Traduction d'un extrait de "A History of Algebra" de Bartel L. van der Waerden concernant Galois (p. 105 à 111) (Denise Vella-Chemla, août 2023).

Le mémoire de 1831

Pour nous, qui avons appris la théorie de Galois d'un livre ou de séances d'un cours, il n'est pas aussi difficile de comprendre le mémoire de Galois que cela l'a été pour Poisson.

Galois commence avec une équation $f(x) = 0$. Les coefficients sont supposés connus, par exemple, ce sont des nombres rationnels ou irrationnels ou juste des lettres. Toutes les fonctions rationnelles de ces coefficients sont dites rationnelles. On peut aussi *adjoindre* d'autres quantités, par exemple les racines m-ièmes de quantités rationnelles, et considérer comme rationnel au sens plus large toutes les fonctions rationnelles de ces quantités, dit Galois. En terminologie moderne, on dirait qu'un certain "corps de base" est présupposé, qui peut être étendu par des adjonctions au cours des recherches.

Si un polynôme $f(x)$ peut être factorisé sans quitter le corps de base, on le dit *réductible*, sinon il est dit *irréductible*.

Souvent, mais pas régulièrement, Galois utilise les mots *permutation* et *substitition* dans le même sens que Cauchy. Une permutation est un ordre d'un ensemble fini, et une substitution est un passage d'un ordre à un autre (ou au même).

Galois considère maintenant des *groupes* de substitutions ayant la propriété : si S et T appartiennent au groupe, ST y appartient aussi.

Si un polynôme f a une racine en commun avec un polynôme irréductible g, alors f est divisible par g. Ceci est le premier lemme de Galois. C'est aussi le premier théorème du mémoire de 1829 d'Abel. Le lemme implique que l'extension de corps $K(V)$ obtenue en adjoignant une racine V d'un polynôme irréductible $g(x)$ est complètement connue dès que le corps de base K et le polynôme g sont connus. En terminologie moderne, le corps $K(V)$ est isomorphe à l'anneau des classes résiduelles $K[x]/(g)$.

Galois prouve ensuite : si une équation $g(x) = 0$ n'a pas de racine multiple et si $a, b, c, \ldots$ sont ses racines, on peut toujours former une fonction V des racines telle que toutes les valeurs de V obtenues en permutant les racines soient différentes.

Par exemple, on peut prendre

$$V = Aa + Bb + Cc + \ldots \tag{1}$$

avec des entiers convenablement choisis A, B, C,..., dit Galois.

De ce lemme, Galois déduit un cas particulier de ce qu'on appelle maintenant le "théorème de l'élément primitif" :

Lemme 3. Si V est choisi comme précédemment, toutes les racines $a, b, c, \ldots$ sont exprimables comme des fonctions rationnelles de V.

Pour prouver ce lemme important, Galois pose

$$V = \varphi(a, b, c, ...).$$

Il permute maintenant les racines b, c, de toutes les manières possibles, en gardant seulement l'une des racines fixe a, et il forme le produit

$$[V - \varphi(a, b, c, ...)] \cdot [V - \varphi(a, c, b, ...)].....$$

Ceci est une fonction symétrique de $b, c, \ldots$ qui sont les racines du polynôme

$$g(x)/(x - a),$$

par conséquent elle peut être exprimée comme une fonction rationnelle de a. On a donc une équation

$$F(V, a) = 0. \tag{2}$$

Cett équation et

$$g(a) = 0 \tag{3}$$

ont seulement une racine a en commun, car il ne peut pas advenir, par exemple, que $F(V, b)$ soit nul, dit Galois.

Maintenant, si deux équations comme (2) et (3) ont seulement une racine a en commun, cette racine peut être calculée rationnellement. Donc a est une fonction rationnelle de V.

Galois a raison de dire que $F(V, b)$ ne peut être nul, car $F(V, b)$ est un produit de facteurs

$$[V - \varphi(b, a, c, ...)] \cdot [V - \varphi(b, c, a, ...)] \cdot ...$$

dans lequel les permutations $(b, a, c, ...)$ etc. sont toutes les permutations de $(a, b, c, ...)$ dans lesquelles b est en première position, alors que les autres $(a, c, ...)$ sont permutées de toutes les façons possibles. Cela découle de la définition de $F(V, a)$, comme l'a remarqué H. M. Edwards dans son livre "Galois Theory" (Springer-Verlag 1984), p. 44-45. Notamment : puisque toutes les expressions $\varphi(b, a, c, ...)$ etc. sont supposées être différentes de $V = \varphi(a, b, ...)$, il en découle que les $F(V, b)$ sont différents de zéro, et il en est de même des $F(V, c)$, etc.

