Troisième séance
samedi 12 mai 2007

Idées galoisiennes (symétries et invariants)

«Il existe pour ces sortes d'équations
un certain ordre de considérations métaphysiques
qui planent sur les calculs
et qui souvent les rendent inutiles.»

«Sauter à pieds joints sur les calculs,
grouper les opérations, les classer
suivant leur difficulté et non suivant leur forme,
telle est selon moi la mission des géomètres futurs.»
É. Galois.

****

Évariste Galois : révolutionnaire - en politique et en mathématique - mort en 1832 dans sa vingtième année.

Éduqué par sa mère à Bourg-la-Reine (dont son père est le maire), puis élève au lycée Louis-le Grand où il se passionne pour les mathématiques suite à la lecture, à quinze ans, des Éléments de Géométrie de Legendre, Galois commence à lire les mémoires des grands mathématiciens contemporains (Lagrange, Gauss, Jacobi), et obtient le premier prix du concours général dans cette discipline. Il échoue néanmoins au concours d'entrée à l'École Polytechnique, quelques jours après le suicide de son père suite à une cabale du curé du village. Il obtient, dès dix-huit ans, des résultats mathématiques d'une portée incomparable («théorie de l'ambiguïté», théorie des intégrales abéliennes) qu'on a pu qualifier d'acte de naissance des mathématiques contemporaines.

Pendant la révolution de juillet 1830, Galois est élève à l'École Préparatoire (future École Normale Supérieure), et consigné comme ses condisciples[1]. Suite à la publication de deux lettres de lui (brocardant le directeur, et la misère de l'enseignement scientifique), il est renvoyé, et, sans ressource, ouvre un cours privé d'algèbre supérieure chez un libraire du quartier latin.

Il s'engage alors très activement dans la lutte politique, au sein de la Société des Amis du Peuple présidée par Raspail. Toast régicide puis manifestation en tenue illégale de garde républicain lui valent de passer l'essentiel de la dernière année de sa vie en prison. C'est en partie là qu'il rédige ses mémoires les plus importants, dont la plupart ont été perdus (par Cauchy et par Fourier) ou rejetés (par Poisson). Il meurt fin mai 1832, à vingt ans et demi, le lendemain d'un duel dont les circonstances restent obscures

[1] du côté musical, rappelons que 1830 est l'année de la Symphonie Fantastique de Berlioz.

(«pour une infâme coquette», écrit-il). La nuit précédant le duel, il a écrit une splendide lettre-testament qui sera évoquée ci-dessous.

Épilogue : en 1843, Liouville exhume un mémoire de Galois et expose la «théorie de l'ambiguïté» à l'Académie des Sciences. Depuis, l'influence de ces idées n'a cessé de croître.

En suivre certaines lignes de force jusque dans les mathématiques les plus contemporaines, tel est l'objet de cet exposé dont le thème central est celui de *groupe de symétries* et d'*invariant*.

Plan

****

1 Théorie de Galois des équations algébriques.

1.1 Résolubilité par radicaux.

«Mon cher Ami, j'ai fait en analyse plusieurs choses nouvelles. Les unes concernent la théorie des équations, les autres les fonctions intégrales. Dans la théorie des équations, j'ai recherché lesquelles étaient résolubles par radicaux...» Ainsi débute la lettre-testament de Galois.

Une équations algébrique de degré n est une équation de la forme

$$(*) \quad x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$$

où les coefficients a_i sont des constantes (par exemple des nombres rationnels), et x est l'inconnue (appelée racine de l'équation).

La recherche de «formules» pour les racines x d'une telle équation est un problème très ancien, qui, au XVI^e siècle avait été résolu jusqu'au degré $n = 4$ au moyen de techniques de changement de variables et substitutions (Tartaglia, Cardano[2], del Ferro, Ferrari). Ces formules se présentent sous la forme d'expressions faisant intervenir des radicaux $\sqrt[m]{}$, pour $m \leq n$.

[2]Ars Magna, 1545.

Par exemple, la formule donnant une solution de l'équation du troisième degré

$$x^3 + a_1 x + a_0 = 0$$

est

$$x = \sqrt[3]{-\frac{a_0}{2} + \sqrt{(\frac{a_0}{2})^2 + (\frac{a_1}{3})^3}} + \sqrt[3]{-\frac{a_0}{2} - \sqrt{(\frac{a_0}{2})^2 + (\frac{a_1}{3})^3}}.$$

On notera toutefois que de telles formules présentent des ambiguïtés techniques (dans la prise des radicaux), liées à une ambiguïté de fond : comment briser l'indiscernabilité a priori des racines de l'équation ?

