Équations, des Babyloniens à Abel et Galois

Daniel PERRIN

Table des matières

Introduction

Ce texte est la rédaction d'une conférence donnée le 13 mars 2019 à l'IREM de Paris 7 dans le double cadre de la journée Maths-Monde et du séminaire de l'IREM. Il a été revu en mars 2022 pour une conférence dans le cadres des soirées mathématiques de l'ENS de Lyon.

Équations ou mathématiques ?

La notion d'équation est omniprésente en mathématiques, à tel point qu'on peut se demander si elle n'en est pas synonyme. J'en veux pour preuve l'énoncé des fameux problèmes du millenium qui tous parlent, peu ou prou, d'équations :

- L'hypothèse de Riemann : les solutions de l'équation $\zeta(s) = 0$.
- La conjecture de Birch et Swinnerton-Dyer : les solutions rationnelles de l'équation $y^2 = x^3 + px + q$.
- La conjecture de Hodge : elle établit un lien entre la topologie algébrique d'une variété algébrique complexe définie par des équations polynomiales et sa géométrie.
- Les équations de Navier-Stokes.
- Les équations de Yang-Mills.
- L'équation ... $P = NP$.

Et, pour citer un résultat célèbre et récent : le grand théorème de Fermat et l'équation $x^n + y^n = z^n$.

Qu'est-ce qu'une équation ?

Une définition

Une définition assez générale d'équation peut être la suivante : *Soit* $f : X \to A$ *une application et soit* $a \in A$. *Résoudre l'équation* $f(x) = a$ *en l'inconnue* x *consiste à trouver les* x *qui s'envoient sur* a, *c'est-à-dire ce qu'on appelle la fibre* $f^{-1}(\{a\})$. C'est une situation universelle en mathématiques.

Quelques types d'équations

Avec cette définition, on voit surgir un nombre considérable d'exemples : les équations $f(x) = 0$ avec une fonction réelle, voire un polynôme, leurs variantes arithmétiques sur $\mathbf{Z}$ (Fermat), $\mathbf{Q}$ (les courbes elliptiques), $\mathbf{F}_q$ (les conjectures de Weil), etc., les équations de la forme $f(x_1, \ldots, x_n) = 0$ qui définissent les variétés et mènent à la géométrie algébrique ou analytique ou

différentielle, enfin les équations de l'analyse : différentielles, aux dérivées partielles, intégrales, stochastiques, etc.

Quelques types de problèmes

Par ailleurs, les problèmes posés par les équations sont aussi multiples. On peut citer l'existence de solutions : où et combien ? (D'Alembert, Fermat), le calcul des solutions (par radicaux, approché), la description de l'ensemble des solutions (par exemple en géométrie algébrique : degré, irréductibilité, topologie, etc.)

Soyons modestes ...

Dans ce texte on se contentera d'étudier les équations algébriques c'est-à-dire les équations de la forme $P(x) = 0$ où P est un polynôme :

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0.$$

C'est une question qui a une histoire très ancienne et très riche et on se contentera d'en donner un aperçu, centré notamment sur la résolution par radicaux. Pour justifier l'importance qu'on leur accorde encore, on n'oubliera pas que c'est pour résoudre ces équations que deux notions capitales ont été inventées : les nombres complexes et la notion de groupe.

Avertissement

On utilisera librement ici des éléments de théorie des corps (extensions, éléments algébriques, degré, ...) et de théorie de Galois pour lesquels on renvoie à [11], [9], [10]. Une notion reviendra souvent, c'est celle de corps de décomposition d'un polynôme $P \in K[X]$. Il s'agit d'un corps L (unique à isomorphisme près) engendré sur K par toutes les racines de P, voir [9].

1 L'histoire ancienne

Ce paragraphe a pour but de donner un arrière-plan aux travaux de Lagrange, Abel et Galois. Il est volontairement succinct et il ne prétend pas être complet, surtout du point de vue historique.

1.1 L'équation du second degré

Nous nous contentons ici d'évoquer les équations algébriques de degré ≥ 2. Le cas du degré 2 est connu depuis très longtemps comme en témoignent les deux exemples suivants.

1.1.1 Les Babyloniens

Les anciens Babyloniens disposaient d'un algorithme de résolution de l'équation du second degré. Voici un exemple : il s'agit du problème 1 de la tablette BM 13901 - 1 dans la traduction [1] de Thureau-Dangin (1936).

