arXiv:1207.3381v1 [math.HO] 14 Jul 2012

Idées galoisiennes

Yves André

0.1. On célèbre cette année le bicentenaire d'Évariste Galois, né le 25 octobre 1811.

Galois est à l'origine de la notion de groupe, cette notion fondamentale qui allait, sous divers avatars, envahir toutes les mathématiques, ainsi qu'une bonne part de la physique et même de la chimie. Dans ses Récoltes et Semailles, A. Grothendieck n'hésite pas à parler de l'invention du zéro et de l'idée de groupe et comme des deux plus grandes innovations mathématiques de tous les temps.

Galois est aussi le premier à avoir formulé le principe de correspondance entre symétries et invariants, qui s'avérera fécond, comme il semble l'avoir lui-même pressenti, bien au-delà du contexte originel de la théorie des équations algébriques.

Ces idées semées, qui en germant ont révolutionné les mathématiques, ont été consignées sur quelques dizaines de feuillets par un jeune homme qui mourut dans sa vingtième année. La veille du duel fatal, il écrivit une splendide lettre-testament, qui débute ainsi :

> 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 dans quels cas les équations étaient résolubles par des radicaux : ce qui m'a donné occasion d'approfondir cette théorie, et de décrire toutes les transformations possibles sur une équation lors même qu'elle n'est pas soluble par radicaux.

C'est dans cette lettre qu'il appelle « théorie de l'ambiguité » le corpus d'idées élaboré par lui pour élucider la théorie des équations algébriques.

0.2. Nous proposons un libre parcours autour de l'héritage de ces idées.

Les domaines les plus classiques d'application de la « théorie de l'ambiguité » concernent les *nombres algébriques* et les *fonctions algébriques*. Nous les survolerons, avant d'aborder ceux des *fonctions transcendantes* et des *nombres transcendants* qui semblent avoir aussi été envisagés par Galois, comme en témoigne la fin de sa lettre :

> 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.

1. Nombres algébriques et groupes de Galois

1.1. Dans la première encyclopédie mathématique de la renaissance [1], l'auteur-compilateur L. Pacioli compare l'impossibilité de résoudre les équations de degré 3 à l'impossibilité de la quadrature du cercle. Pourtant, une vingtaine d'années plus tard, son collègue S. Del Ferro trouvait la formule par radicaux. On connaît la saga de secrets, querelles et trahisons qui s'ensuivit. A la fin XVIe, Bombelli était en mesure de donner un exposé complet de la résolution par radicaux des équations de degré au plus 4, y compris une discussion des ambiguités et des nombres imaginaires comme $\sqrt{-1}$ qui interviennent dans les formules.

La résolution par radicaux des équations d'ordre au moins 5 a résisté... jusqu'à ce qu'Abel en démontre l'impossibilité en général, et que Galois fasse toute la lumière sur cette question [2].

Les progrès sont venus d'une réflexion de plus en plus poussée autour des symétries entre racines d'un polynôme (Viète, van der Monde, Leibniz, Lagrange, Cauchy, Abel) qui culmine dans la théorie de Galois.

1.2. Avec Galois, les ambiguités ne constituent plus une nuisance, elles constituent un groupe !

Soit α un *nombre algébrique*, racine d'un polynôme $x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ à coefficients rationnels, de degré n minimal. Factorisons-le en $(x-\alpha_1)\cdots(x-\alpha_n)$, où les α_i (les autres racines) sont les *conjugués* de $\alpha=\alpha_1$.

Les α_i engendrent un « corps de nombres », et le *groupe de Galois* associé à α est le groupe d'automorphismes de ce corps (c'est-à-dire le groupe des permutations des α_i qui respectent l'addition et la multiplication) [3].