Autre souci : ces formules peuvent faire intervenir des racines carrées de nombres négatifs (exclus jusqu'au XVI^e siècle), même lorsque la solution x est rationnelle : par exemple la formule précédente exprime la racine $x = 4$ de l'équation $x^3 - 15x - 4$ sous la forme alambiquée

$$x = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}}.$$

Ces problèmes étaient néanmoins à peu près circonscrits (sinon réglés) après les travaux de Bombelli. À la fin du XVI^e, Viète systématisa l'usage des lettres pour noter coefficients et inconnues, et découvrit la relation entre coefficients de $(*)$ et fonctions symétriques des racines. Malgré tout l'intérêt du bouleversement conceptuel qui accompagna l'assimilation progressive des racines imaginaires et la clarification de la notion-même de racine[3], je n'en dirai pas plus, considérant que cela appartient à la préhistoire de notre sujet.

Il fallut plus de deux siècles avant de pouvoir aller au-delà du degré $n = 4$ dans la question de la résolution «par radicaux» des équations. Les travaux de Lagrange sur la technique des résolvantes à la fin du XVIII^e siècle mirent en lumière le rôle crucial joué par les permutations des racines, sans toutefois résoudre le problème.

Mais c'est N. Abel, précurseur de Galois mort à 26 ans en 1829, qui le premier démontra rigoureusement l'impossibilité de résoudre l'équation générale du 5^e degré par radicaux.

Peu après, Galois s'empara du problème de la résolubilité par radicaux et le résolut complètement en donnant une condition nécessaire et suffisante portant sur un certain groupe de symétries des racines de l'équation,

1.2 Le groupe de Galois.

Voici comment Galois l'introduit lui-même, sous forme d'un

«*Théorème.* Soit une équation donnée, dont $a, b, c \ldots$ sont les racines. Il y aura toujours un groupe de permutations des lettres $a, b, c \ldots$ qui jouira de la propriété suivante :

1. que toute fonction des racines, invariable par les substitutions de ce groupe, soit rationnellement connue,[4]

[3] dans le cas des équations dont les coefficients sont des nombres, on peut considérer que la question a été complètement élucidée par le classique «théorème fondamental de l'algèbre» (énoncé par Girard, «justifié» par D'Alembert, puis démontré rigoureusement par Gauss) : toute équation $(*)$ de degré non nul, à coefficients a_i dans le corps $\mathbb{C}$ des nombres complexes, a au moins une racine dans $\mathbb{C}$.

[4] ce qui signifie : exprimable à partir des coefficients de l'équation *rationnellement*, c'est-à-dire en ne faisant intervenir que l'addition, la soustraction, la multiplication, la division.

2. réciproquement, que toute fonction des racines, déterminable rationnellement, soit invariable par ces substitutions. »

C'est sans doute là l'une des toutes premières apparitions de la notion mathématique de groupe. En fait, Galois ne considère pas de «groupes abstraits»[5], mais seulement des groupes de substitutions, c'est-à-dire des ensembles de permutations de $a, b, c \ldots$ qui sont stables par composition et par passage à l'inverse. Mais, comme on va voir, c'est bien la structure de ces groupes qui l'intéresse, et non le calcul des permutations des $a, b, c \ldots$ elles-mêmes (comme chez Lagrange).

Mon but n'étant pas de nature historique, c'est non pas avec les mots-mêmes de Galois, mais sous la forme moderne et compacte que lui ont donnée au tournant du XX^e siècle Kronecker, Weber, et (définitivement) Artin, que je vais exposer, brièvement, les notions et résultats de base de la théorie.

On part d'un corps de base k qui contient les coefficients a_i de l'équation (par exemple le corps $\mathbb{Q}$ des nombres rationnels). Sans perte de généralité, on peut supposer, et nous supposerons toujours, que l'équation $(*)$ est *irréductible* sur k, c'est-à-dire que le polynôme $x^n + a_{n-1}x^{n-1} + \ldots + a_0$ n'est pas produit de polynômes à coefficients dans k de degrés moindres.

Alors $(*)$ a exactement n racines complexes. On aimerait bien les appeler $x_1, \ldots, x_n$, mais comment les distinguer a priori les unes des autres pour les numéroter ?

C'est précisément sur cette ambiguïté, sur les substitutions indétectables de racines - ou mieux : sur les symétries intrinsèques de l'équation -, que va jouer Galois pour fonder sa théorie, qu'il baptise «théorie de l'ambiguïté»[6].