J'ai additionné[2] *la surface et le côté de mon carré : 45'.*

Traduction. Rappelons que l'unité est fractionnée en 60 minutes, de sorte que $45' = 3/4$. Ici, on cherche x (le côté du carré) tel que $x^2 + x = 45'$ (on reconnaît une équation $ax^2 + bx + c = 0$ avec $a = 1, b = 1, c = -3/4$).

Solution : Tu poseras 1, l'unité. Tu fractionneras en deux 1 : 30'. Tu croiseras 30' et 30' : 15'. Tu ajouteras 15' à 45' : 1. C'est le carré de 1. Tu soustrairas 30', que tu as croisé, de 1 : 30', le côté du carré.

En clair : L'unité est b, on la divise en deux : $30' = 1/2$ et on "croise", c'est-à-dire qu'on multiplie : $(\frac{b}{2})^2 = \frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$; on ajoute le résultat à $-c = 45'$, on trouve 1 : $(\frac{b}{2})^2 - c = \frac{1}{4} + \frac{3}{4} = 1 = 1^2$, on en prend la racine à laquelle on retranche $\frac{b}{2}$: $x = -\frac{b}{2} + \sqrt{(\frac{b}{2})^2 - c} = -\frac{1}{2} + 1 = \frac{1}{2}$. Avec nos yeux actuels on reconnaît la formule donnant les racines de l'équation !

1.1.2 Les Grecs

Les Grecs ne s'intéressent pas directement aux nombres (autres que les entiers). C'est pourquoi les équations n'apparaissent que sous forme géométrique dans les mathématiques d'Euclide et somme toute assez rarement. Voici un exemple qui revient à la résolution d'une équation du second degré (Euclide II, prop. 11) : *Partager une droite donnée de manière que le rectangle compris sous la droite entière et l'un de ses segments soit égal au carré de l'autre segment.* En termes modernes, une longueur b étant donnée, trouver a telle que $b(b - a) = a^2$. La construction d'Euclide est donnée sur la figure ci-dessous.

1. Pour une intéressante discussion sur ce thème on renvoie à l'article de Christine Proust `http://images.math.cnrs.fr/Mathematiques-en-Mesopotamie.html`.

2. On notera que les Babyloniens ajoutent des longueurs et des aires. Les Grecs n'auraient jamais fait ça !

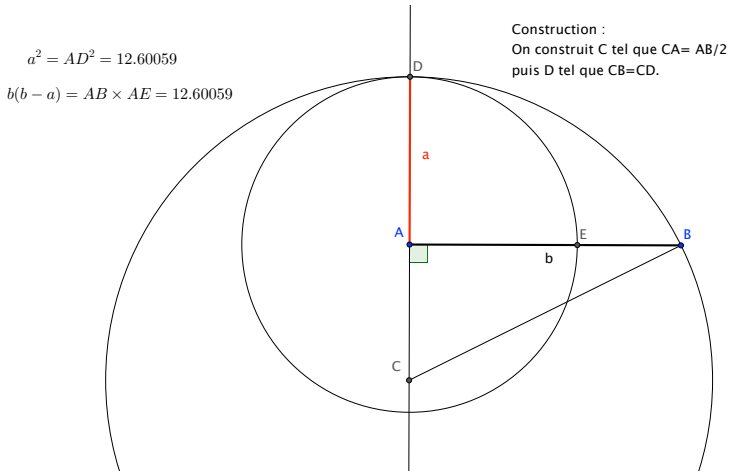

FIGURE 1 – La construction d'Euclide

On notera que le rapport $\phi = \frac{b}{a}$ vérifie $\phi^2 - \phi - 1 = 0$. C'est bien sûr le nombre d'or [3]. Dans Euclide, cette construction mène à celle d'un triangle d'angles $36°, 72°, 72°$, puis à celle du pentagone régulier.

Un autre exemple est le suivant : *Couper une droite en moyenne et extrême raison* (Euclide, Livre VI, prop. 30). Un segment est dit coupé en extrême et moyenne raison lorsque le segment total est au plus grand segment comme le plus grand segment est au plus petit : pour a donné, on cherche x tel que $\dfrac{a}{x} = \dfrac{x}{a-x}$, soit encore $x(x+a) = a^2$, il s'agit bien d'une équation du second degré et on retombe encore sur le nombre d'or.

1.1.3 Bilan sur l'équation du second degré

On voit que la résolution de l'équation du second degré est déjà maîtrisée par les Anciens. En termes modernes, il s'agit de l'équation $ax^2 + bx + c = 0$ et deux faits sont connus depuis longtemps et en tout cas à la fin du Moyen-âge : la somme et le produit des racines sont donnés par $x_1 + x_2 = -b/a$, $x_1 x_2 = c/a$ (ce qu'on appelle parfois théorème de Viète) et on connaît la méthode pour enlever le terme en bx en rendant la somme des racines nulles en posant $X = x + \frac{b}{2a}$.