Le point de vue de Galois lui-même était sensiblement différent (un siècle de réélaborations séparent ces points de vue [4]). Il est bien rendu par cette analyse de G. Châtelet :

> La théorie de Galois constitute probablement un des plus beaux exemples du principe de dissymétrie créatrice en mathématiques. [...] Ces racines passeront dans l'existence concrète dans le domaine $D(\alpha_1,\cdots,\alpha_n)$ lorsque je ne serai pas seulement capable d'écrire un signe « formel » mais capable aussi d'exhiber un procédé de discernement entre ces racines. Ce procès de discernement est bien une cassure de la symétrie du groupe des racines. Discerner plus, c'est se montrer capable d'exhiber certaines « grandeurs tests », non rationnelles, et invariantes par un groupe de symétrie plus restreint. Les racines vont s'individuer au fur et à mesure de la précision des « expressions algébriques test » construites par certaines adjonctions aux rationnels. [...]
>
> *Rendre raison* de l'existence conscrète de ces racines est équivalent à la *présentation du groupe de symétrie* de l'équation comme une chaîne

1. Summa de arithmetica, geometria, de proportioni et de proportionalita (Venise, 1494).

2. Galois avait démontré, à dix-sept ans, cette impossibilité ; avant de découvrir qu'Abel venait de publier le résultat (Beweis der Unmglichkeit der algebraischen Auflsbarkeit der allgemeinen Gleichungen, J. de Crelle, 1826, 65-84), et écrivit une courte note exposant son approche. Abel mourut de tuberculose, deux ans avant Galois, à l'âge de 26 ans.

3. Galois avait aussi imaginé de prendre pour a_i des entiers modulo un nombre premier, et avait construit ainsi les « corps finis » (imaginaires de Galois).

4. on renvoie à la thèse de C. Ehrhardt (Paris, 2007) pour une analyse détaillée de ces réélaborations. La notion même de groupe a elle aussi subi de nombreuses vicissitudes, la condition d'associativité n'ayant été clairement dégagée qu'au début du XXème siècle.

> descendante construite de telle manière que l'écart entre deux de ses maillons soit le manque de discernement relatif entre les racines lorsque je calcule dans le domaine associé. [5]

La correspondance de Galois met en regard extensions de corps obtenues par adjonction de racines, et certains groupes de symétrie de ces racines. Elle remplace, si on veut, l'imbrication de deux opérations commutatives (l'addition et la multiplication) dans des extensions, par une seule opération non commutative (la composition des permutations).

1.3. Lorsque l'on adjoint de plus en plus de nombres algébriques, la correspondance de Galois donne lieu à un système « projectif » de groupes finis s'envoyant les uns sur les autres, et dont la « limite » $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, appelée *groupe de Galois absolu de* $\mathbb{Q}$, n'est autre que le groupe infini [6] des automorphismes du corps $\bar{\mathbb{Q}}$ des nombres (complexes) algébriques.

C'est cette démarche qu'A. Lautman appelle la « montée vers l'absolu » [7] : un seul objet mathématique, $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, code les propriétés de toutes les équations algébriques à coefficients rationnels à la fois. Ce groupe de Galois absolu, objet central de la théorie des nombres, reste largement un mystère après un siècle et demi d'efforts intenses pour en comprendre la structure.

Ses quotients commutatifs sont décrits par la cyclotomie, qui remonte à Gauss. Pour aller au-delà, on peut faire agir linéairement ce groupe, tâcher d'étudier ses représentations linéaires [8]. La théorie des représentations linéaires est d'ailleurs née, entre les mains de Frobenius, à propos d'un problème que lui avait soumis Dedekind en 1896 concernant des groupes de Galois de corps de nombres. Bien des conquêtes récentes de la théorie des nombres (et notamment la preuve par A. Wiles du « théorème » de Fermat) reposent sur l'étude des déformations de ces objets « souples » que sont les représentations galoisiennes.

Une autre façon de « comprendre » $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ est d'en décrire les quotients finis : le fameux problème de Galois inverse, toujours ouvert, consiste à savoir si tout groupe fini est groupe de Galois d'un corps de nombres.

