L'influence de Galois

par Jean DIEUDONNÉ

Les travaux de Galois en Algèbre mettent le point final à la solution du problème de la résolution "par radicaux" des équations algébriques, abordé avant lui sous divers angles par Lagrange, Vandermonde, Gauss, Ruffini et Abel. C'est de l'étude de ce problème que sont issues les notions modernes de groupe et de corps, ainsi que ce qu'on appelle la "théorie de Galois" qui relie ces deux notions.

On sait que les mémoires de Galois ne furent publiés qu'en 1846 par Liouville. Répondant complètement à une question qui avait arrêté les mathématiciens pendant 200 ans, il semble qu'ils auraient dû aussitôt susciter de nouvelles recherches développant les idées qu'ils contenaient. S'il n'en a rien été, c'est sans doute que le style de Galois, étonnamment "moderne" par l'absence presque complète de calculs explicites et qui nous paraît maintenant d'une parfaite limpidité dans sa concision, déroutait ses contemporains qui le considéraient comme trop "abstrait". Toujours est-il que jusqu'en 1860 les rares publications sur les groupes se bornent à exposer les résultats de Cauchy et de Galois sans rien y ajouter de substantiel ; c'est seulement ensuite que la situation s'est modifiée et que l'influence des travaux de Galois n'a cessé de s'amplifier pendant toute la fin de XIX^{e} siècle. Nous nous bornerons à indiquer les directions les plus élémentaires dans lesquelles cette influence s'est fait sentir.

Groupes. — Le concept de groupe de permutations d'un nombre fini d'objets (sans l'usage du terme "groupe" qui n'est introduit que par Galois) est dû à Cauchy (1813) et dès cette époque il avait démontré quelques théorèmes généraux sur ces groupes et leurs sous-groupes ; il devait seulement y revenir en 1845, introduisant de nouvelles notions, telles que celles de groupe transitif et de groupe primitif (*) ; c'est aussi dans ce travail qu'il prouve que si un nombre premier p divise l'ordre d'un groupe fini G, G contient un élément d'ordre p, première étape vers le théorème de Sylow (**). Mais le progrès décisif, aussi bien pour l'étude "abstraite" des groupes que pour celle de leurs applications, a été l'introduction par Galois de la notion de sous-groupe *distingué* (ou invariant), et celle de groupe simple (***) qui s'en déduit.

Il est immédiat que pour tout groupe fini G, il y a une suite strictement décroissante de sous-groupes

$$(1) \qquad G = G_0 \supset G_1 \supset G_2 \supset \dots \supset G_n = \{e\}$$

où chaque G_{i+1} est distingué dans G_i, et les groupes quotients G_i/G_{i+1} sont tous simples ; en outre, il peut y avoir plusieurs suites de ce type qui sont différentes, mais les groupes simples G_i/G_{i+1} sont toujours les mêmes à l'ordre près (théorème de Jordan-Hölder). Si on veut classifier les groupes finis, il est donc naturel d'essayer de commencer par trouver tous les groupes simples. C'est un problème qui a débuté avec Galois lui-même, et qu'il a fallu exactement 150 ans et une masse colossale de travaux pour résoudre : depuis 1981, on sait décrire explicitement tous les groupes simples (*).

Le théorème de Cauchy rappelé plus haut montre que les seuls groupes simples commutatifs sont les groupes cycliques d'ordre premier. Le groupe simple non commutatif le plus petit fut découvert par Galois, c'est le groupe alterné A_5 des permutations paires de 5 objets, d'ordre 60, et son raisonnement montre que tous les groupes alternés A_n sont simples pour $n>5$. Dans sa recherche des groupes des équations irréductibles de degré premier p, il avait introduit, pour tout $n\geqslant 2$, le groupe projectif unimodulaire que nous notons maintenant $\mathbf{PSL}(n,\mathbf{F}_p)$, quotient par son centre du groupe des matrices carrées d'ordre $n\geqslant 2$ à coefficients dans le corps premier $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ (ou, comme on disait alors, entiers modulo p), et de déterminant 1 (**). Jordan montra que ces groupes sont tous simples ; il obtint aussi plusieurs autres séries de groupes de matrices à coefficients dans $\mathbf{F}_p$, qu'on appelle maintenant "groupes classiques" et dont les plus connus sont les groupes orthogonaux ; puis Dickson, vers 1900, généralisa les résultats de Jordan en y remplaçant $\mathbf{F}_p$ par un corps fini quelconque (***).