3. Mais Euclide n'évoque jamais un tel nombre.

1.2 Les italiens de la Renaissance

L'équation de degré 3 en revanche résiste à tous les efforts jusqu'au XVI-ième siècle où elle est résolue par les mathématiciens italiens (Scipion del Ferro 1515, Tartaglia 1535, la solution est publiée par Cardan en 1545 et c'est sous son nom qu'elle est connue aujourd'hui).

1.2.1 La méthode de Cardan

On considère une équation de la forme $x^3 + ax^2 + bx + c = 0$, avec $a, b, c \in \mathbf{R}$. Comme pour l'équation du second degré, les Anciens savent supprimer le terme en x^2 par le changement de variable $X = x + \frac{a}{3}$. En effet, l'équation devient alors :

$$X^3 + \big(b - \frac{a^2}{3}\big)X + c - \frac{ab}{3} + \frac{2a^3}{27} = 0$$

qui est de la forme $X^3 + pX + q = 0$. On supposera désormais qu'on est dans ce cas.

On cherche donc les racines de $x^3 + px + q = 0$. L'astuce consiste à poser $x = u + v$ en introduisant deux inconnues au lieu d'une. L'intérêt – non évident *a priori* – est d'avoir un degré de liberté supplémentaire. L'équation devient :

$$u^3 + v^3 + (u + v)(3uv + p) + q = 0.$$

C'est ici que se révèle l'intérêt de l'astuce. Comme on a deux inconnues u, v, on peut leur imposer une relation supplémentaire, et ici, on va imposer la relation $(*) : 3uv + p = 0$, ce qui tue un des termes et il reste $u^3 + v^3 + q = 0$. On constate alors qu'on connaît la somme $u^3 + v^3 = -q$ et le produit $u^3 v^3 = -\frac{p^3}{27}$ grâce à $(*)$. Quand on a la somme S et le produit P de deux nombres, on sait qu'ils sont racines de l'équation du second degré $Y^2 - SY + P = 0$. Ici, u^3 et v^3 sont donc racines de l'équation $(**) : Y^2 + qY - \frac{p^3}{27}$.

On résout cette équation, on obtient u^3 et v^3, on extrait leurs racines cubiques [4] u et v et on obtient x comme la somme $u + v$:

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{4p^3 + 27q^2}{4 \times 27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{4p^3 + 27q^2}{4 \times 27}}}.$$

Par exemple, pour l'équation $x^3 + 6x + 2$ on trouve un discriminant 36 pour $(**)$ et la solution $x = \sqrt[3]{2} - \sqrt[3]{4}$.

4. Il faut parfois faire attention, voir ci-dessous.

Appliquons cette méthode à une équation étudiée par Newton : $x^3 - 2x - 5 = 0$. L'équation qui donne u^3, v^3 est alors $Y^2 - 5Y + \frac{8}{27} = 0$. Le discriminant en est $\Delta = 25 - \frac{32}{27} = \frac{643}{27}$ et on obtient :

$$u^3 = \frac{5}{2} + \frac{\sqrt{643}}{6\sqrt{3}}, \quad v^3 = \frac{5}{2} - \frac{\sqrt{643}}{6\sqrt{3}}.$$

On en déduit l'unique racine de l'équation donnée :

$$x = \sqrt[3]{\frac{5}{2} + \frac{\sqrt{643}}{6\sqrt{3}}} + \sqrt[3]{\frac{5}{2} - \frac{\sqrt{643}}{6\sqrt{3}}}.$$

On vérifie que l'on a $x \sim 2,09455148154$ comme le donne aussi la méthode (des tangentes) de Newton.

1.2.2 Le cas irréductible et l'introduction des complexes

Ce qui précède s'applique sans difficulté lorsque le discriminant $\Delta = \frac{4p^3 + 27q^2}{27}$ de l'équation $(**)$ est positif, ce qui correspond au cas où l'équation admet une unique racine réelle en vertu du lemme suivant :