Une troisième façon, apparemment beaucoup plus modeste, consisterait à distinguer, nommer ou construire des éléments particuliers. Or il faut avouer qu'après l'identité et la conjugaison complexe, on ne sait pas décrire un troisième élément, même si la théorie des « dessins d'enfants » de Grothendieck vise une compréhension graphique des groupes de Galois et irait dans ce sens [9].

2. Fonctions algébriques et groupes de Galois

2.1. Galois était bien conscient que sa « théorie de l'amguïté s'appliquait aussi bien aux fonctions algébriques qu'aux nombres algébriques. Cela ressort de son

5. G. Châtelet, La physique mathématique comme projet, L'enchantement du virtuel, p. 115-117, Presses de l'ENS

6. naturellement muni d'une structure de groupe topologique compact.

7. Essai sur les notions de structure et d'existence en mathématiques. Réédition Vrin 2006.

8. comme l'a montré bien plus tard Grothendieck, la cohomologie étale des variétés algébriques fournit de telles représentations galoisiennes, tandis que le programme de Langlands relie certaines représentations galoisiennes à certains objets de l'analyse spectrale : les représentations automorphes.

9. on renvoie à l'exposé de A. Zvonkine aux Journées mathématiques X-UPS 2004 pour une introduction à cette théorie.

calcul du groupe de Galois des points de division d'une courbe elliptique, et de ses mystérieux travaux sur les intégrales abéliennes [10], qu'il introduit ainsi dans sa lettre :

> On traite à la fois toutes les intégrales dont la différentielle est une fonction de la variable et d'une même fonction irrationnelle de la variable, que cette irrationnelle soit ou ne soit pas un radical, qu'elle s'exprime ou ne s'exprime pas par des radicaux.

Mais c'est F. Klein [11] qui en croisant la théorie de l'ambiguité et celle des surfaces à plusieurs feuillets de Riemann, a inauguré une tradition qui, via la théorie de l'uniformisation et du groupe fondamental de Poincaré, aboutira à la fusion qu'A. Grothendieck effectuera vers 1960 entre théorie de Galois et théorie des revêtements, pierre de touche de la fusion plus générale qu'il a mise en oeuvre entre géométrie algébrique et théorie des nombres.

2.2. En langage moderne, voici de quoi il s'agit. Une fonction algébrique est racine d'un polynôme à coefficients fonctions rationnelles d'une variable auxiliaire t. Les solutions complexes de l'équation forment une surface de Riemann, qui est un revêtement du plan complexe (muni de la coordonnée complexe t).

Plus généralement, on a la notion de revêtement fini normal $Y \to X$ de surfaces de Riemann (qu'on suppose non ramifié pour simplifier) . Dans ce contexte géométrique, ce qui remplace les racines d'une équation, ce sont les points $\{y_1, \ldots, y_n\}$ de Y qui s'envoient sur un point x arbitraire fixé de X. Le groupe de Galois $\mathrm{Gal}(Y/X)$ est un sous-groupe du groupe des permutations de $\{y_1, \ldots, y_n\}$ [12]. 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 » 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 déformation (homotopie) près. C'est ainsi que s'obtiennent les éléments de $\mathrm{Gal}(Y/X)$.

2.3. Dans ce contexte, on peut encore effectuer une « montée vers l'absolu ». Ce qui correspond au corps $\overline{\mathbb{Q}}$ est maintenant le *revêtement universel* de X (pointé en x), et son groupe d'automorphismes n'est autre que le *groupe fondamental* de Poincaré $\pi_1(X, x)$: 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 $\pi_1(X, x)$ par la limite projective $\hat{\pi}_1(X, x)$ des groupes $\mathrm{Gal}(Y/X)$, lorsque le revêtement Y/X grossit. Dand le point de vue catégorique de Grothendieck, $\hat{\pi}_1(X, x)$ s'interprète comme groupe des automorphismes du foncteur fibre en x

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

10. on renvoie à l'exposé de P. Popescu dans ce volume pour une introduction aux intégrales abéliennes et une discussion des ambiguïtés qu'elles charrient. On ignore comment Galois avait pu obtenir les résultats sur les intégrales abéliennes exposés dans sa lettre, qui préfigurent ceux de B. Riemann un quart de siècle plus tard.