Ces groupes "classiques" finis se définissaient curieusement par les mêmes équations que les groupes de Lie simples, dits aussi "classiques", qui sont des groupes de matrices à éléments complexes, en remplaçant les nombres complexes par des éléments d'un corps fini ; et Dickson avait même montré qu'on obtenait encore des groupes simples finis en opérant de même sur deux des 5 groupes de Lie simples "exceptionnels" (ceux de dimension 14 et 78). Cette coïncidence resta inexpliquée jusqu'en 1955, date à laquelle Chevalley étendit à tous les groupes de Lie simples,

(*) Un groupe G de permutations de n objets est dit *primitif* s'il n'est pas possible de partager les n objets en $m>1$ sous-ensembles tels que toute permutation de G transforme chacun de ces sous-ensembles en un autre.

(**) Le théorème de Sylow (1872), qui généralise le résultat de Cauchy, dit que si l'ordre de G est de la forme $p^m r$, où p est premier et ne divise pas r, il y a dans G un sous-groupe d'ordre p^m, et tous ces sous-groupes sont conjugués ; Galois connaissait ce résultat mais n'en a pas laissé de démonstration.

(***) Un groupe est dit *simple* s'il ne contient pas de sous-groupe distingué autre que lui-même et le groupe réduit à l'élément neutre.

(*) Cf. Bulletin de l'A.P.M.E.P. n° 334, p. 459.

(**) Pour $n=2$, ce groupe peut aussi se définir comme celui des transformations homographiques $z \longmapsto (az+b)/(cz+d)$, où a,b,c,d sont des entiers modulo p et $ad-bc=1$.

(***) Un corps fini $\mathbf{F}_q$ a un nombre d'éléments q qui est une puissance p^m d'un nombre premier ; leur découverte est due en substance à Gauss (qui ne publia pas ses résultats) et (indépendamment) à Galois ; on désigne souvent leurs éléments sous le nom d'"imaginaires de Galois".

par un raisonnement général (et non plus en examinant séparément chaque groupe par une méthode *ad hoc*), cette correspondance avec des groupes finis simples. Les séries de groupes simples finis provenant ainsi des groupes de Lie sont maintenant appelés groupes de Chevalley, ou groupes du type de Lie.

Mais dès 1860, E. Mathieu avait découvert 5 groupes simples finis qui n'étaient isomorphes, ni à des groupes alternés, ni à des groupes du type de Lie. Un siècle plus tard, on crut un moment qu'avec ces groupes on avait épuisé la liste de tous les groupes simples ; mais entre 1965 et 1980 on découvrit, par des procédés très variés, 21 autres groupes simples (dont le plus grand est d'ordre $>10^{53}$), ne rentrant dans aucune série, si bien que l'optimisme de 1960 fit place à la crainte qu'il existât peut-être encore bien des groupes simples, peut-être même une infinité. Mais finalement, ce pessimisme s'est trouvé injustifié, et par un travail herculéen, auquel ont contribué plus de 20 mathématiciens, et qui actuellement occupe environ 10000 pages (*), on est arrivé (si aucune erreur n'a été commise) à montrer qu'il n'y a pas d'autre groupe simple fini que ceux des séries connues et les 26 groupes (dits "sporadiques") qui n'y figurent pas.

