Lettre de Galois
à M. Auguste Chevalier

Évariste Galois

Journal de mathématiques pures et appliquées, vol. XI, November 1846, pp. 408-415

(Insérée en 1832 dans la *Revue encyclopédique*, numéro de septembre, page 568.)[1]

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 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.

On pourra faire avec tout cela trois Mémoires.

Le premier est écrit, et, malgré ce qu'en a dit Poisson, je le maintiens, avec les corrections que j'y ai faites.

Le second contient des applications assez curieuses de la théorie des équations. Voici le résumé des choses les plus importantes :

1°. D'après les propositions II et III du premier Mémoire, on voit une grande différence entre adjoindre à une équation une des racines d'une équation auxiliaire ou les adjoindre toutes.

Dans les deux cas, le groupe de l'équation se partage par l'adjonction en groupes tels, que l'on passe de l'un à l'autre par une même substitution; mais la condition que ces groupes aient les mêmes substitutions n'a lieu certainement que dans le second cas. Cela s'appelle *la décomposition propre*.

En d'autres termes, quand un groupe G en contient un autre H, le groupe G peut se partager en groupes, que l'on obtient chacun en opérant sur les permutations de H une même substitution; en sorte que

$$\mathrm{G} = \mathrm{H} + \mathrm{HS} + \mathrm{HS}' + \ldots.$$

Et aussi il peut se décomposer en groupes qui ont tous les mêmes substitutions, en sorte que

$$\mathrm{G} = \mathrm{H} + \mathrm{TH} + \mathrm{T}'\mathrm{H} + \ldots.$$

Ces deux genres de décompositions ne coïncident pas ordinairement. Quand ils coïncident, la décomposition est dite *propre*.

Il est aisé de voir que, quand le groupe d'une équation n'est susceptible d'aucune décomposition propre, on aura beau transformer cette équation, les groupes des équations transformées auront toujours le même nombre de permutations.

Au contraire, quand le groupe d'une équation est susceptible d'une décomposition propre, en sorte qu'il se partage en M groupes de N permutations, on pourra résoudre l'équation donnée au moyen de deux équations : l'une aura un groupe de M permutations, l'autre un de N permutations.

Lors donc qu'on aura épuisé sur le groupe d'une équation tout ce qu'il y a de décompositions propres possibles sur ce groupe, on arrivera à des groupes qu'on pourra transformer, mais dont les permutations seront toujours en même nombre.

Si ces groupes ont chacun un nombre premier de permutations, l'équation sera soluble par radicaux; sinon, non.

Le plus petit nombre de permutations que puisse avoir un groupe indécomposable, quand ce nombre n'est pas premier, est 5.4.3.

2°. Les décompositions les plus simples sont celles qui ont lieu par la méthode de M. Gauss.

Comme ces décompositions sont évidentes, même dans la forme actuelle du groupe de l'équation, il est inutile de s'arrêter longtemps sur cet objet.

Quelles décompositions sont praticables sur une équation qui ne se simplifie pas par la méthode de M. Gauss?

J'ai appelé *primitives* les équations qui ne peuvent se simplifier par la méthode de M. Gauss; non que ces équations soient réellement indécomposables, puisqu'elles peuvent même se résoudre par radicaux.

Comme lemme à la théorie des équations primitives solubles par radicaux, j'ai mis en juin 1830, dans le *Bulletin de Férussac*, une analyse sur les imaginaires de la théorie des nombres.

On trouvera ci-jointe[2] la démonstration des théorèmes suivants :

1°. Pour qu'une équation primitive soit soluble par radicaux, elle doit être du degré p^ν, p étant premier.

2°. Toutes les permutations d'une pareille équation sont de la forme

$$x_{k,\,l,\,m\ldots} \mid x_{ak+bl+cm+\ldots+h,\ a'k+b'l+c'm+\ldots+h',\ a''k+\ldots,\ \ldots},$$

$k,\ l,\ m, \ldots$ étant ν indices, qui, prenant chacun p valeurs, indiquent toutes les racines. Les indices sont pris suivant le module p; c'est-à-dire que la racine sera la même quand on ajoutera à l'un des indices un multiple de p.

Le groupe qu'on obtient en opérant toutes les substitutions de cette forme linéaire contient, en tout,

$$p^\nu(p^\nu - 1)(p^\nu - p)\ldots(p^\nu - p^{\nu-1}) \text{ permutations.}$$

Il s'en faut que dans cette généralité les équations qui lui répondent soient solubles par radicaux.

La condition que j'ai indiquée dans le *Bulletin de Férussac* pour que l'équation soit soluble par radicaux est trop restreinte; il y a peu d'exceptions, mais il y en a.

La dernière application de la théorie des équations est relative aux équations modulaires des fonctions elliptiques.