Notons K le corps engendré sur k par ces racines, c'est-à-dire le corps qu'on obtient en formant toutes les expressions bâties à partir des éléments de k et des racines par addition, soustraction, multiplication, division. Une extension (= sur-corps) du type K/k est dite *normale*.

Le *groupe de Galois* de l'équation algébrique $(*)$ est le groupe des automorphismes du corps K qui fixent k[7] : c'est le groupe des «symétries» de l'extension K/k.

Il est noté $Gal(K/k)$ en l'honneur de son inventeur. Il vérifie les deux propriétés énoncées par Galois :

1. toute expression rationnelle en les racines (c'est-à-dire tout élément de K) qui est invariant par $Gal(K/k)$ est en fait dans k,

[5] C'est semble-t-il Cayley qui donna en 1854 une première définition générale de groupe abstrait (en indiquant d'ailleurs que tout groupe abstrait peut être vu comme groupe de permutations de ses éléments, de sorte que la considération des seuls groupes de substitutions n'est pas limitative) ; mais la condition d'associativité n'est clairement mise en avant que plus tard (Huntington, Moore, 1902). La définition d'un groupe (abstrait) s'est alors stabilisée : un *groupe* est un ensemble G muni d'une loi de composition interne $(x, y) \mapsto x \cdot y$ qui est associative $(x \cdot (y \cdot z) = (x \cdot y) \cdot z)$, admet un élément neutre 1 $(1 \cdot x = x \cdot 1 = x)$, et telle que tout élément x admet un inverse x^{-1} $(x \cdot x^{-1} = x^{-1} \cdot x = 1)$. Exemples : le groupe des permutations d'un ensemble d'objets, le groupe des déplacements dans l'espace, le groupe des transformations canoniques du sujet d'une fugue, etc... Les groupes abstraits (non donnés comme groupes de transformations concrètes, comme dans les exemples précédents) sont souvent définis par générateurs et relations.

Un groupe G est dit *commutatif* ou *abélien* si on a toujours $x \cdot y = y \cdot x$. Exemples : l'addition des vecteurs dans un espace vectoriel, le groupe des transpositions d'un mode musical, etc...

[6] et que l'on a appelée après lui «théorie de Galois».

[7] ce sont les opérateurs du k-espace vectoriel K qui respectent la multiplication.

2. réciproquement, tout élément de k est invariant par $Gal(K/k)$.

Les éléments de $Gal(K/k)$ sont entièrement déterminés par les valeurs qu'ils prennent sur les racines de $(*)$, valeurs qui sont encore des racines de $(*)$. Ainsi $Gal(K/k)$ s'identifie à un sous-groupe du groupe $\mathfrak{S}_n$ des permutations des n racines. On montre que c'est un groupe d'ordre égal à la dimension[8] du k-espace vectoriel K.

1.3 La correspondance de Galois.

Le cœur de la théorie de Galois est une correspondance bijective entre extensions ℓ de k contenues dans l'extension normale K, et sous-groupes H du groupe de Galois $Gal(K/k)$. Elle est définie ainsi :

1. à l'extension ℓ, on associe le sous-groupe H formé des éléments qui fixent ℓ (autrement dit, le groupe de symétries de l'extension K/ℓ),

2. réciproquement, au sous-groupe H, on associe l'extension ℓ formés des éléments de K invariants par H.

Cette *correspondance entre extensions (de corps) et groupes (de symétries)* renverse le sens des inclusions.

Par ailleurs, Galois dégage la notion de sous-groupe *normal* H d'un groupe G. C'est un sous-groupe tel que pour tout $g \in G$, la conjugation par g :

$$h \mapsto g \cdot h \cdot g^{-1}$$

envoie H dans lui-même ; on peut alors former le groupe quotient G/H. Dans la correspondance de Galois, les sous-groupe normaux de $Gal(K/k)$ correspondent aux extensions normales ℓ/k.

Galois introduit aussi la notion de groupe *résoluble*. C'est un groupe qui se «dévisse en groupes abéliens». Plus précisément, un groupe G est dit résoluble s'il existe une chaîne finie de sous-groupes inclus les uns dans les autres, commençant à $\{1\}$ et finissant à G, chacun étant normal dans le suivant avec un quotient abélien. Galois démontre que l'équation $(*)$ est résoluble si et seulement si son groupe de Galois est résoluble. Il démontre en outre que le groupe $\mathfrak{S}_n$ n'est pas résoluble dès que $n \geq 5$, et en déduit qu'il y a des équations de tout degré $n \geq 5$ qui ne sont pas résolubles par radicaux.