En vue d'obtenir son critère de résolubilité d'une équation par radicaux, Galois avait d'autre part considéré le cas où, dans la suite (1), les quotients G_i/G_{i+1} sont cycliques d'ordres premiers ; on dit alors que le groupe G est *résoluble*. Jordan (qui doit être considéré comme le continuateur direct de Galois et le "pape" de la théorie des groupes dans le dernier tiers du XIX^e siècle) fit une étude approfondie de ces groupes. Depuis lors, on a surtout étudié le cas des groupes d'ordre une puissance p^k d'un nombre premier, qu'on appelle *p-groupes* ; ils sont toujours résolubles, par exemple en vertu d'un théorème de Burnside d'après lequel tout groupe dont l'ordre ne comporte que 2 facteurs premiers au plus est résoluble.

Bien entendu, tous ces résultats n'ont pu être obtenus que par la création et l'emploi de nombreuses techniques nouvelles, auxquelles on ne pouvait songer au temps de Galois ou de Jordan ; un des résultats les plus profonds et les plus utiles est le théorème de Feit-Thompson, d'après lequel tout groupe d'ordre *impair* est résoluble.

Corps.— La notion de corps n'apparaît pas explicitement dans les mémoires de Galois, car elle suppose l'usage d'un langage "ensembliste" qu'on n'emploie pas encore à cette époque. Mais pour Galois (et déjà avant lui pour Abel), la conception que recouvre ce mot est tout à fait claire : ils parlent d'éléments qui sont "fonctions rationnelles d'un certain nombre de quantités connues". Ils conçoivent clairement aussi ce qu'est un polynôme *irréductible* P : cela signifie pour eux que P ne peut pas s'écrire comme produit P_1P_2 de deux polynômes non constants, dont les coefficients s'expriment rationnellement en fonction des coefficients de P. Enfin, ils savent que si, en outre des coefficients de P, on considère d'autres nombres comme "quantités connues", un polynôme irréductible P peut se décomposer en produit de polynômes dont les coefficients s'expriment rationnellement en fonction des coefficients de P et de ces nouvelles "quantités connues" ; c'est ce que nous appelons maintenant le passage d'un corps à une *extension* de ce corps par adjonction de nouveaux éléments.

Théorie de Galois.— Ce sont là les idées qui sont à la base du théorème de Galois sur la résolubilité des équations par radicaux. A un polynôme P dont les coefficients appartiennent (dans notre langage) à un corps infini K, et irréductible sur K, dont les racines sont $x_1, x_2, \ldots, x_n$, Galois associe d'abord un élément

$$(2) \qquad V = \alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n$$

où les α_j sont dans K, et choisis de sorte que les $n!$ éléments obtenus par toutes les permutations des x_j dans l'expression de V soient tous distincts. Un résultat de Lagrange montre que chaque x_j s'exprime sous la forme

$$(3) \qquad x_j = f_j(V)$$

où f_j est un polynôme à coefficients dans K. Si alors $V_1 = V, V_2, \ldots, V_m$ sont les conjugués de V (racines du polynôme irréductible sur K dont V est une racine), on a $P(f_j(V)) = 0$, donc aussi $P(f_j(V_h)) = 0$ pour $1 \leqslant h \leqslant m$, autrement dit chaque V_h définit une permutation

$$(4) \quad \sigma_h : (f_1(V), \ldots, f_n(V)) \longmapsto (f_1(V_h), \ldots, f_n(V_h))$$

des racines de P ; c'est le groupe formé par *ces* permutations-là qui est le *groupe de Galois* de P (ou de l'équation $P=0$), et on a

$$(5) \quad V_h = \alpha_1\sigma_h(x_1) + \alpha_2\sigma_h(x_2) + \ldots + \alpha_n\sigma_h(x_n) \ .$$

Cette méthode générale conduit à des calculs inextricables lorsqu'on veut déterminer le groupe de Galois d'un polynôme explicitement donné. Un sujet de recherche qui se développa de 1830 à 1880 environ consista à obtenir par des méthodes plus efficaces le groupe de Galois de diverses équations algébriques particulières qui se présentaient en Analyse ou en Géométrie. Galois lui-même (sans publier de démonstration) détermina ainsi le groupe de l'équation modulaire, une des notions importantes de la théorie des fonctions elliptiques, très étudiée à cette époque ; ses travaux furent poursuivis notamment par Kronecker et Klein. Jordan se distingua dans ce domaine, déterminant entre autres des suites de composition (1) pour les groupes de Galois d'équations célèbres, telles que celles qui déterminent les 27 droites d'une surface cubique, ou les 28 bitangentes d'une quartique plane, ou encore les 16 points singuliers d'une surface de Kummer.

