbb{Q}$ et les corps de fonctions $F(C)$ des courbes C algébriques sur un corps dont le nombre d'éléments est fini sont appelés des corps globaux. A toute représentation galoisienne d'un tel corps on peut associer une fonction analytique L qui est un produit infini de facteurs indexés par les points de Spec $\mathbb{Z}$ ou C. Ce sont des généralisations de la fonction ζ de Riemann $\left(\zeta(s) = \prod_p \dfrac{1}{1 - p^{-s}}\right)$ et on s'attend à ce que, comme celle-ci, elles admettent un prolongement analytique et une équation fonctionnelle reliant leurs valeurs en s et $1 - s$. Grothendieck l'a

Encadré 2

VARIÉTÉS ALGÉBRIQUES ET SCHÉMAS

*L'objet le plus simple étudié en géométrie algébrique est l'*espace affine $\mathrm{A}^n_{\mathbb{K}}$*, où* $\mathbb{K}$ *est un corps algébriquement clos. Comme ensemble,* $\mathrm{A}^n_{\mathbb{K}}$ *est égal à* $\mathbb{K}^n$*. Il est muni d'une topologie, dite de Zariski, dont les fermés sont les ensembles* $V(I)$ *de zéros dans* $\mathbb{K}^n$ *d'un idéal* I *de* $\mathbb{K}[X_1, ..., X_n]$*.*
Néanmoins, cette topologie est trop pauvre pour permettre de distinguer suffisamment les variétés algébriques. Il faut donc rajouter de la structure. Pour chaque ouvert $U \subset \mathrm{A}^n_{\mathbb{K}}$*, on définit ainsi les* fonctions régulières *sur* U *comme les applications de* U *dans* $\mathbb{K}$ *s'écrivant sous la forme* $\frac{P}{Q}$*, où* P *et* Q *sont deux polynômes,* Q *ne s'annulant pas sur* U*. Ces fonctions ont une propriété remarquable. En effet, se donner une fonction* f *régulière sur* U *équivaut à se donner un recouvrement* $\{U_i\}$ *de* U *par des ouverts, et des fonctions régulières* f_i *sur* U_i *telles que* $f_i = f_j$ *sur* $U_i \cap U_j$*.*
On dit que la correspondance $U \longmapsto \{$ *fonctions régulières sur* U $\}$ *est un* faisceau *sur* $\mathrm{A}^n_{\mathbb{K}}$ *(noter l'analogie avec le faisceau des fonctions* C^∞ *sur une variété* C^∞*).*
Plus généralement, la théorie des schémas de Grothendieck associe à tout anneau commutatif A *un espace topologique, dont les points sont les idéaux premiers de* A*, et les fermés les ensembles* $V(I)$ *d'idéaux premiers contenant un idéal* $I \subset A$*. Cet espace est muni d'un faisceau d'anneaux, moralement construit de sorte que* A *s'identifie aux fonctions régulières sur cet espace. L'objet ainsi créé s'appelle* spectre de A*, noté* $\mathrm{Spec}(A)$*. C'est un schéma affine. Les schémas généraux s'obtiennent par recollement de tels schémas. Regardons de plus près* $\mathrm{Spec}(\mathbb{Z})$ *et* $\mathrm{Spec}(\mathbb{K}[X])$*. On peut les dessiner ainsi :*