Il a par ailleurs utilisé sa correspondance pour classifier tous les corps finis[9].

2 Portée et enjeux de la «théorie de l'ambiguïté».

Galois était pleinement conscient du caractère révolutionnaire, à divers titres, de ses conceptions, et du fait qu'elles dépassaient largement le cadre spécifique des équations algébriques.

[8] qui est comprise entre n et $n! = 1.2 \ldots n$.

[9] on ne connaissait guère avant lui que l'exemple des corps finis obtenus par réduction des entiers modulo un nombre premier p.

2.1 Émergence d'un corps de concepts d'un type nouveau.

L'usage d'une structure algébrique - celle de groupe en l'occurence, suivie par celle d'extension de corps que la théorie «appelle» - comme outil fondamental, et de notions abstraites comme celles de sous-groupes normaux, de groupes résolubles, a modifié l'idée qu'on se faisait de la nature des objets mathématiques.

En mettant l'accent sur les concepts d'opération («abstraite de son résultat») et d'invariant, la démarche galoisienne ouvre un champ conceptuel nouveau aux mathématiques qui marque la naissance de l'algèbre moderne, *cf.* [14].

2.2 Fécondité du principe de correspondance galoisienne.

Selon S. Lie, premier grand continuateur (avec F. Klein) de l'œuvre de Galois, «la grande portée de l'œuvre de Galois tient au fait que sa théorie originale des équations algébriques est une application systématique des deux notions fondamentales de *groupe* et d'*invariant*, notions qui tendent à dominer la science mathématique[10].»

L'idée galoisienne de correspondance entre symétries d'une structure mathématique et treillis de ses sous-structures a essaimé dans d'autres domaines des mathématiques. L'un des premiers et plus célèbres avatars est le programme d'Erlangen de Klein, qui jette un pont entre géométrie et théorie des groupes : il s'agit de classifier les géométries de l'espace à n dimensions où le «mouvement d'une figure invariable est possible» - et, en toile de fond, de comprendre de manière unifiée les géométries classiques de l'époque (géométries euclidienne, affine, projective, sphérique, elliptique, hyperbolique, conforme). Klein montre qu'elles correspondent à certains groupes G de «déplacements» : la géométrie correspondant à G est définie par les propriétés des figures (parties de l'espace) telles que G soit exactement le groupe de déplacements qui conservent ces propriétés, ou par les classes invariantes par G de figures (on peut alors chercher à classifier ces figures pour l'action de G, c'est-à-dire déterminer les orbites). Par exemple, pour le groupe affine G, les coniques forment une classe invariante, et se répartissent en trois orbites : ellipses, paraboles, hyperboles.

Comme l'écrit G. Bachelard dans sa polémique contre E. Meyerson sur le principe d'identité [3, p. 83], «des êtres géométriques qui sont *invariants* dans les opérations d'un sous-groupe G' du groupe général G de la géométrie euclidienne peuvent cesser d'être invariants pour des opérations qui, comprises dans G, ne figurent pas dans G'. Leur «identité» est donc simplement relative au groupe qui définit le système rationnel qui sert de base à l'examen de leurs propriétés. [...] Qu'une sphère et un ellipsoïde soient des surfaces identiques du point de vue de l'Analysis Situs, voilà un fait qui nous libère d'une *identité en soi*. [...]

Dès qu'on aborde les géométries très spécialisées, le principe d'identité pose un discernement très travaillé. [...] Les géométries ont besoin chacune d'un protocole d'identification. [...] Si l'on suivait en détail ces *applications* de la pensée algébrique à la géométrie, on s'apercevrait que fonctionne toujours - plus ou moins tacitement - une fonction d'adverbe à côté de l'adjectif *identique*. [...] On devrait donc, si l'on veut se cantonner dans la géométrie usuelle, parler de figures *euclidiennement* identiques.»

[10] de l'époque, tout au moins !

Le point de vue que promeut Klein est que c'est le groupe sous-jacent qui fonde une géométrie, car c'est lui qui permet la définition même de l'identité des figures. Qu'il apparaisse encore - en second lieu - comme groupe de symétries des figures est le reflet du principe de correspondance galoisienne.

Nous verrons d'autres avatars plus récents de correspondances galoisiennes dans la suite.

2.3 Thématisation des obstructions.

Avec Galois, la notion vague, à connotation esthétique, de symétrie devient un concept mathématique précis et opératoire.