Mais à partir de 1855 environ, le point de vue commence à changer avec Kronecker et Dedekind, qui introduisent et manient la notion de corps (*) dans leurs travaux d'Algèbre et de Théorie des nombres. Au lieu de considérer un polynôme P à coefficients dans un corps K et irréductible sur K, on lui associe son *corps des racines* $N = K(x_1, x_2, \ldots, x_n)$, engendré par adjonction à K des racines de P ; cela a l'avantage

(*) Comme dans plusieurs cas analogues, il faut espérer qu'on arrivera à obtenir des démonstrations plus simples.

(*) Kronecker désigne un corps sous le nom de "domaine de rationalité".

de travailler sur un objet plus intrinsèque, car plusieurs polynômes différents peuvent avoir même corps des racines. Ces corps sont appelés *extensions galoisiennes* de K ; ils contiennent les conjugués sur K de chacun de leurs éléments. Avec les notations ci-dessus, $N = K(V)$; N est aussi engendré par chacun des conjugués $V_2, \ldots, V_m$ de V et est de degré m sur K ; en outre l'application $F(V) \longmapsto F(V_h)$ (où F parcourt les polynômes à coefficients dans K) est un *automorphisme* du corps N laissant invariants les éléments de K et se réduisant à la permutation σ_h dans l'ensemble $\{x_1, x_2, \ldots, x_n\}$, de sorte qu'on peut le noter aussi σ_h . Le groupe de Galois de P, formé des σ_h , s'identifie donc au groupe de tous les automorphismes du corps N qui laissent invariants les éléments de K ; on dit donc que c'est le *groupe de Galois de l'extension galoisienne* N de K, et de nouveau on a affaire à une notion intrinsèque, indépendante de la définition de N par un polynôme particulier.

Dans cette optique, le *théorème fondamental* de la théorie de Galois est le suivant : si Γ est le groupe de Galois d'une extension galoisienne N de K, on définit une application *bijective* de l'ensemble des corps L tels que $K \subset L \subset N$ (dits corps intermédiaires entre K et N) et l'ensemble des sous-groupes de Γ en faisant correspondre à tout corps intermédiaire L le groupe de Galois de N sur L.

La fin du XIX^e siècle voit aussi se terminer l'influence directe des idées de Galois, relayées par de nouvelles notions et de nouvelles techniques qu'il ne pouvait prévoir : avec Jordan, Lie et Klein, ce sont les groupes infinis qui entrent en scène ainsi que leurs liaisons avec l'Analyse et la Géométrie, en attendant que l'idée générale de groupe, avec toutes ses variantes (groupes topologiques, groupes de Lie, groupes algébriques, schémas en groupes, groupes formels), n'envahisse toute la mathématique actuelle et la physique théorique, accompagnée des idées fondamentales de représentation linéaire et d'invariant. Aux corps "classiques" (sous-corps de $\mathbf{C}$) que connaissaient Galois et ses successeurs immédiats viennent s'ajouter une foule d'autres (corps de caractéristique quelconque, corps locaux, corps de séries formelles) dont l'étude générale fait apparaître de nouveaux phénomènes comme l'inséparabilité et de nouvelles notions comme celle de dérivation.

Mais on peut dire que la théorie de Galois n'a cessé, de façon indirecte, de fasciner et d'inspirer les mathématiciens : en donnant l'exemple d'une manière canonique d'associer, à des objets mathématiques d'une certaine nature, comme les corps, des objets d'une autre nature, comme les groupes, elle a servi de modèle dans des théories diverses (revêtements, équations différentielles algébriques, Théorie des nombres algébriques), et il n'est peut-être pas exagéré d'y voir le premier exemple de la notion de *foncteur*.