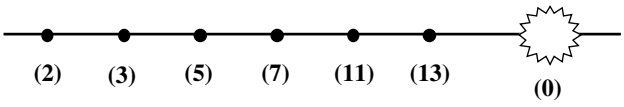

Figure 1 - *Spec* $(\mathbb{Z})$*.*

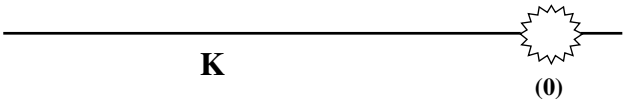

Figure 2 - *Spec* $(\mathbb{K}[X])$*.*

Dans les deux cas, l'espace topologique considéré ressemble à une droite avec la topologie des parties finies, plus un point dense η *correspondant à l'idéal nul. Si* $\mathbb{K}$ *est dénombrable, ces deux espaces sont homéomorphes. Néanmoins, les deux schémas considérés ne sont pas isomorphes : leurs faisceaux de fonctions régulières sont tout à fait différents.*
Considérons le schéma $S = \mathrm{Spec}(\mathbb{K}[X_1, ..., X_n]/(P))$*, où* P *est un polynôme irréductible. Les points fermés de* S *correspondent aux idéaux maximaux de* $\mathbb{K}[X_1, ...X_n]$ *contenant* P *qui, d'après le théorème des zéros de Hilbert, sont en bijection avec les solutions dans* $\mathbb{K}^n$ *de l'équation* $P = 0$ *: il en résulte que* S *est une* hypersurface algébrique*.*

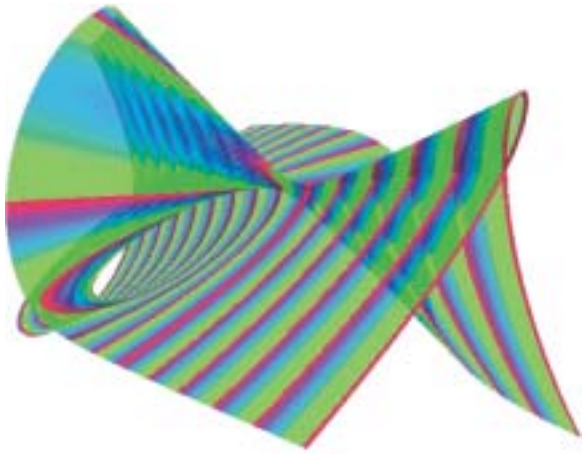

Figure 3 - *Une hypersurface algébrique.*

Cet exemple, joint à celui de $\mathrm{Spec}(\mathbb{Z}[i])$ *étudié dans l'encadré 3, montre comment la théorie des schémas est une généralisation commune de l'arithmétique et de la géométrie algébrique.*

prouvé dans le cas des corps de fonctions comme conséquence d'un résultat venu de la topologie, la « dualité de Poincaré ». Mais on ne connaît toujours pas la dualité sur $\mathrm{Spec}\,\mathbb{Z}$ ...

C'est *via* les fonctions L que, selon la prédiction du mathématicien canadien Robert Langlands, la théorie de Galois rejoint l'analyse harmonique. Il s'agit de la branche des mathématiques créée au XIX$^{\mathrm{e}}$ siècle par

Encadré 3

REVÊTEMENTS ÉTALES ET GROUPE FONDAMENTAL

Nous expliquons ici comment la notion de revêtement, bien connue pour les bons espaces topologiques, se généralise aux schémas. Pour simplifier, tous les schémas seront ici supposés connexes. Nous devons donc traduire en géométrie algébrique la notion d'isomorphisme local qui, transposée naïvement, ne donnerait rien. Un morphisme surjectif entre schémas, qui est un isomorphisme local, est en effet un isomorphisme, car les ouverts de Zariski sont denses pour une classe très large de schémas. Il faut donc raffiner cette topologie, pour en obtenir une nouvelle appelée topologie étale. *Ce n'est pas une topologie au sens usuel : elle consiste en la donnée, pour tout schéma X, de familles de morphismes entre schémas* $\{U_i \xrightarrow{f_i} X\}$ *vérifiant certaines propriétés qui axiomatisent la notion de « recouvrement de X par des ouverts* $U_i \hookrightarrow X$ *».*

Les applications $\{U_i \xrightarrow{f_i} X\}$ *considérées ici sont les* morphismes étales. *Une bonne définition de ces morphismes est celle du* critère jacobien *:* $\{U \xrightarrow{f_i} X\}$ *est dit étale si localement f présente U à l'aide d'équations polynomiales* $P_1(X_1, ..., X_n) = ... = P_n(X_1, ..., X_n) = 0$ *avec* $\det(\frac{\delta P_i}{\delta P_j})$ *inversible. On pourrait penser que U est une bande horizontale étalée sans rebroussement sur X :*