11. 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.

12. 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.

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.

2.4. Une approche indirecte fascinante de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ 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. 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, $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ opère sur les revêtements finis de X, donc sur $\hat{\pi}_1(X)$, et cette opération est *fidèle : le groupe de Galois absolu arithmétique* $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ *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 $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ 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 $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ sur ces dessins [13]. .

Pour ce faire, il faut disposer au préalable d'un codage combinatoire des éléments de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ lui-même. C'est ce qui a été obtenu par V. Drinfeld autour de 1990 (en découvrant un lien insoupçonné entre $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ et groupes quantiques) : il plonge $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ dans un groupe de nature combinatoire GT - le groupe de Grothendieck-Teichmüller, défini par générateurs (topologiques) 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 $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ (on le soupçonne).

3. Fonctions transcendantes et groupes de Galois

3.1. J. Liouville, qui a exhumé, étudié et fait connaître les papiers de Galois, est aussi le premier à avoir poursuivi les intuitions galoisiennes vers les fonctions transcendantes : au lieu de se demander quand une équation algébrique est résoluble par radicaux, il se demande quand une équation différentielle linéaire est résoluble par quadratures (intégrales et exponentielles d'intégrales). Mais c'est E. Picard qui, en 1883, sous doute inspiré par des idées de S. Lie, a introduit dans ce contexte le *groupe de Galois différentiel* : c'est le groupe formé des automorphismes commutant à la dérivation, parmi tous les automorphismes de l'extension du corps de fonctions de base obtenue en adjoignant les solutions de l'équation différentielle et leurs dérivées.

Du fait que les solutions d'une équation 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 algébrique (groupe de matrices). C'est d'ailleurs, via les travaux d'E. Kolchin, l'une des sources historiques de la théorie des groupes algébriques.

13. sur tout cela, on pourra consulter R. Douady, A. Douady, Algèbgre et théories galoisiennes, Cassini 2005.

On dispose d'une correspondance de Galois différentielle mettant en regard extensions de corps différentiels obtenues par adjonction de solutions, et certains groupes de transformations linéaires des espaces de solutions.

3.2. La théorie a mûri lentement. 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 que *dans ce cadre analytique local, il y a trois types, et trois seulement, d'ambiguïtés galoisiennes* (qui sont des éléments du groupe de Galois différentiel) :

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 [14]. Considérons par exemple 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 $\mathbb{C}^\times$ engendré par ces recalibrages.

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

$$xy' + y = x$$

au voisinage de la singularité 0. L. Euler l'avait déjà rencontrée dans son fameux mémoire sur les séries divergentes [15] : c'est l'équation satisfaite par la série formelle $\hat{y} = \sum (-1)^n n! x^{n+1}$, qui diverge en tout point $x \neq 0$. Euler utilisait d'ailleurs cette

14. cette notion est due à Riemann, qui l'avait mise en évidence dans le contexte des équations différentielles hypergéométriques. Mais Galois a probablement pu avoir l'intuition de cette ambiguïté, notamment à propos des périodes d'intégrales abéliennes dépendant d'un paramètre, comme il ressort du passage de sa lettre où il parle des ≪ périodes relatives à une même *révolution* ≫.

15. De seriebus divergentibus, publié en 1760 à l'Académie de St. Petersbourg. Voir aussi http ://www.maa.org/news/howeulerdidit.html, juin 2006.