1.1 Lemme. *L'équation $x^3 + px + q = 0$ admet une unique racine réelle si et seulement si on a $4p^3 + 27q^2 > 0$.*

Démonstration. On étudie la fonction $f(x) = x^3 + px + q$, sa dérivée est $f'(x) = 3x^2 + p$. Si p est positif, on voit que f est croissante, donc a un unique zéro, et $4p^3 + 27q^2$ est bien > 0. Sinon, f est croissante jusqu'à $\alpha = -\sqrt{-\frac{p}{3}}$, puis décroissante jusqu'à $\beta = \sqrt{-\frac{p}{3}}$, puis croissante. Elle admet un maximum relatif M en α et un minimum relatif m en β. Dire que l'équation a une seule racine réelle c'est dire que m et M sont de même signe, donc que le produit mM est > 0. Or, on a :

$$mM = \left(q + \frac{2p}{3}\sqrt{-\frac{p}{3}}\right)\left(q - \frac{2p}{3}\sqrt{-\frac{p}{3}}\right) = \frac{4p^3 + 27q^2}{27} = \Delta,$$

d'où le résultat.

On voit que, dans le cas $\Delta > 0$ où l'équation a une unique racine réelle, les choses se passent bien : l'équation $(**)$ a deux racines réelles u^3, v^3, chacune

admet une unique racine cubique réelle u, v et on trouve $x = u + v$, unique racine de l'équation comme dans l'exemple ci-dessus.

En revanche, lorsque l'équation a 3 racines réelles, le discriminant Δ est négatif et l'équation $(**)$ n'a plus de solutions [5]. Plus de solutions ? Au moins dans les réels, car on peut faire le calcul de Cardan avec les complexes, et c'est d'ailleurs pour faire ce calcul qu'ils ont été inventés par Bombelli [6] vers 1572. En fait, Bombelli introduit une sorte de signe supplémentaire à côté des signes plus (*piu*) et moins (*meno*), signe qu'il appelle *piu di meno* (plus de moins) et qui correspond en langage moderne à $i = \sqrt{-1}$. Il utilise aussi $-i$ appelé *meno di meno*.

En langage moderne, lorsque Δ est négatif, on trouve d'abord les deux racines u^3, v^3 de $(**)$, qui sont complexes conjuguées, puis on extrait leurs racines cubiques u, v. Attention, il y a deux difficultés ici. La première est de trouver vraiment ces racines. Le lecteur y exercera sa sagacité. La seconde tient au fait que u^3 admet trois racines cubiques : u, ju, j^2u et de même pour v. Si on calcule toutes les sommes possibles de ces racines, on va trouver 9 valeurs pour x, ce qui est trop pour une équation de degré 3. En fait, il faut se souvenir ici qu'on a imposé la relation $uv = -\dfrac{p}{3}$, de sorte que si on effectue l'un des trois choix possibles pour u, l'autre valeur v est bien déterminée, donc aussi x et on a les racines $x_1 = u + v$, $x_2 = j^2u + jv$ et $x_3 = ju + j^2v$.

1.2 *Exemple.* Pour convaincre de la valeur de leurs méthodes, les anciens utilisaient souvent des équations à solutions évidentes et nous allons les copier ici. Considérons donc l'équation $x^3 - 7x + 6 = 0$, qui admet les racines évidentes $1, 2, -3$ et appliquons lui la méthode de Cardan. L'équation $(**)$ est $Y^2 + 6Y + \dfrac{343}{27} = 0$, dont le discriminant est $\Delta = -\dfrac{400}{27}$. Les racines de $(**)$ sont $u^3 = -3 + \dfrac{10}{3\sqrt{3}}i$ et $v^3 = -3 - \dfrac{10}{3\sqrt{3}}i$ et il faut en extraire les racines cubiques. Comme on l'a dit, ce n'est pas si facile [7]. On trouve que les trois racines cubiques sont $u_1 = 1 + \dfrac{2i\sqrt{3}}{3}$, $u_2 = ju_1 = -\dfrac{3}{2} + \dfrac{i\sqrt{3}}{6}$ et $u_3 = ju_1 = \dfrac{1}{2} - \dfrac{5i\sqrt{3}}{6}$. Pour trouver les valeurs correspondantes de v, on utilise la relation $(*)$ $uv = \dfrac{7}{3}$, en notant que $7/3$ est exactement le carré du module des u_i, ce qui montre que les v_i sont leurs conjugués. On a donc

5. On parle traditionnellement de "cas irréductible" de l'équation de degré 3 dans cette situation.

6. D'autres en voient l'origine dans le *Ars magna* de Cardan en 1545.

7. Sur ce sujet on pourra consulter : `https://www.math.u-psud.fr/~perrin/CAPES/algebre/Cardan10.pdf`

$v_1 = \overline{u_1} = 1 - \dfrac{2i\sqrt{3}}{3}$ qui donne $x_1 = u_1 + v_1 = 2$, de même $v_2 = \overline{u_2}$, qui donne $x_2 = -3$ et enfin $v_3 = \overline{u_3}$ qui fournit $x_3 = 1$.