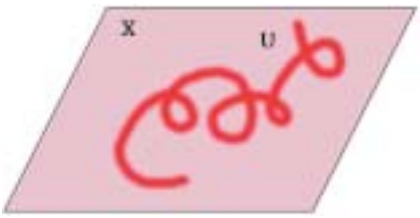

Figure 1

Cela ne reflète cependant pas la richesse de cette notion. Par exemple, si $X = \mathrm{Spec}(\mathbb{K})$*, alors U sera du type* $\mathrm{Spec}(\mathbb{L})$*, où* $\mathbb{L}$ *est un corps, extension finie séparable de* $\mathbb{K}$*.*

Un revêtement *entre schémas est, à peu de choses près, un morphisme* $U \to X$ *étale et surjectif. Par exemple,* $\mathbb{C}^* \to \mathbb{C}^*$*,* $x \mapsto x^n$*, est un revêtement étale du schéma* $\mathbb{C}^* = \mathrm{Spec}(\mathbb{C}[X, \frac{1}{X}])$*. Comme en topologie, on a la notion de* revêtement galoisien*, et tout revêtement est en dessous d'un revêtement galoisien. De plus, si* $X = \mathrm{Spec}(\mathbb{K})$*, les revêtements galoisiens correspondent aux extensions de corps galoisiennes.*

Bien qu'il n'existe pas en général de revêtement universel pour un schéma S donné, il existe un groupe fondamental Π_S*, dont les quotients finis sont les groupes d'automorphismes des revêtements galoisiens. Il est remarquable, et non trivial, que* $\Pi_{\mathrm{Spec}(\mathbb{Z})} = \{e\}$*, c'est-à-dire que tout corps de nombres* $\mathbb{K}$ *est ramifié en au moins un nombre premier p. Par exemple, le morphisme canonique* $\mathrm{Spec}(\mathbb{Z}[i]) \mapsto \mathrm{Spec}(\mathbb{Z})$ *est ramifié au point* $(1+i)$ *: si l'on enlève ce point, le morphisme obtenu sera étale. Le morphisme en question peut se dessiner ainsi :*

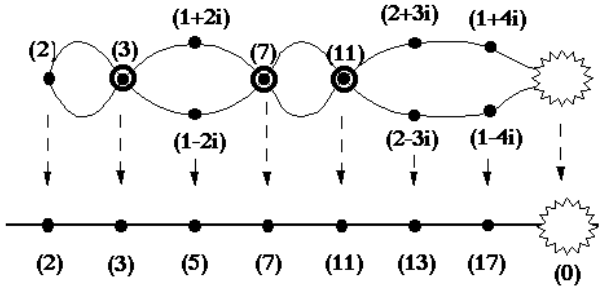

Figure 2

Joseph Fourier pour analyser les ondes et qui étudie les fonctions périodiques, par exemple cos et sin sur $\mathbb{R}$ avec le groupe de périodes $2\pi\mathbb{Z}$. On associe à un corps global $F = \mathbb{Q}$ ou $F(C)$ son « anneau[4] des adèles » $\mathbb{A}_F$ qui est un produit infini de corps F_p « localisés de F » en tous les points p de $\mathrm{Spec}\,\mathbb{Z}$ ou C. On appelle automorphes les fonctions sur le groupe $\mathrm{GL}_r(\mathbb{A}_F)$ des matrices $r \times r$ inversibles à coefficients dans $\mathbb{A}_F$ qui admettent $\mathrm{GL}_r(F)$ comme groupe de périodes ; sous une forme différente leur première étude remonte à Poincaré. A toute représentation automorphe de $\mathrm{GL}_r(\mathbb{A}_F)$, Langlands a associé une fonction analytique L, définie aussi par un produit infini de facteurs indexés par p et qui admet un prolongement analytique et une équation fonctionnelle. Il conjectura le fabuleux énoncé suivant : pour tout $r \geqslant 1$, il existe une unique correspondance préservant les fonctions L, $\sigma \mapsto \pi_\sigma$, $\pi \mapsto \sigma_\pi$ entre l'ensemble des représentations galoisiennes σ de dimension r de F et celui des représentations automorphes π de $\mathrm{GL}_r(\mathbb{A}_F)$.