Euler n'hésitait pas à braver la divergence en écrivant des formules comme :

$$1 + 2 + 4 + 8 + 16 + \cdots = -1, \quad 1 + 2 + 3 + 4 + 5 + \cdots = -1/12,$$

ou en attribuant une valeur précise à la somme $1 - 1! + 2! - 3! + 4! - 5! + \cdots$ (qu'il évalue numériquement, de six manières différentes). Ces formules ≪ scandaleuses ≫, sévèrement critiquées aux temps de la quête de la rigueur en Analyse, furent pleinement éclaircies et justifiées ultérieurement (à l'abus de notation près qu'elles commettent). Par exemple, la première formule n'est autre que l'évaluation en $x = 1$ de la série de puissances $1+2x+4x^2+\cdots = 1/(1-2x)$; stricto sensu, c'est la valeur en 1 du prolongement analytique de la fonction $1/(1-2x)$ de la variable complexe x définie par cette série. La seconde formule est nettement plus profonde et attendit 120 ans sa justification : elle exprime la valeur en $s = -1$ du prolongement analytique de la fonction $\zeta(s) = \sum_1^\infty n^{-s} = \prod_p \frac{1}{1-p^{-s}}$ de Riemann. Dans son article visionnaire de 1859 (Über die Anzahl der Primzahlen unter einer gegebenen Grösse, Monatsberichte der Berliner Akademie), Riemann prouve, pour tout nombre complexe s, la symétrie suggérée par Euler entre $\zeta(s)$ et $\zeta(1-s)$, et il explique le lien entre la distribution des nombres premiers et la position des zéros de ζ.

équation pour « sommer » cette série divergente, en identifiant la « somme » à la « vraie » solution $y = \int_0^\infty \frac{e^{-t/x}}{1+t} dt$, dont $\hat{y}$ est le développement asymptotique (Euler écrit « evolutio ») dans le plan privé de la demi-droite réelle négative.

Mais dans un autre secteur, le développement asymptotique de y peut changer. Ces ambiguités liées au choix des secteurs donnent lieu à des ambiguïtés galoisiennes, les ambiguïtés de Stokes [16].

De manière générale, le groupe de Galois différentiel est engendré (au sens des groupes algébriques) par ces trois types de matrices [17].

4. Nombres transcendants et groupes de Galois

4.1. Peut-on attacher à un nombre transcendant donné des conjugués, et un groupe de Galois qui les permute, comme dans le cas des nombres algébriques ?

Commençons par considérer le cas de π, dont F. von Lindemann a montré en 1882 qu'il est transcendant, c'est-à-dire ne satisfait aucune équation polynômiale à coefficients rationnels (démontrant ipso facto l'impossibilité de la quadrature du cercle). Mais, comme Euler l'avait observé, π satisfait une telle équation mais de degré infini (où une série de puissances remplace un polynôme) [18]

$$\prod_{n \in \mathbf{Z} \setminus 0} (1 - \frac{x}{n\pi}) = \frac{\sin x}{x} = 1 - \frac{x^2}{6} + \frac{x^4}{120} + \cdots \in \mathbb{Q}[[x]].$$

Ce qui suggère de considérer les multiples de π comme ses conjugués. En fait, si l'on veut qu'un groupe permute transitivement les conjugués, on est amené à prendre pour conjugués de π tous ses multiples rationnels non nuls - le groupe de Galois serait alors le groupe multiplicatif $\mathbb{Q}^\times$.

Peut-on généraliser cette approche ? Un vieux résultat peu connu de A. Hurwitz assure que tout nombre complexe est racine d'une série de puissances à coefficients rationnels qui converge partout. Peut-on alors considérer ses autres racines comme des conjugués ?

Hélas, cette approche est un cul-de-sac [19], car il existe une infinité indénombrable de telles séries, et aucun moyen d'en choisir une canonique en général.

4.2. Nous allons voir qu'on peut tout de même s'attendre à pouvoir définir des conjugués et un groupe de Galois pour une vaste classe de nombres (en général transcendants), incluant la plupart des constantes mathématiques classiques. Ces

16. G. Stokes les a mises en évidence, au milieu du XIXème siècle, sur l'équation différentielle d'Airy $y'' = xy$, après avoir remarqué qu'il était bien plus efficace de calculer les zéros de la solution d'Airy en se servant du développement asymptotique divergent, à l'infini, plutôt qu'avec le développement de Taylor convergent à l'origine comme faisait G. Airy.