Inutile de dire qu'à l'époque de Bombelli, ce calcul (qui n'était évidemment pas formulé ainsi) passait pour magique et le nom d'imaginaires pour les nouveaux nombres en témoigne. Il faudra plus de 200 ans pour que le statut des nombres complexes soit clairement élucidé.

1.2.3 Le degré 4

L'équation de degré 4 est résolue en 1540 par Ferrari, qui est un disciple de Cardan. On trouvera sa méthode et une explication géométrique en termes de pinceaux de coniques sur ma page web : `https://www.math.u-psud.fr/~perrin/CAPES/algebre/Ferrari.pdf`

En revanche, malgré un certain nombre de travaux, l'équation du cinquième degré résiste.

1.3 Deux résultats importants

1.3.1 Coefficients et racines, Viète (1540-1603)

Il s'agit de généraliser les formules qui donnent la somme et le produit des racines dans le cas du second degré. On considère l'équation :

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = 0.$$

Si $x_1, \ldots, x_n$ sont ses racines, on a les formules :

$$a_1 = -(x_1 + \cdots + x_n), \quad a_2 = x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n, \ldots$$

$$a_k = (-1)^k \sum_{i_1 < \ldots < i_k} x_{i_1} \cdots x_{i_k}, \quad \cdots, \quad a_n = (-1)^n x_1 \cdots x_n.$$

On voit que ces éléments sont invariants par permutation [8] des racines (ce sont des polynômes symétriques) et le théorème fondamental (dû à Newton ?) affirme : *Tout polynôme symétrique en les x_i est un polynôme en les fonctions symétriques élémentaires, donc en les a_i.*

1.3.2 Le théorème de D'Alembert-Gauss

Il joue un rôle important en arrière-plan de la théorie :

8. Cette notion va jouer un rôle capital dans toute la suite.

1.3 Théorème. *Tout polynôme de degré n à coefficients réels (ou complexes) admet n racines complexes, comptées avec multiplicités.*

Ce résultat est énoncé par Albert Girard en 1629 : *Toutes les équations d'algèbre reçoivent autant de solutions que la dénomination de la plus haute quantité le démontre.*

Voici ce qu'en dit Descartes, un peu plus tard : *En chaque équation autant que la quantité inconnue a de dimensions, autant peut-il y avoir de diverses racines : mais souvent il arrive que ces racines soient fausses ou moindres que rien. Comme si on suppose que x désigne aussi le défaut d'une quantité qui soit 5, on a $x + 5 = 0$, qui multipliée par $x^3 - 9x^2 + 26x - 24 = 0$ fait $x^4 - 4x^3 - 19x^2 + 106x - 120 = 0$ pour une équation en laquelle il y a quatre racines, à savoir trois vraies qui sont $2, 3, 4$ et une fausse qui est 5.*

Et il ajoute, plus loin : *Ces racines sont quelquefois seulement imaginaires c'est-à-dire que l'on peut toujours en imaginer autant que j'ai dit en chaque équation, mais qu'il n'y a quelquefois aucune quantité qui corresponde à celle qu'on imagine...*

D'Alembert propose une preuve du théorème en 1746 (pas tout à fait correcte [9]), ainsi qu'Euler, Lagrange, Laplace et surtout Gauss qui en donne quatre preuves (1799, 1815, 1816, 1849).

2 Lagrange et Vandermonde

2.1 Les deux articles fondateurs

En 1770-1771 paraissent deux articles essentiels :

• Joseph-Louis Lagrange (1736-1813), *Réflexions sur la résolution algébrique des équations.* Mémoires de l'Académie royale des sciences et Belles-Lettres de Berlin, 1770-1771, Œuvres Tome III. Voir [7].

• Alexandre -Théophile Vandermonde (1735-1796) [10], *Mémoire sur la résolution des équations*, Mémoires de l'Académie des sciences de Paris, 1771. Voir [12].

Tous deux portent sur la résolution des équations du troisième et du quatrième degré, mais, par rapport à leurs devanciers, leur but est de donner une explication à des calculs jusque là abscons. Lagrange explique très clairement cet objectif :

9. Mais moins fausse qu'on ne l'a dit.

10. Au moment où ce texte a été écrit je ne disposais que du mémoire de Lagrange. Je n'évoquerai donc pas le travail de Vandermonde. Depuis, Michèle Lacombe m'a communiqué la référence du texte de Vandermonde sur Gallica et je l'en remercie vivement.