Le cas $r = 1$ est une reformulation, déjà connue d'Emil Artin (1898-1962), de la théorie du « corps de classes » qui a occupé tous les arithméticiens au XIX$^{\text{e}}$ siècle et jusque dans les années 1930. Les cas $r \geqslant 2$ sont encore plus subtils car les groupes $\mathrm{GL}_r(\mathbb{A}_F)$ ne sont plus commutatifs.

Pour $F = F(C)$ et grâce aux équations fonctionnelles de Grothendieck, on a pu montrer que s'il y a des appli-

Encadré 4

THÉORIE DU CORPS DE CLASSES

Un problème majeur des mathématiques actuelles est la description du groupe de Galois de $\overline{\mathbb{Q}}/\mathbb{Q}$. *Cette question est extrêmement délicate. Néanmoins, la théorie du corps de classes apporte une réponse partielle. Elle comporte deux volets.*
Le premier est local : on s'intéresse aux corps locaux, *par exemple les nombres p-adiques ou les séries formelles sur un corps fini. Le résultat principal est le suivant.*
La correspondance :

$$\{extensions\ finies\ abéliennes\ de\ \mathbb{K}\}$$
$$\longrightarrow \{sous\text{-}groupes\ de\ \mathbb{K}^* d'indice\ fini\}$$

$$\mathbb{L} \longmapsto \mathrm{N}_{\mathbb{L}/\mathbb{K}}(\mathbb{L}^*)$$

est bijective, $\mathrm{N}_{\mathbb{L}/\mathbb{K}}$ *désignant la norme de l'extension* $\mathbb{L}/\mathbb{K}$. *De plus, on dispose d'un isomorphisme, défini pour toute extension galoisienne* $\mathbb{L}/\mathbb{K}$ *:*

$$(\alpha, \mathbb{L}/\mathbb{K}) \ : \ \mathbb{K}^*/\mathrm{N}_{\mathbb{L}/\mathbb{K}}(\mathbb{L}^*) \xrightarrow{\sim} \mathrm{Gal}^{ab}_{\mathbb{L}/\mathbb{K}}$$