17. voir par exemple M. van der Put, M. Singer, Galois theory of linear differential equations, Springer Grundlehren der Math. Wiss. 328, 2003.

18. formellement, l'équation d'Euler $\sum n^{-2} = \pi^2/6$ résulte de l'extension à cette série de la formule de Newton pour la somme des carrés des racines en terme des coefficients d'une équation polynômiale. Galois avait d'ailleurs fait la remarque que ce type de formules ne dépendait pas du nombre de racines, ayant sans doute en vue la possibilité de faire tendre ce nombre vers l'infini...

19. sauf à imposer de fortes contraintes arithmétiques sur les dénominateurs des coefficients. Cette possibilité est d'ailleurs loin d'avoir été explorée systématiquement.

nombres sont des intégrales, les *périodes*[20] $\int_\Delta \omega$, ou plus généralement les *périodes-exponentielles* $\int_\Delta e^f\omega$ (où à la fois l'intégrant ω et le domaine Δ sont définis par des expressions algébriques d'une ou plusieurs variables à coefficients des nombres algébriques : par exemple $\pi = \int_0^\infty \frac{2dt}{1+t^2}$.

4.3. D'où cette idée vient-elle ?

Elle vient d'une théorie initiée par A. Grothendieck (le mathématicien qui a révolutionné la géométrie algébrique dans les années 60), la théorie des *motifs*, qui vise à unifier les aspects combinatoires, topologiques et arithmétiques de la géométrie algébrique. Ces motifs jouent un peu le rôle de "particules élémentaires" algébro-géométriques, susceptibles de décomposition et recombinaison suivant des règles relevant de la théorie des représentations des groupes. Les groupes en question, baptisés *groupes de Galois motiviques*, représentent une formidable *généralisation des groupes de Galois usuels aux systèmes de plusieurs polynômes à plusieurs variables*. Ce ne sont plus des groupes finis, mais des groupes algébriques (comme dans le cas des groupes de Galois différentiels).

En tant que groupes de symétrie de motifs (attachés à de tels systèmes à coefficients rationnels), ils devraient aussi agir sur leurs périodes (et même sur les avatars exponentiels), ce qui permettrait de définir les conjugués d'une période comme ses images sous les éléments du groupe de Galois motivique. Toutefois, comme il peut arriver qu'un nombre complexe s'exprime de plusieurs manières différentes comme période, la cohérence d'une telle action requiert de postuler que toute relation entre périodes provient d'une relation entre motifs, ce qui est la *conjecture des périodes de Grothendieck*. On s'attend en particulier à ce que le nombre maximal de périodes d'un motif sur $\mathbb{Q}$ qui sont algébriquement indépendantes sur $\mathbb{Q}$ soit égal à la dimension du groupe de Galois motivique associé[21].

4.4. Par exemple, $2\pi\sqrt{-1} = \int dt/t$ est la période attachée au motif de la droite privée de l'origine, dont le groupe de Galois motivique est le groupe multiplicatif $\mathbb{Q}^\times$, les conjugués de $2\pi\sqrt{-1}$ étant ses multiples rationnels non nuls. Ici, la cohérence postulée par la conjecture de Grothendieck n'est autre que la transcendance de π.

Citons aussi à titre d'exemples de périodes, très étudiés actuellement mais qui remontent en fait à Euler, les nombres polyzeta

$$\sum_{n_1>\cdots>n_k\geq 1} n_1^{-s_1}\dots n_k^{-s_k} \;=$$

$$\int_{1\geq t_1\geq\cdots\geq t_s\geq 0} \frac{dt_1}{\epsilon_1 - t_1}\cdots\frac{dt_s}{\epsilon_s - t_s} \quad (s_i\in\mathbb{Z}_{\geq 1},\ ; s=\sum s_i,\ \epsilon_j = 0 \text{ ou } 1).$$