Je me propose dans ce Mémoire d'examiner les différentes méthodes que l'on a trouvées jusqu'à présent pour la résolution algébrique des équations, de les réduire à des principes généraux, et de faire voir a priori pourquoi ces méthodes réussissent pour le troisième et le quatrième degré, et sont en défaut pour les degrés ultérieurs. Et il ajoute : *... je donnerai à cette occasion les vrais principes et, pour ainsi dire, la métaphysique de la résolution des équations du troisième et du quatrième degré.*

2.2 Retour à Cardan

2.2.1 Analyse de la résolution

On considère une équation $x^3 + px + q = 0$ et on cherche à calculer ses racines x_1, x_2, x_3. On reprend la méthode de Cardan (dans la version Bombelli). Elle consiste à introduire u, v qui vont donner $u + v = x_1$ et à imposer $uv = -p/3$. On trouve u^3, v^3 comme solution d'une équation de degré 2, puis on en prend des racines cubiques, et on a $x_2 = j^2u + jv$ et $x_3 = ju + j^2v$.

Les éléments u et v et leurs cubes u^3, v^3 jouent donc un rôle crucial en scindant la résolution de l'équation en deux étapes : résoudre une équation du second degré pour trouver u^3, v^3 et en extraire ensuite les racines cubiques. Lagrange va examiner ces éléments avec l'idée de généraliser éventuellement cette méthode en degré plus grand.

Pour cela, il commence par renverser le problème en calculant u, v en fonction des racines. C'est facile, on a trois équations $x_1 = u+v$, $x_2 = j^2u+jv$, $x_3 = ju + j^2v$, dont on tire $3u = x_1 + jx_2 + j^2x_3$ et $3v = x_1 + j^2x_2 + jx_3$. Il appelle "résolvantes" ces éléments (on dit aujourd'hui "résolvantes de Lagrange").

Inversement, on retrouve les x_i en résolvant le système [11] :

$$\begin{cases} x_1 + x_2 + x_3 = 0 \\ x_1 + jx_2 + j^2x_3 = 3u \\ x_1 + j^2x_2 + jx_3 = 3v \end{cases}$$

qui donne en particulier $x_1 = u + v$.

Il cherche ensuite ce que deviennent les éléments u, v par permutation [12]. Si on pose $\sigma = (123)$, on a $\sigma(u) = j^2u$, $\sigma(v) = jv$, et avec $\tau = (23)$, on a $\tau(u) = v$ et $\tau(v) = u$. On en déduit que u^3 et v^3 sont invariants par σ et échangés par τ. On voit que u^3 et v^3 ne sont que partiellement symétriques.

11. On notera que le déterminant de ce système est un déterminant de Vandermonde !
12. C'est l'idée fondamentale !

En revanche, u^3+v^3 et u^3v^3 sont symétriques donc, en vertu du théorème de Newton, ils se calculent avec les coefficients du polynôme (précisément, on a vu les formules $u^3+v^3=-q$ et $u^3v^3=-\frac{p^3}{27}$).

2.1 *Remarque.* Il y a une ici une petite difficulté qui échappe à Lagrange et ne s'éclaire qu'avec la notion de groupe de Galois : si $u(x_1,x_2,x_3)$ est une fonction des racines et si σ est le cycle (123), l'écriture $\sigma(u)(x_1,x_2,x_3)=u(x_2,x_3,x_1)$ n'a peut-être aucun sens. Pour que σ définisse un homomorphisme (ce qui est indispensable pour déduire $\sigma(u^3)=u^3$ de $\sigma(u)=j^2u$), il faut que σ conserve les relations entre les racines. Par exemple, si $P(X)=(X^2-2)X$, avec les racines $x_1=0, x_2=\sqrt{2}$ et $x_3=-\sqrt{2}$, si $u=x_1+2x_2+2x_3=0$, on a $x_2+2x_3+2x_1=-\sqrt{2}$ et donc pas $\sigma(u)=0$! Ou encore, on a $x_1=-2x_2-2x_3$, mais si l'on applique σ, on n'a plus $x_2=-2x_3-2x_1$, σ n'a de sens que sur l'écriture formelle (i.e. dans l'anneau de polynômes en x_1,x_2,x_3), pas sur les nombres. Pour que l'écriture ait un sens il faut en tous cas que le polynôme soit irréductible, ce que Lagrange suppose implicitement.