jouissant de nombreuses propriétés fonctorielles. On a ainsi une description de $\mathrm{Gal}^{ab}_{\mathbb{L}/\mathbb{K}}$, *le plus grand quotient abélien de* $\mathrm{Gal}_{\mathbb{L}/\mathbb{K}}$. *Ces résultats peuvent s'obtenir de multiples manières, notamment grâce à la dualité de Nakayama-Tate entre certains groupes de cohomologie galoisienne.*
L'autre volet de la théorie du corps de classes traite des corps globaux. *Pour fixer les idées,* $\mathbb{K}$ *désigne maintenant un corps de nombres. Le rôle joué dans le cas local par* $\mathbb{K}^*$ *est ici tenu par le groupe* $\mathrm{C}_{\mathbb{K}} = \mathrm{I}_{\mathbb{K}}/\mathbb{K}^*$ *des* classes d'idèles *de* $\mathbb{K}$. *On note ici* $\mathrm{I}_{\mathbb{K}}$ *le groupe des idèles de* $\mathbb{K}$, *défini pour* $\mathbb{K} = \mathbb{Q}$ *par* $\mathrm{I}_{\mathbb{Q}} = \mathbb{R}^* \times \prod'_{p\in\mathcal{P}} \mathbb{Q}_p^*$, *où* $\mathcal{P}$ *désigne l'ensemble des nombres premiers,* $\mathbb{Q}_p$ *le corps des nombres p-adiques et* $\prod'$ *la partie du produit formée des éléments qui sont presque partout des unités. En général, les facteurs du produit définissant* $\mathrm{I}_{\mathbb{K}}$ *sont les complétés de* $\mathbb{K}$ *pour toutes les valeurs absolues de* $\mathbb{K}$. *Ces corps sont* $\mathbb{R}$ *ou* $\mathbb{C}$ *pour des valeurs absolues archimédiennes et des extensions finies de corps p-adiques pour les autres. On a alors deux théorèmes analogues aux précédents, en remplaçant* $\mathbb{K}^*$ *(resp.* $\mathbb{L}^*$*) par* $\mathrm{C}_{\mathbb{K}}$ *(resp.* $\mathrm{C}_{\mathbb{L}}$*). Les ingrédients de la démonstration sont toujours de nature cohomologique, mais également analytique : le théorème de Cebotarev – vaste généralisation du théorème de la progression arithmétique de Dirichlet – intervient à un point crucial de la preuve. En fait, la théorie du corps de classes donne même une description de l'abélianisé de* $\mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ *tout entier pour un corps global* $\mathbb{K}$. *Cela revient à décrire toutes les représentations continues de dimension 1 de* $\mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ *; c'est en cela que cette théorie coïncide avec le programme de Langlands pour* $r = 1$.

Encadré 5

REPRÉSENTATIONS AUTOMORPHES

Nous précisons ici la notion de représentation automorphe *du groupe* $\mathrm{GL}_r(\mathbb{A})$. *Pour simplifier l'exposé, nous considérons ici un corps* F *de fonctions sur une courbe algébrique C définie sur un corps fini, par exemple* $\mathrm{F} = \mathbb{F}_p(t)$. L'anneau des adèles *de F est ici* $\mathbb{A} = \prod'_{x\in C} \mathrm{F}_x$, *où* F_x *désigne le corps local obtenu par complétion de* F *au point* $x \in C$, *et* $\prod'$ *la sous-partie du produit formée des éléments qui sont presque partout des entiers, c'est-à-dire éléments de l'anneau des entiers* $\mathrm{O}_x \subset \mathrm{F}_x$.
L'anneau $\mathbb{A}$ *est muni d'une topologie dont une base de voisinages ouverts de* 0 *est donnée par les ensembles* $\prod_{x\in\mathcal{S}} \mathrm{H}_x \times \prod_{x\notin\mathcal{S}} \mathrm{O}_x$, *où* $\mathcal{S} \subset C$ *est fini et* $\mathrm{H}_x \subset \mathrm{F}_x$ *est ouvert pour* $x \in \mathcal{S}$. *On a une injection naturelle* $\mathrm{F} \hookrightarrow \mathbb{A}$.
On appelle forme automorphe *sur* $\mathrm{GL}_r(\mathbb{A})$ *une fonction* $f : \mathrm{GL}_r(\mathbb{A}) \to \mathbb{C}$ *possédant les propriétés :*

- *f est invariante à gauche par* $\mathrm{GL}_r(\mathbb{F})$ *:* $f(\gamma x) = f(x)$ $(\gamma \in \mathrm{GL}_r(\mathbb{F}),\ x \in \mathrm{GL}_r(\mathbb{A}))$
- *f est invariante à droite par un sous-groupe ouvert* $\mathrm{H} \subset \mathrm{GL}_r(\mathbb{A})$ *:* $f(x) = f(xh)$ $(h \in \mathrm{H},\ x \in \mathrm{GL}_r(\mathbb{A}))$