On sait que le groupe de l'équation qui a pour racines les sinus de l'amplitude des $p^2 - 1$ divisions d'une période est celui-ci :

$$x_k, \qquad x_{\frac{ak+b}{ck+d}};$$

par conséquent l'équation modulaire correspondante aura pour groupe

$$x_{\frac{k}{l}}, \qquad x_{\frac{ak+bl}{ck+dl}},$$

dans laquelle $\frac{k}{l}$ peut avoir les $p+1$ valeurs

$$\infty,\ 0,\ 1,\ 2, \ldots,\ p-1.$$

Ainsi, en convenant que k peut être infini, on peut écrire simplement

$$x_k, \qquad x_{\frac{ak+b}{ck+d}}.$$

En donnant à $a,\ b,\ c,\ d$ toutes les valeurs, on obtient

$$(p+1)\,p\,(p-1) \text{ permutations.}$$

Or ce groupe se décompose *proprement* en deux groupes, dont les substitutions sont

$$x_k, \qquad x_{\frac{ak+b}{ck+d}},$$

$ad - bc$ étant un résidu quadratique de p.

Le groupe ainsi simplifié est de

$$(p+1)\,p \cdot \frac{p-1}{2} \text{ permutations.}$$

Mais il est aisé de voir qu'il n'est plus décomposable proprement, à moins que $p = 2$, ou $p = 3$.

Ainsi, de quelque manière que l'on transforme l'équation, son groupe aura toujours le même nombre de permutations.

Mais il est curieux de savoir si le degré peut s'abaisser.

Et d'abord il ne peut s'abaisser plus bas que p, puisqu'une équation de degré moindre que p ne peut avoir p pour facteur dans le nombre des permutations de son groupe.

Voyons donc si l'équation de degré $p+1$, dont les racines x_k s'indiquent en donnant à k toutes les valeurs, y compris l'infini, et dont le groupe a pour substitutions

$$x_k, \qquad x_{\frac{ak+b}{ck+d}},$$

$ad - bc$ étant un carré, peut s'abaisser au degré p.

Or il faut pour cela que le groupe se décompose (improprement, s'entend) en p groupes de $(p+1)\frac{p-1}{2}$ permutations chacun.

Soient 0 et ∞ deux lettres conjointes dans l'un de ces groupes. Les substitutions qui ne font pas changer 0 et ∞ de place seront de la forme

$$x_k, \qquad x_{m^2k}.$$

Donc si M est la lettre conjointe de 1, la lettre conjointe de m^2 sera m^2M. Quand M est un carré, on aura donc M² = 1. Mais cette simplification ne peut avoir lieu que pour $p = 5$.

Pour $p = 7$ on trouve un groupe de $(p+1)\frac{p-1}{2}$ permutations, où

$$\infty \quad 1 \quad 2 \quad 4$$

ont respectivement pour lettres conjointes

$$0 \quad 3 \quad 6 \quad 5.$$

Ce groupe a ses substitutions de la forme

$$x_k, \qquad x_{a\frac{k-b}{k-c}},$$

b étant la lettre conjointe de c, et a une lettre qui est résidu ou non résidu en même temps que c.

Pour $p = 11$, les mêmes substitutions auront lieu avec les mêmes notations,

$$\infty \quad 1 \quad 3 \quad 4 \quad 5 \quad 9$$

ayant respectivement pour conjointes

$$0 \quad 2 \quad 6 \quad 8 \quad 10 \quad 7.$$

Ainsi, pour les cas de $p = 5,\ 7,\ 11$, l'équation modulaire s'abaisse au degré p.

En toute rigueur, cette réduction n'est pas possible dans les cas plus élevés.

Le troisième Mémoire concerne les intégrales.

On sait qu'une somme de termes d'une même fonction elliptique se réduit toujours à un seul terme, plus des quantités algébriques ou logarithmiques.

Il n'y a pas d'autres fonctions pour lesquelles cette propriété ait lieu.

Mais des propriétés absolument semblables y suppléent dans toutes les intégrales de fonctions algébriques.

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.

On trouve que le nombre des périodes distinctes de l'intégrale la plus générale relative à une irrationnelle donnée est toujours un nombre pair.

Soit $2n$ ce nombre, on aura le théorème suivant :

Une somme quelconque de termes se réduit à n termes, plus des quantités algébriques et logarithmiques.

Les fonctions de première espèce sont celles pour lesquelles la partie algébrique et logarithmique est nulle.

Il y en a n distinctes.

Les fonctions de seconde espèce sont celles pour lesquelles la partie complémentaire est purement algébrique.

Il y en a n distinctes.