2.2.2 La métaphysique

L'idée de Lagrange est maintenant claire. Pour résoudre l'équation, les éléments u^3, v^3 ont joué un rôle essentiel. Or, quelle est la propriété de ces éléments, c'est d'être **partiellement** invariants par permutation : ce sont des fonctions des racines qui, par permutation, **prennent seulement deux valeurs** comme dit Lagrange, ici $u^3=(x_1+jx_2+j^2x_3)^3$ et $v^3=(x_1+j^2x_2+jx_3)^3$ et sont donc racines d'une équation du second degré.

Plus généralement, pour résoudre par radicaux une équation de degré n, il s'agit de trouver des fonctions des racines qui, par permutation, prennent r valeurs avec $1<r<n$ comme u^3 ci-dessus ou, dans le cas d'une équation de degré 4, $\alpha:=x_1x_2+x_3x_4$ qui, par permutation ne prend que 3 valeurs : α, $\beta=x_1x_3+x_2x_4$ et $\gamma=x_1x_4+x_2x_3$. En effet, α est alors racine de l'équation $(Y-\alpha)(Y-\beta)(Y-\gamma)=0$ dont les coefficients sont des fonctions symétriques des x_i donc se calculent à partir des coefficients de l'équation. On voit ainsi apparaître ici, en filigrane, le sous-groupe du groupe des permutations qui laissent fixe α, et l'extension qui lui correspond. C'est la théorie de Galois avant l'heure ...

Comme le dit Lagrange : *Voilà, si je ne me trompe, les vrais principes de la résolution des équations et l'analyse la plus propre à y conduire ; tout se réduit, comme on le voit, à une espèce de calcul des combinaisons, par lequel on trouve a priori les résultats auxquels on doit s'attendre.*

2.2.3 Lagrange et le degré 5

Lagrange essaie d'appliquer sa méthode aux équations de degré 5 en introduisant la résolvante $r_1 := x_1 + \zeta x_2 + \zeta^2 x_3 + \zeta^3 x_4 + \zeta^4 x_5$ (où ζ est une racine cinquième primitive de l'unité) et les variantes évidentes. Par la permutation circulaire $\sigma = (12345)$ on a $\sigma(r_1) = \zeta^{-1} r_1$ donc r_1^5 est invariant par σ. Si on sait le calculer, on trouve les x_i par un système de type Vandermonde comme ci-dessus. Le problème est donc de trouver r_1^5 et ses comparses comme on a trouvé u^3, v^3 ci-dessus. Malheureusement, *a priori*, l'équation que vérifie r_1^5 (la résolvante) est de degré $24 = 120/5$. On peut cependant, comme l'explique Lagrange, se ramener à des équations de degré plus petit en considérant en plus de r_1 les éléments obtenus en permutant les x_i d'indices $2, 3, 4, 5$ par exemple par $\tau = (2453)$. On obtient ainsi quatre éléments r_i, par exemple $r_2 = x_1 + \zeta^2 x_2 + \zeta^4 x_3 + \zeta x_4 + \zeta^3 x_5$ et on cherche à calculer les fonctions symétriques en les r_i^5. Comme elles sont invariantes par les 20 permutations engendrées par σ et τ, ces fonctions vérifient des équations de degré $120/20 = 6$, mais on a encore une équation de degré > 5.

Une autre voie (que n'aborde pas Lagrange) est la suivante. Les fonctions rationnelles génériques en les x_i "prennent" 120 valeurs par permutation, mais on peut tenter d'introduire des éléments invariants par un certain nombre de ces permutations, à la manière de l'élément $x_1x_2 + x_3x_4$ apparu dans la résolution de l'équation de degré 4. Ici, un tel candidat plausible est :

$$u = (x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1) - (x_1x_3 + x_2x_4 + x_3x_5 + x_4x_1 + x_5x_2)$$

qui est invariant par les permutations (12345) et (25)(34), donc qui a vocation à être racine d'une équation de degré < 120. Mais ce degré est encore plus grand que 5. Par exemple, dans le cas $P(X) = X^5 + pX + q$ l'équation vérifiée par u est :

$$R(X) = X^6 - 20pX^4 + 240p^2X^2 - 32\delta X + 320p^3$$

où δ est la racine carrée du discriminant Δ de l'équation, de sorte que u est racine d'un polynôme de degré 12 ou 6 (si Δ est un carré) à coefficients dans le corps de base. On obtient un élément de degré 6 en considérant u^2 (car u est anti-invariant par le 4-cycle (2354)).