Les ambiguïtés constituent-elles une *nuisance* ? Non, répond Galois en substance, elles constituent un *groupe* !

Loin d'être un simple zeugma, c'est là un geste de pensée étonnant : geste inaugural de la théorie de l'obstruction (mentionnée dans l'exposé précédent) dont l'objet est de réaliser les obstructions à effectuer telle ou telle opération mathématique comme éléments d'un nouvel objet mathématique (souvent un groupe) ; l'étude de ce nouvel objet *per se* livre la clé du problème. Sur un plan philosophique beaucoup plus général, ce geste inaugure un

2.4 Changement de paradigme dans la conception des problèmes mathématiques.

Ce point a été bien cerné par G. Deleuze [6, p. 233] :

«On se rappelle, en effet, le cercle dans lequel tourne la théorie des problèmes : un problème n'est résoluble que dans la mesure où il est «vrai», mais nous avons toujours tendance à fonder le caractère extrinsèque de la résolubilité dans le caractère intérieur du problème (Idée), nous faisons dépendre le caractère interne du simple critère extérieur. Or, si un tel cercle a été brisé, c'est d'abord par le mathématicien Abel ; c'est lui qui élabore toute une méthode d'après laquelle la résolubilité doit découler de la forme du problème. Au lieu de chercher comme au hasard si une équation est résoluble en général, il faut déterminer des conditions de problèmes qui spécifient progressivement des champs de résolubilité, de telle manière que «l'énoncé contienne le germe de la solution». Il y a là un renversement radical dans le rapport solution-problème [...]

Le même jugement se confirme, appliqué aux travaux de Galois : à partir d'un «corps» de base, les adjonctions successives à ce corps permettent une distinction de plus en plus précise des racines d'une équation, par limitation progressive des substitutions possibles. Il y a donc une cascade de «résolvantes partielles» ou un emboîtement de «groupes», qui font découler la solution des conditions mêmes du problème : qu'une équation ne soit pas résoluble algébriquement, par exemple, cela n'est plus découvert à l'issue d'une recherche empirique ou d'un tâtonnement, mais d'après les caractères des groupes et des résolvantes qui constituent la synthèse du problème et de ses conditions. [...]

Le groupe de l'équation caractérise à un moment, non pas ce que nous savons des racines, mais l'objectivité de ce que nous n'en savons pas. Inversement, ce non-savoir n'est plus un négatif, une insuffisance, mais une règle, un *apprendre* auquel correspond une dimension fondamentale de l'objet.»

3 Revêtements, groupes fondamentaux, dessins d'enfants.

3.1 La «montée vers l'absolu». Le groupe $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$.

La correspondance galoisienne concerne les extensions intermédiaires $k \subset \ell \subset K$, l'extension normale K/k étant fixée. On peut aussi ne fixer que le corps de base k, disons $k = \mathbb{Q}$, et faire varier l'extension normale $K/\mathbb{Q}$: lorsque K grossit (c'est-à-dire lorsqu'on adjoint de plus en plus de nombres algébriques), on obtient ainsi un système «projectif» de groupes finis s'envoyant les uns sur les autres :

$$\cdots \to Gal(K/\mathbb{Q}) \to \cdots \to Gal(\mathbb{Q}/\mathbb{Q}) = \{1\}.$$

La limite $\varprojlim_K Gal(K/\mathbb{Q})$ de ce système est le groupe infini[11]

$$Gal(\bar{\mathbb{Q}}/\mathbb{Q})$$

des automorphismes du corps $\bar{\mathbb{Q}}$ des nombres algébriques[12].

C'est cette démarche qu'A. Lautman appelle la «montée vers l'absolu» [10, III] : un seul objet mathématique, le groupe de Galois absolu, code les propriétés de toutes les équations algébriques à coefficients rationnels à la fois.

Ce *groupe de Galois absolu* $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$, objet central de la théorie des nombres, reste largement un mystère après un siècle et demi d'efforts intenses pour en comprendre la structure.

3.2 Théorie de Galois des revêtements.

Il s'agit d'une «jumelle» géométrique de la théorie de Galois des nombres algébriques. En voici un aperçu dans le cadre des revêtements de surfaces de Riemann évoqués dans l'exposé précédent.

L'histoire commence en 1877 lorsque Klein remarque que le groupe des isométries laissant invariant l'icosaèdre est isomorphe au groupe de Galois d'une équation quintique à coefficients dans le corps de fonctions rationnelles d'une variable auxiliaire. On a maintenant deux variables, et les solutions complexes de l'équation quintique forment une surface de Riemann, qui est un revêtement du plan complexe.