Depuis Euler, on a découvert tout un écheveau de relations algébriques les liant les uns aux autres, et on a vérifié que toutes ces relations sont bien d'origine motivique. La théorie motivique sous-jacente aux polyzeta est maintenant bien comprise (grâce surtout aux travaux d'A. Goncharov puis de F. Brown). C'est d'ailleurs le point de vue motivique qui fournit la meilleure majoration d_s - la meilleure connue et

20. le nom vient de ce que, dans le cas particulier des courbes algébriques (définies sur un corps de nombres), ce sont les périodes d'intégrales abéliennes, que considérait Galois dans le passage évoqué plus haut où il parle de ≪ révolution ≫, et qui apparaissent comme périodes (au sens usuel) des fonctions abéliennes correspondantes.

21. sur tout cela, on peut consulter l'Introduction aux Motifs de l'auteur, Panoramas et Synthèses 17, SMF 2004.

conjecturalement la meilleure possible - pour la dimension du $\mathbb{Q}$-espace vectoriel engendré par les polyzeta avec s fixé : une récurrence à la Fibonacci $d_s = d_{s-2} + d_{s-3}$.

4.5. Fort heureusement, M. Kontsevich a trouvé une formulation élémentaire, particulièrement frappante, de la conjecture des périodes de Grothendieck, qui ne fait pas appel aux motifs. La voici [22].

Les deux règles fondamentales du calcul intégral que sont la formule de Stokes et le changement (algébrique) de variables

$$\int_\Delta d\omega = \int_{\partial\Delta} \omega, \qquad \int_\Delta f^*\omega = \int_{f_*\Delta} \omega,$$

fournissent immédiatement des relations (polynômiales à coefficients rationnels) entre périodes (ou périodes-exponentielles). La conjecture prédit que, réciproquement, toute relation (polynômiale à coefficients rationnels) entre périodes proviendrait de ces deux règles.

Par exemple, l'identité d'Euler $\zeta(2) = \pi^2/6$ peut être comprise comme l'identité de périodes $\int_0^1 \int_0^1 \frac{2dxdy}{(1-xy)\sqrt{xy}} = (\int_0^\infty \frac{2dt}{1+t^2})^2$ (par développement en série géométrique de $1/1-xy$ et intégration terme à terme, le premier membre s'identifie à $6\zeta(2)$). E. Calabi a trouvé comment établir cette identité par changement de variables algébrique idoine : en posant $x = u^2\frac{1+v^2}{1+u^2}$, $y = v^2\frac{1+u^2}{1+v^2}$, de jacobien $|\frac{d(x,y)}{d(u,v)}| = \frac{4uv(1-u^2v^2)}{(1+u^2)(1+v^2)} = \frac{4(1-xy)\sqrt{xy}}{(1+u^2)(1+v^2)}$, on obtient $\int_0^1 \int_0^1 \frac{2dxdy}{(1-xy)\sqrt{xy}} = \int\int_{u,v\geq 0, uv\leq 1} \frac{8dudv}{(1+u^2)(1+v^2)}$, qu'on identifie à $(\int_0^\infty \frac{2dt}{1+t^2})^2$ en utilisant l'involution $(u, v \mapsto u^{-1}, v^{-1})$ [23].

4.6. En résumé, on arrive à cette idée spéculative générale, tout à fait dans l'esprit de la lettre-testament de Galois, que *l'arithmétique de cette vaste classe de nombres - les périodes-exponentielles - devrait être dictée par les règles élémentaires du calcul intégral (et s'il en est ainsi, se décrire en termes de groupes « galoisiens »).*

On peut aller un peu plus loin, comme l'a montré tout récemment J. Ayoub, en ne retenant que la règle de Stokes : la règle du changement de variable en découle.