En toute rigueur, il faudrait demander une troisième condition que nous omettons ici.
Le groupe $\mathrm{GL}_r(\mathbb{A})$ *opère sur l'espace* $\mathcal{A}$ *des formes automorphes par :*
$(g.f)(x) = f(xg)$ *(avec* $f \in \mathcal{A}$ *et* $x, g \in \mathrm{GL}_r(\mathbb{A})$*).*
Une représentation automorphe *est une représentation irréductible de* $\mathrm{GL}_r(\mathbb{A})$ *qui se réalise dans l'espace* $\mathcal{A}$.
Rappelons qu'une représentation $\rho : \mathrm{G} \to \mathrm{GL(V)}$ *est dite irréductible si les seuls sous-espaces de* V *stables par* ρ *sont* {0} *et* V. *Une représentation automorphe s'écrit toujours comme produit tensoriel infini de facteurs locaux, qui sont des représentations irréductibles des groupes* $\mathrm{GL}_r(\mathrm{F}_x)$.
En cela réside l'aspect local de cette théorie. L'aspect global est quant à lui contenu dans l'invariance à gauche des formes automorphes par le sous-groupe $\mathrm{GL}_r(\mathrm{F})$.

cations $\pi \mapsto \sigma_\pi$ en rangs $< r$, il y en a en sens inverse $\sigma \mapsto \pi_\sigma$ en rangs $\leqslant r$. Pour $F = \mathbb{Q}$ et en dehors de $r = 1$, le cas le plus important de construction $\sigma \mapsto \pi_\sigma$ connu à ce jour est dû à Andrew Wiles : c'est quand σ provient d'une courbe elliptique (une variété abélienne de dimension 1). D'après le théorème de Faltings cité plus haut, cela signifie que toute courbe elliptique sur $\mathbb{Q}$ se paramètre par ce que l'on appelle une courbe modulaire et, comme chacun sait, cela implique le théorème de Fermat.

Dans l'autre sens $\pi \mapsto \sigma_\pi$, on cherche à trouver les σ_π dans la cohomologie ℓ-adique de variétés algébriques sur F convenables. Pour $F = F(C)$, le mathématicien ukrainien Vladimir Drinfeld a proposé au début des années 70 une réponse conjecturale à cette question, les variétés de « chtoucas » ; il démontra le cas $r = 2$. Récemment, l'auteur de cet article a généralisé en rang arbitraire la preuve de Drinfeld si bien qu'aujourd'hui la correspondance de Langlands sur les corps de fonctions est démontrée. Sur $F = \mathbb{Q}$, une réponse partielle est fournie conjecturalement par des variétés introduites dès avant que Langlands formule son programme par le mathématicien japonais Shimura et qui généralisent les courbes modulaires. Mais la cohomologie de ces variétés ne peut contenir qu'une partie des représentations galoisiennes et, en général, on ne sait pas encore la calculer.

Les théories de Galois et de Grothendieck et le programme de Langlands qui les complète sont une grande et belle réalisation de l'esprit humain. Nul doute que les problèmes non résolus qu'ils proposent – les motifs, la cohomologie des variétés de Shimura ou d'autres plus générales qui restent à définir, les propriétés des fonctions L des représentations galoisiennes – resteront longtemps à l'horizon de la géométrie algébrique et de l'arithmétique.

Quelques définitions

(1) Un groupe est un ensemble muni d'une loi de composition $(g_1, g_2) \longmapsto g_1 g_2$, d'un élément 1 et d'un passage à l'inverse $g \longmapsto g^{-1}$. Il est dit commutatif ou abélien si l'on a toujours $g_1 g_2 = g_2 g_1$.

Une action d'un groupe sur un ensemble fini consiste à associer à tout élément du groupe une permutation des éléments de l'ensemble, de façon compatible avec les lois de composition.

(2) Une catégorie est une collection d'objets et de relations entre ces objets.

(3) Une représentation linéaire d'un groupe est un espace vectoriel muni de transformations linéaires indexées par les éléments du groupe, de façon compatible avec les lois de composition.

(4) Un anneau est un ensemble où existent les trois opérations +, – et $\times$ mais pas nécessairement la division /.