Plus généralement, on a la notion de revêtement[13] fini normal $Y \to X$ de surfaces de Riemann. C'est l'avatar géométrique d'une équation $(*)$: ce qui joue le rôle de racines de l'équation est l'ensemble $\{y_1, \ldots, y_n\}$ des points de Y qui s'envoient sur un point x arbitraire fixé de X. Le groupe de Galois $Gal(Y/X)$ est un sous-groupe du groupe $\mathfrak{S}_n$ des permutations de $\{y_1, \ldots, y_n\}$[14]. Il peut se calculer comme suit : traçons sur X un lacet γ pointé en x, et choisissons un point y_i de Y au-dessus de x. Un tel γ se «relève»

[11] il est naturellement muni d'une structure de groupe topologique compact.

[12] nombres vérifiant une équation algébrique à coefficients rationnels.

[13] qu'on suppose non ramifié pour simplifier.

[14] dans le cas de la quintique de Klein, le groupe de Galois est le groupe de l'icosaèdre, auquel Klein a consacré un ouvrage classique.

alors en un chemin sur Y partant de y_i, qui en général aboutira à un autre point y_j, d'où une permutation $y_i \mapsto y_j$ de l'ensemble des points au-dessus de x, qui ne dépend en fait du lacet γ qu'à homotopie (= déformation) près. C'est ainsi que s'obtiennent les éléments de $Gal(Y/X)$.

Dans ce contexte, on peut encore effectuer une «montée vers l'absolu». Ce qui correspond au corps $\bar{\mathbb{Q}}$ est maintenant le *revêtement universel* de X, et son groupe d'automorphismes n'est autre que le *groupe fondamental* de Poincaré $\pi_1(X)$: c'est groupe des lacets tracés sur X à homotopie près, partant et aboutissant à un point x fixé.

On peut algébriser la construction en remplaçant $\pi_1(X)$ par la limite projective $\hat{\pi}_1(X)$ des groupes $Gal(Y/X)$, lorsque le revêtement Y/X grossit. D'après Grothendieck, $\hat{\pi}_1(X)$ s'interprète comme groupe des automorphismes du foncteur fibre en x

$$Y \mapsto Y_x = \{y_1, \ldots, y_n\}$$

sur la catégorie des revêtements de (X, x) (à valeurs dans la catégorie des ensembles), ce qui permet d'unifier les théories de Galois arithmétique et géométrique dans un même moule.

3.3 Une vision géométrique, voire graphique, de $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$.

Une approche indirecte fascinante de $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ consiste à le relier à la géométrie des surfaces de Riemann.

Pour fixer les idées, prenons pour X le plan complexe privé des points 0 et 1. Son groupe fondamental $\pi_1(X)$ est le groupe libre à deux générateurs, les lacets γ_0 et γ_1 autour de 0 et de 1 (qu'on ne peut «défaire» par déformation). Son complété $\hat{\pi}_1(X)$ s'obtient en permettant des «mots infinis» en γ_0 et γ_1 (et leurs inverses).

Suivant Grothendieck et Belyi, $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ opère sur les revêtements finis de X, donc sur $\hat{\pi}_1(X)$, et cette opération est *fidèle : le groupe de Galois absolu arithmétique* $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ *se plonge dans le groupe des automorphismes du groupe de Galois absolu géométrique* $\hat{\pi}_1(X)$.

De là, Grothendieck a alors proposé de décrire $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ au moyen de notions graphiques «si simples qu'un enfant peut les connaître en jouant». Considérons un revêtement $Y \to X$, en supposant pour simplifier que Y est le plan complexe privé de quelques points. L'image inverse dans Y du segment $]0, 1[$ de X est un objet combinatoire très simple que Grothendieck appelle «dessin d'enfant». Le défi est de comprendre en termes combinatoires l'opération fidèle de $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ sur ces dessins.

Pour ce faire, il faut disposer au préalable d'un codage combinatoire des éléments de $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ lui-même. C'est ce qui a été obtenu par Drinfeld autour de 1990 (en découvrant un lien insoupçonné entre $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ et groupes quantiques) : il plonge $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ dans un groupe de nature combinatoire GT (le groupe de Grothendieck-Teichmüller, défini par générateurs et trois relations très simples), qui s'avère agir fidèlement sur les dessins d'enfants. On ignore à l'heure actuelle si GT est réellement «plus gros» que $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ (on le soupçonne).