Avec d'expliquer pourquoi, voici la formulation qu'Ayoub donne de la conjecture des périodes. Soit $\mathcal{A}$ l'algèbre des fonctions d'un nombre quelconque de variables complexes z_i, qui sont holomorphes dans le polydisque $z_i \leq 1$, et algébriques sur $\mathbb{Q}(z_1, \ldots, z_i, \ldots)$. On a une forme linéaire $\mathcal{A} \xrightarrow{\int_\square} \mathbb{C}$ donnée par l'intégrale sur l'hypercube réel $z_i \in [0,1]$, et il s'agit de décrire son noyau.

Pour tout indice i et toute fonction $g_i \in \mathcal{A}$, la fonction $h_i = \frac{\partial g_i}{\partial z_i} - g_{i|z_i=1} + g_{i|z_i=0}$ est dans le noyau de $\int_\square$. La conjecture prédit que, réciproquement, tout élément du noyau de $\int_\square$ serait combinaison linéaire de telles h_i.

Par exemple, partant de $h(z_1) \in \mathcal{A}$ et d'une fonction $f(z_1)$ algébrique qui envoie le dique unité (*resp.* l'intervalle $[0,1]$) dans lui-même en fixant 0 et 1, la formule de changement de variable montre que $f'(z_1)h(f(z_1)) - h(z_1)$ est dans le noyau de $\int_\square$.

---

22. voir aussi M. Kontsevich, D. Zagier : Periods. Mathematics unlimited—2001 and beyond, 771–808, Springer.

23. C. Viola vient de me communiquer une variante encore plus simple, consistant à identifier $\zeta(2)$ à $\int_0^1 \int_0^1 \frac{dxdy}{(1-xy}$, et poser $x = u - v, y = u + v$, ce qui donne $\zeta(2)/4 = \int_0^{1/2} du \int_0^u \frac{dv}{1-u^2+v^2} + \int_{1/2}^1 du \int_0^{1-u} \frac{dv}{1-u^2+v^2}$, qu'on évalue par des moyens élémentaires à $\pi^2/24$.

Comme l'a observé Ayoub, on peut, quitte à ajouter une variable, écrire $f'(z_1)h(z_1) - h'(z_1)$ sous la forme prédite par la conjecture : poser $f_1 = f(z_1) - z_1$, $f_2 = -z_2 f'(z_1) + z_2 - 1$, et $g_i = f_i \cdot h(z_2 f(z_1) + (1 - z_2)z_1)$ pour $i = 1, 2$.

5. Coda : un groupe de Galois « cosmique » ?

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

La divergence, plus importune encore en physique qu'en mathématique, infeste la physique des champs quantiques. À partir des travaux de R. Feynman et J. Schwinger, les physiciens ont dû bâtir un arsenal de techniques, bien plus élaborées que celles de Euler, pour la dépasser. Le procédé le plus simple et le plus utilisé 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.

En jonglant avec des intégrales divergentes, donc dépourvues de sens physique (et même mathématique, *a priori*), la renormalisation aboutit à des quantités finies, en accord remarquable avec l'expérience de surcroît. Elle réussit le tour de force d'*extraire, systématiquement, du (dé)fini de l'in(dé)fini.*

La « mœlle » mathématique de ce procédé a récemment été extraite par A. Connes et D. Kreimer, qui ont associé aux théories quantiques des champs des groupes de symétries infinis directement construits en termes de diagrammes de Feynman. En effectuant une « montée vers l'absolu », ils obtiennent un groupe de Galois absolu - le groupe de Galois « cosmique » prédit par P. Cartier [24] - qui agit sur les « constantes » de toutes les théories quantiques des champs.

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 est très proche du groupe de Galois motivique attaché aux nombres polyzêtas (nombres qu'on retrouve souvent en calculant des intégrales de Feynman).
- c'est une variante algébro-géométrique du groupe GT de Drinfeld.

C'est ainsi qu'en théorie quantique des champs, les divergences, loin d'être des nuisances, donnent naissance à des ambiguïtés galoisiennes formant le groupe de symétries d'une riche structure qui apparaît dans des domaines mathématiques très éloignés les uns des autres.

24. « La folle journée, de Grothendieck à Connes et Kontsevich », Festschrift des 40 ans de l'IHES.