Poisson a écrit une note dans la marge du lemme 3, disant : "La preuve de ce lemme est insuffisante, mais le lemme est vrai par l'article 100 du mémoire de Lagrange." Il est facile de comprendre l'attitude de Poisson. La preuve de Galois est seulement une esquisse, et il ne démontre pas l'assertion que $F(V, b)$ est non nul. La dernière phrase de Poisson "Il est vrai par l'article 100 de Lagrange" est correcte, car dans l'article 100 des "Réflexions" de Lagrange, une preuve complète

du lemme est fournie.

Selon moi, Galois avait raison de dire que sa preuve est essentiellement correcte, mais Poisson avait raison de déclarer qu'elle était incomplète.

En notation moderne, on peut maintenant écrire

$$K(a, b, c, ...) = K(V) \tag{4}$$

où K est le corps de base. L'"élément primitif" V est une racine d'une équation irréductible. Appelons

$$V, V', V'', ...V^{(n-1)}$$

les racines de cette équation. Le lemme 4 dit : si $a = \varphi(V)$ est une racine de l'équation originale, $\varphi(V')$ sera aussi une racine. La preuve est aisée.

Ensuite vient le théorème principal :

Proposition I. Il y a un groupe de permutations des lettres $a, b, c, \ldots$, tel que

1° Toute fonction des racines, invariable selon les substitutions du groupe, est connue rationnellement ;

2° inversement, toute fonction des racines connue est invariable selon le groupe.

La terminologie de Galois n'est pas consistante. Il parle d'abord des "permutations" et ensuite des "substitutions" formant le groupe, mais ce qu'il veut dire est complètement clair.

Pour prouver ce théorème, Galois exprime les racines comme des fonctions rationnelles de V :

$$\varphi V, \varphi_1 V, ..., \varphi_{m-1} V.$$

Il écrit ensuite les permutations

$$\begin{array}{llll} \varphi V, & \varphi_1 V, & \varphi_2 V, & \ldots, \ \varphi_{m-1} V \\ \varphi V', & \varphi_1 V', & \varphi_2 V', & \ldots, \ \varphi_{m-1} V' \\ \ldots & \ldots & \ldots & \ldots \ \ \ldots \\ \varphi V^{(n-1)}, & \varphi_1 V^{(n-1)}, & \varphi_2 V^{(n-1)}, & \ldots, \ \varphi_{m-1} V^{(n-1)} \end{array}$$

et il énonce que le "groupe des permutations" (signifiant le groupe correspondant des substitutions) satisfait les conditions requises. La preuve est très courte, mais il n'est pas difficile pour un lecteur moderne d'en compléter les étapes.

Galois recherche ensuite comment le groupe de l'équation change quand le corps de base est étendu par l'adjonction d'une racine ou de toutes les racines d'une équation auxiliaire. Il est clair qu'après l'adjonction le groupe de Galois sera un sous-groupe H du groupe original G. Si H est un sous-groupe propre, G peut être décomposé comme suit :

(5) $$G = H + HS + HS' + ...$$

ou, alternativement, comme

(6) $$G = H + TH + T'H + ...$$

Ces deux décompositions sont plus clairement expliquées dans la lettre à Chevalier (Œuvres de Galois, 1897, p. 25-32).

Les deux décompositions ne coïncident pas toujours, dit Galois. Si elles coïncident, la décomposition est dite "propre". En terminologie moderne, c'est le cas quand H est un "sous-groupe invariant", ou un "diviseur normal" de G. En particulier, si *toutes* les racines d'une équation auxiliaire sont adjointes, les deux décompositions coïncideront. Ceci est la proposition III de Galois. La preuve est omise ("On trouvera la démonstration").

Galois en vient maintenant à son principal problème : dans quel cas une équation est-elle résoluble par radicaux ?

On peut, bien sûr, se restreindre aux radicaux de degré premier p. À chaque fois qu'une racine p-ième est extraite, Galois suppose que les racines p-ièmes de l'unité sont adjointes au préalable. Ceci n'est pas une restriction essentielle, parce que Gauss avait déjà démontré que les racines p-ièmes de l'unité peuvent s'exprimer au moyen de radicaux de degrés moindres que p.