4 Ambiguïtés galoisiennes en analyse.

Voici la fin de la lettre-testament de Galois : «Tu sais, mon cher Auguste, que ces sujets ne sont pas les seuls que j'ai explorés. Mes principales méditations depuis quelque temps

étaient dirigées sur l'application à l'analyse transcendante de la théorie de l'ambiguîté. Il s'agissait de voir a priori dans une relation entre quantités ou fonctions transcendantes quels échanges on pouvait faire, quelles quantités on pouvait substituer aux quantités données sans que la relation pût cesser d'avoir lieu. Cela fait reconnaître tout de suite l'impossibilité de beaucoup d'expressions que l'on pouvait chercher. Mais je n'ai pas le temps et mes idées ne sont pas encore bien développées sur ce terrain qui est immense...»

Liouville est le premier à avoir poursuivi dans cette direction : au lieu de se demander quand une équation algébrique est résoluble par radicaux, il se demande quand une équation différentielle linéaire est résoluble à l'aide de fonctions élémentaire (des radicaux, des logarithmes, des exponentielles), et obtient un critère galoisien. Au début du XX^e siècle, Picard et Vessiot introduisent dans ce contexte le *groupe de Galois différentiel* : c'est le groupe formé des automorphismes de l'extension du corps des fonctions de base, obtenu en adjoignant les solutions et leurs dérivées, qui commutent à la dérivation. Du fait que les solutions d'une équations différentielle linéaire forment non plus un ensemble fini, mais un espace vectoriel de dimension finie, le groupe de Galois différentiel n'est plus un groupe fini en général, mais un groupe «continu» de matrices.

La théorie a mûri lentement, et la classification des ambiguïtés galoisiennes dans le cadre des équations différentielles linéaires analytiques au voisinage d'une singularité, due à J. P. Ramis, date seulement de la fin du XX^e siècle. Le résultat est qu'il y a trois types, et trois seulement, de telles ambiguïtés galoisiennes - qui prennent en fait la forme de matrices :

1) la *monodromie* : c'est l'ambiguïté qui résulte de ce que l'on ne retombe pas la valeur initiale lorsque l'on fait subir à une solution un tour autour de la singularité. On a déjà vu ce phénomène dans l'exposé précédent (2.1). Considérons l'équation différentielle

$$y' = \frac{1}{2x} y$$

au voisinage de la singularité 0 ; une solution est $y = \sqrt{x}$, et un tour autour de l'origine la transforme en $-y$. Le groupe de Galois différentiel de cette équation est le groupe à deux éléments engendré par la monodromie.

2) le *recalibrage des exponentielles* : considérons l'équation différentielle

$$xy' + y = 0$$

au voisinage de la singularité 0 ; une solution est $y = e^{1/x}$, et toute autre solution non nulle s'obtient en multipliant y par une constante non nulle. Le groupe de Galois différentiel de cette équation est le groupe multiplicatif $\mathbb{C}^\times$ (des nombres complexes non nuls) engendré par ces recalibrages.

3) les *ambiguïtés de Stokes* : considérons l'équation différentielle

$$xy' + y = x$$

au voisinage de la singularité 0 ; une solution formelle est $\hat{y} = \sum (-1)^n n! x^{n+1}$, qui diverge en tout point $x \neq 0$. Toutefois, il y a moyen de «resommer» cette série divergente de manière canonique pour obtenir une vraie solution dans certains secteurs de sommet 0. Par exemple, dans un secteur bissecté par le demi-axe réel positif, une vraie solution, asymptotique à $\hat{y}$, est $y = \int_0^\infty \frac{e^{-t/x}}{1+t} dt$, mais les changements de secteurs introduisent des ambiguïtés dans ces vraies solutions resommées, les ambiguïtés de Stokes.

De manière générale, le groupe de Galois différentiel est engendré (au sens des groupes «continus») par ces trois types de matrices.

Ainsi la théorie de Galois s'étend, comme Galois l'avait pressenti, aux fonctions transcendantes solutions d'équations différentielles (*cf.* [12]).

5 Groupes de Galois motiviques et nombres transcendants.

Mais laissons là les équations différentielles et même les fonctions, pour revenir aux nombres. La théorie de Galois, initialement conçue dans le cadre des nombres algébriques, s'étend-elle aux nombres transcendants ?