On peut supposer que les différentielles des autres fonctions ne soient jamais infinies qu'une fois pour $x = a$, et, de plus, que leur partie complémentaire se réduise à un seul logarithme, log P, P étant une quantité algébrique. En désignant par $\Pi(x, a)$ ces fonctions, on aura le théorème

$$\Pi(x, a) - \Pi(a, x) = \Sigma \phi a\, \psi x,$$

ϕa et ψx étant des fonctions de première et de seconde espèce.

On en déduit, en appelant $\Pi(a)$ et ψ les périodes de $\Pi(x, a)$ et ψx relatives à une même révolution de x,

$$\Pi(a) = \Sigma\psi \times \phi a.$$

Ainsi les périodes des fonctions de troisième espèce s'expriment toujours en fonctions de première et de seconde espèce.

On peut en déduire aussi des théorèmes analogues au théorème de Legendre

$$\mathrm{FE}' + \mathrm{EF}' - \mathrm{FF}' = \frac{\pi}{2}.$$

La réduction des fonctions de troisième espèce à des intégrales définies, qui est la plus belle découverte de M. Jacobi, n'est pas praticable, hors le cas des fonctions elliptiques.

La multiplication des fonctions intégrales par un nombre entier est toujours possible, comme l'addition, au moyen d'une équation de degré n dont les racines sont les valeurs à substituer dans l'intégrale pour avoir les termes réduits.

L'équation qui donne la division des périodes en p parties égales est du degré $p^{2n} - 1$. Son groupe a en tout

$$(p^{2n} - 1)(p^{2n} - p)\ldots(p^{2n} - p^{2n-1}) \text{ permutations.}$$

L'équation qui donne la division d'une somme de n termes en p parties égales est du degré p^{2n}. Elle est soluble par radicaux.

De la transformation. On peut d'abord, en suivant des raisonnements analogues à ceux qu'Abel a consignés dans son dernier Mémoire, démontrer que si, dans une même relation entre des intégrales, on a les deux fonctions

$$\int \Phi(x, \mathrm{X})\, dx, \qquad \int \Psi(y, \mathrm{Y})\, dy,$$

la dernière intégrale ayant $2n$ périodes, il sera permis de supposer que y et Y s'expriment moyennant une seule équation de degré n en fonction de x et de X.

D'après cela on peut supposer que les transformations aient lieu constamment entre deux intégrales seulement, puisqu'on aura évidemment, en prenant une fonction quelconque rationnelle de y et de Y,

$$\Sigma \int f(y, \mathrm{Y})\, dy = \int \mathrm{F}(x, \mathrm{X})\, dx + \text{une quant. alg. et log.}$$

Il y aurait sur cette équation des réductions évidentes dans le cas où les intégrales de l'un et de l'autre membre n'auraient pas toutes deux le même nombre de périodes.

Ainsi nous n'avons à comparer que des intégrales qui aient toutes deux le même nombre de périodes.

On démontrera que le plus petit degré d'irrationnalité de deux pareilles intégrales ne peut être plus grand pour l'une que pour l'autre.

On fera voir ensuite qu'on peut toujours transformer une intégrale donnée en une autre dans laquelle une période de la première soit divisée par le nombre premier p, et les $2n - 1$ autres restent les mêmes.

Il ne restera donc à comparer que des intégrales où les périodes seront les mêmes de part et d'autre, et telles par conséquent que n termes de l'une s'expriment sans autre équation qu'une seule du degré n, au moyen de ceux de l'autre, et réciproquement. Ici nous ne savons rien.

Tu sais, mon cher Auguste, que ces sujets ne sont pas les seuls que j'aie explorés. Mes principales méditations, depuis quelque temps, étaient dirigées sur l'application à l'analyse transcendante de la théorie de l'ambiguïté. Il s'agissait de voir à priori, dans une relation entre des 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 de suite l'impossibilité de beaucoup d'expressions que l'on pourrait chercher. Mais je n'ai pas le temps, et mes idées ne sont pas encore bien développées sur ce terrain, qui est immense.

Tu feras imprimer cette Lettre dans la *Revue encyclopédique*.

Je me suis souvent hasardé dans ma vie à avancer des propositions dont je n'étais pas sûr; mais tout ce que j'ai écrit là est depuis bientôt un an dans ma tête, et il est trop de mon intérêt de ne pas me tromper pour qu'on me soupçonne d'avoir énoncé des théorèmes dont je n'aurais pas la démonstration complète.

Tu prieras publiquement Jacobi ou Gauss de donner leur avis, non sur la vérité, mais sur l'importance des théorèmes.

Après cela, il y aura, j'espère, des gens qui trouveront leur profit à déchiffrer tout ce gâchis.

Je t'embrasse avec effusion.

E. Galois.

Le 29 mai 1832.

1 Écrite, on se le rappelle, la veille de la mort de l'auteur. (J. L.)

2 Galois parle des manuscrits, jusqu'ici inédits, que nous publions. (J. L.)