Supposons maintenant que l'adjonction d'un radical r, racine d'une équation

(7) $$x^p - s = 0,$$

amène à une réduction du groupe de Galois. Parce que les racines p-ièmes de l'unité

$$\alpha, \alpha^2, ..., \alpha^p = 1$$

sont dans le corps de base, la même réduction est obtenue en adjoignant *toutes* les racines de l'équation (7). Par la proposition III, la décomposition (5) sera une décomposition propre, c'est-à-dire que le sous-groupe H est un diviseur normal. Galois a affirmé, mais n'a pas démontré, que le nombre de termes dans la décomposition (5) (qu'on appelle l'indice de H dans G) est juste un nombre premier p. Inversement, si G a un diviseur normal H d'indice premier p, on peut réduire le groupe de Galois G au sous-groupe H en adjoignant un radical de degré p. Ceci est démontré comme dans nos livres en prenant une fonction invariante selon le groupe H et en formant un "résolvant de Lagrange"

(8) $$z = \theta + \alpha\theta_1 + \alpha^2\theta_2 + \ldots + \alpha^{p-1}\theta_{p-1}$$

où α est une racine p-ième de l'unité, alors que $\theta_1, \theta_2, \ldots$, les substitutions sont obtenues à partir de θ par les substitutions

$$S, S^2, ..., S^{p-1}$$

représentant les cosets dans la décomposition (5).

Il en découle qu'une équation $g(x) = 0$ est résoluble par radicaux si et seulement si une séquence de sous-groupes

$$G \supset H_1 \supset H_2 \supset ... \supset H_m = E$$

existe, telle que tout H_k est un diviseur normal du précédent H_{k-1} ou G, alors que tous les indices sont des nombres premiers. Si tel est le cas, on dit que le groupe G est *résoluble*.

Galois suppose ensuite que l'équation $f(x) = 0$ est irréductible et de degré premier n. Il démontre : l'équation peut être résolue par radicaux si et seulement si chacune des substitutions de G transforme x_k en $x_{k'}$ par une transformation linéaire de k modulo n :

$$k' = ak + b \pmod{n}.$$

Le groupe de Galois de l'équation générale quintique n'est pas de cette forme, par conséquent son équation ne peut être résolue par radicaux. Ainsi le résultat d'Abel découle de la théorie de Galois.

Dans la dernière version de son mémoire de l'Académie, Galois a cité Abel, mais au moment où il a envoyé sa première version à l'Académie, il ne connaissait même pas le nom d'Abel. Ses sources principales étaient les travaux de Lagrange, Gauss, et Cauchy.

Les corps de Galois

À la fois Abel et Galois avaient une notion claire de ce que l'on appelle maintenant un "corps". Galois énonce bien au début de son grand mémoire :

"On peut s'accorder à considérer comme rationnelle toute fonction rationnelle d'un certain nombre de quantités regardées comme connues a priori", et il continue en expliquant ce qu'il veut dire par adjoindre une certaine quantité au corps des quantités considérées comme connues.

Les corps considérés par Abel et Galois dans leurs articles sur la résolution des équations contiennent tous le corps des nombres rationnels. En terminologie moderne, ce sont des corps de caractéristique zéro. Si la caractéristique était p, l'équation

$$x^p - 1 = 0$$

aurait seulement une racine $x = 1$, alors que Abel et Galois supposent toujours que les racines p-ièmes de l'unité sont toutes différentes.

Pourtant, dans son article "Sur la théorie des nombres", qui fut publié en 1830 dans le Bulletin des Sciences de Férussac (Œuvres de Galois, Paris 1897, p. 15-23) Galois construit des corps finis, ce qu'on appelle les *corps de Galois*. Il énonce dès le tout début que son objectif est de considérer les structures algébriques dans lesquelles toutes les quantités, multipliées par p, sont considérées comme nulles. Dans ses propres termes, il dit :

> Si l'on s'accorde à regarder comme nulles toutes les quantités qui, dans des calculs algébriques sont multipliées par p, et si on essaie de trouver, selon cette convention, la solution d'une équation algébrique $Fx = 0$, que Mr. Gauss désigne par la notation $Fx \equiv 0$, l'habitude est de considérer les solutions entières seulement. Ayant été amené, par mes propres recherches, à considérer des solutions incommensurables, j'ai atteint certains résultats que je considère comme nouveaux.