Il s'avère que la réponse est oui, du moins conjecturalement, pour des nombres qui s'écrivent comme intégrales multiples

$$\int\int\cdots\int_{\Delta}\omega$$

où le domaine d'intégration Δ est limité par des équations polynômiales définies sur $\mathbb{Q}$ et l'intégrant ω est une algébrique et définie sur $\mathbb{Q}$. Par exemple, le nombre $\pi = \int_0^1 4\sqrt{1-t^2}dt$ est de ce type.

Pour ces nombres, la réponse conjecturale est donnée par la *théorie des motifs* (imaginée par Grothendieck), plus précisément par la théorie de Galois motivique qui est une vaste généralisation (partiellement conjecturale) de la théorie de Galois qui s'applique aux systèmes de plusieurs équations algébriques à plusieurs variables.

Dans le cas de π, la réponse est que le groupe de Galois associé est le groupe multiplicatif $\mathbb{Q}^\times$ des nombres rationnels non nuls.

6 Coda : un groupe de Galois «cosmique» ?

Depuis quelque temps, les idées galoisiennes ont fait irruption en physique quantique, plus précisément en théorie perturbative des champs quantiques.

À partir des travaux de Feynman et Schwinger, les physiciens ont mis au point des techniques sophistiquées pour éliminer les quantités infinies qui se présentent systématiquement, sous forme d'intégrales divergentes, dans la théorie. La plus simple et la plus utilisée de ces techniques est la renormalisation par régularisation dimensionnelle : on fait fluctuer la dimension de l'espace-temps en lui faisant prendre des valeurs complexes voisines de 4, et on développe les intégrales obtenues en séries indexées par des diagrammes de Feynman de complexité croissante. L'élimination des termes «divergents» de la série se fait suivant de subtiles règles combinatoires qui garantissent la cohérence du procédé.

La «mœlle» mathématique de cette technique a récemment été extraite par Connes et Kreimer, qui ont associé à toute théorie quantique des champs un certain groupe de symétries infini (mais résoluble) directement construit en termes de diagrammes de Feynman. En effectuant une «montée vers l'absolu», ils obtiennent, dans la situation universelle, un groupe de Galois absolu - le groupe de Galois «cosmique» (Cartier) - qui agit sur les constantes de toutes les théories quantiques des champs à la fois.

Ce groupe, d'une ubiquité stupéfiante, incarne à lui seul les divers avatars galoisiens évoqués ci-dessus :
- il s'interprète comme groupe de Galois différentiel
- il apparaît comme groupe de Galois motivique
- il est sensé être le groupe de Galois de certaines intégrales de Feynman[15]
- c'est une variante algébro-géométrique du groupe GT de Drinfeld.

En conclusion, on peut dire qu'en théorie quantique des champs, les divergences, loin d'être des nuisances, donnent naissance à des «ambiguïtés galoisiennes» formant le groupe de symétrie d'une riche structure qui apparaît dans des domaines mathématiques très éloignés les uns des autres.

****

Bibliographie

[1] - N. Abel, «Sur la résolution algébrique des équations», Oeuvres t. II.

[2] -Y. André, Une introduction aux motifs, Panoramas et Synthèses 17, SMF, 2004.

[3] - G. Bachelard, Le rationalisme appliqué, P. U. F. 1949.

[4] - P. Cartier, «La folle journée, de Grothendieck à Connes et Kontsevich», Festschrift des 40 ans de l'IHES.

[5] - A. Connes, «La pensée d'Evariste Galois et le formalisme moderne» (en pdf)

[6] - G. Deleuze, La différence et la répétition,

[7] - R. et A. Douady, Algèbre et théories galoisiennes II, Cedic, 1979

[8] - E. Galois, Oeuvres mathématiques, suivies d'une notice de G. Verriest, Gauthiers-Villars, 1951

[9] - A. Grothendieck, Esquisse d'un programme.

[10] - A. Lautman, Essai sur les notions de structure et d'existence en mathématiques. Réédition Vrin 2006.

[11] - G. Mazzola, «Towards a Galois Theory of Concepts». In : Mazzola G., Th. Noll and E.-L. Puebla (eds.) : Perspectives in Mathematical and Computational Music Theory. EpOs Osnabrück, 2004 (en ligne en format html)

[15] nombres présumés transcendants qui généralisent les valeurs aux entiers de la fonction zêta de Riemann.

[12] - M. van der Put, M. Singer, Galois theory of linear differential equations, Springer Grundlehren der Math. Wiss. 328, 2003

[13] - I. Stewart, Galois theory, Chapman and Hall, 2. ed., 1989

[14] - J. Vuillemin, Philosophie de l'algèbre.