En lisant ces mots, il est clair que le point de départ de Galois était le calcul des congruences modulo un nombre premier p, initié par Gauss. Il était connu que des classes résiduelles modulo p peuvent être ajoutées, multipliées, et que la congruence

$$ax \equiv b \text{ (modulo } p)$$

peut toujours être résolue par des solutions rationnelles, en supposant que a n'est pas congru à zéro. En d'autres termes, les classes résiduelles modulo p forment un corps.

Gauss avait aussi considéré les congruences de degrés plus élevés telles que

$$x^2 \equiv a \text{ (modulo } p),$$

mais il admettait seulement des solutions rationnelles. Galois se demande alors si on peut introduire des solutions irrationnelles, c'est-à-dire si on peut élargir le corps de classe résiduelle par l'adjonction de racines non contenues dans le corps original.

Galois suppose que le polynôme Fx est irréductible modulo p. Il se demande si on peut résoudre la congruence $Fx \equiv 0$ en introduisant de nouveaux "symboles", qui peuvent être juste aussi utiles que l'unité imaginaire i en analyse ordinaire.

Galois appelle i l'une des racines de la congruence $Fx \equiv 0$ de degré ν. Il forme les p^ν expressions

$$\text{(A)} \qquad a + a_1 i + a_2 i^2 + \ldots + a_{\nu-1} i^{\nu-1},$$

où $a, a_1, a_2, ..., a_{\nu-1}$ sont les entiers modulo p. Ces p^ν éléments forment ce que nous appelons aujourd'hui un "corps de Galois" $\mathrm{GF}(p^\nu)$.

Il est facile de montrer que les expressions (A) forment un corps, c'est-à-dire qu'elles satisfont les règles bien connues d'addition, soustraction, multiplication, et division.

Galois prend maintenant un élément α de la forme (A), dans lequel les coefficients $a, a_1, \ldots, a_{\nu-1}$ ne sont pas tous nuls. Les puissances $\alpha, \alpha^2, ...$ ne peuvent pas être toutes différentes, par conséqueent une puissance α^n doit être égale à 1. Si n est le plus petit entier pour lequel α^n est égal à 1, les expressions

$$1, \alpha, \alpha^2, ..., \alpha^{n-1}$$

doivent être toutes différentes. En terminologie moderne, elles forment un sous-groupe du groupe multiplicatif du corps de Galois.

En multipliant ces nombres par un autre élément $\beta \neq 0$, on obtient un coset du sous-groupe. En continuant de la même façon, on trouve que tous les cosets ensemble forment le sous-groupe

multiplicatif dans son entièreté d'ordre $p^\nu - 1$, et que l'exposant n est un diviseur de $p^\nu - 1$. Par conséquent, on a

$$\alpha^{p^\nu - 1} = 1.$$

Ensuite on démontre, dit Galois, comme dans la théorie des classes résiduelles modulo p, qu'il existe des "racines primitives" pour lesquelles n est exactement $p^\nu - 1$. Tous les autres éléments non nuls du corps de Galois sont des puissances d'un élément primitif α. La preuve de l'existence d'un tel élément, donnée par Gauss pour le cas d'un corps de classes résiduelles modulo p, marche juste aussi bien que dans le cas de $\mathrm{GF}(p^\nu)$.

On voit maintenant que tous les éléments du corps de Galois, incluant zéro, sont des racines du polynôme

(B) $$x^{p^\nu} - x$$

et que tout polynôme irréductible Fx de degré ν est un diviseur du polynôme (B). Si α est une des racines d'un tel polynôme, les autres sont

$$\alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{\nu-1}}.$$

Cela découle de la congruence bien connue

$$(Fx)^p \equiv F(x^p).$$

À la fin de son traité, Galois inverse la situation. Il commence avec une extension quelconque de corps de $\mathrm{GF}(p)$ dans laquelle le polynôme (B) peut être complètement factorisé. Se restreignant lui-même au sous-corps engendré par les racines, il prend un "élément primitif" i du sous-corps. Un tel élément existe toujours selon un théorème connu d'Abel, dit Galois. Tout tel i est une racine d'un polynôme irréductible (mod p) Fx. Le choix du polynôme irréductible ν qui est choisi n'a pas d'importance, on obtient toujours le même corps $\mathrm{GF}(p^\nu)$. Dans la plupart des cas, la façon la plus simple d'obtenir un tel polynôme est de le faire "par tatônnement", dit Galois, par essai et erreur. Comme exemple, il prend $p = 7$ et $\nu = 3$. Le polynôme $x^3 - 2$ est irréductible (mod 7), et une racine i de ce polynôme engendre le corps $\mathrm{GF}(7^3)$.