La méthode échoue donc et Lagrange lui-même considère qu'il y a peu d'espoir de ce côté : *Il résulte de ces réflexions qu'il est très douteux que les méthodes dont nous venons de parler puissent donner la résolution complète des équations du cinquième degré et à plus forte raison celle des degrés supérieurs.*

3 Le résultat d'Abel

3.1 Introduction

Comme on vient de le voir, après les travaux de Lagrange et Vandermonde, l'impossibilité de la résolution par radicaux des équations de degré ≥ 5 est dans l'air. Après une tentative incomplète de Ruffini en 1799 c'est au mathématicien norvégien Niels Abel (1802-1829) que revient le mérite [13] de montrer en 1824 que l'équation générale de degré 5 n'est pas résoluble par radicaux. Les résultats d'Abel apparaissent dans deux mémoires :

• *Mémoire sur les équations algébriques où l'on démontre l'impossibilité de la résolution de l'équation générale du cinquième degré.*

(Brochure imprimée chez Grondahl, Christiania [14], 1824, œuvres Tome 1, III, p. 28-33.)

• *Démonstration de l'impossibilité de la résolution algébrique des équations générales qui passent le quatrième degré.*

(Journal für die reine und angewandte Mathematik, dit Journal de Crelle, Band 1, Berlin, 1826.) Voir [1].

Le second mémoire étant nettement plus détaillé que le premier, c'est sur lui que je m'appuierai essentiellement dans ce qui suit. Notons déjà que, dès les premiers mots du texte, Abel précise ce qu'il entend par résolution algébrique :

Résoudre algébriquement une équation ne veut dire autre chose, que d'exprimer ses racines par des fonctions algébriques des coefficients.

Il précise juste après ce que sont les fonctions algébriques : celles qui utilisent l'addition, la multiplication, la division et l'extraction des racines avec des exposants premiers et il ajoute qu'alors la soustraction, l'élévation à des puissances entières et l'extraction des racines avec des exposants composés [15] sont comprises dans ces quatre opérations.

Avertissement Dans ce qui suit, j'analyse le mémoire d'Abel avec les mots et les concepts d'un mathématicien actuel, mais en restant toutefois le plus proche possible du texte original. Pour des précisions sur la théorie de Galois, le lecteur se reportera à [9], [11], [10].

13. À bien y réfléchir, je ne suis plus tout à fait sûr que la preuve d'Abel soit vraiment complète. On verra en effet qu'il y a un point douteux, en tous cas un point où je ne sais pas rendre la preuve d'Abel complètement convaincante. Bien entendu, cela n'enlève rien à son mérite car sa preuve contient nombre d'idées absolument essentielles sur le sujet.

14. C'est l'ancien nom d'Oslo.

15. Pour extraire une racine $p_1 \cdots p_r$-ième on extrait successivement des racines p_r-ièmes, etc., p_1-ièmes.

3.2 Le résultat d'Abel

Dans tout ce qui suit, tous les corps sont supposés de **caractéristique nulle** et toutes les extensions $K \subset L$ sont supposées **finies**, c'est-à-dire que L est un K-espace vectoriel de dimension finie.

Dit en termes modernes, voilà le résultat prouvé par Abel :

3.1 Théorème. *Soit k un corps contenant toutes*[16] *les racines de l'unité. On considère le corps des fractions rationnelles en cinq indéterminées $L = k(X_1, \ldots, X_5)$ et son sous-corps $K = k(\Sigma_1, \ldots, \Sigma_5)$ engendré par les polynômes symétriques élémentaires. On pose :*

$$P(X) = X^5 - \Sigma_1 X^4 + \Sigma_2 X^3 - \Sigma_3 X^2 + \Sigma_4 X - \Sigma_5 = (X - X_1)(X - X_2) \cdots (X - X_5).$$

Le polynôme P est à coefficients dans K, ses racines sont $X_1, \ldots, X_5$ et $L = D_K(P)$ est le corps de décomposition de P sur K.

Alors, l'équation $P(x) = 0$ n'est pas résoluble par radicaux sur K.

3.2 *Remarques.* 1) Contrairement à Galois, Abel ne considère que des équations générales ou plutôt génériques[17] ce qui est traduit dans le théorème ci-dessus par le fait que les X_i sont des indéterminées. Ici, c'est dans le mémoire de 1824 qu'il dit les choses de manière explicite :

... comme il s'agit de la résolution de l'équation générale du cinquième degré, il est clair qu'on peut considérer y_1, y_2, y_3, y_4, y_5 comme des variables indépendantes

et il ajoute :

Par conséquent on peut échanger les quantités y_i entre elles ...

Cette dernière phrase signifie que ce dont il a besoin, en fait, c'est que le groupe de Galois de l'équation soit le groupe symétrique $\mathfrak{S}_5$ tout entier, ce qui est réalisé dans le cas de l'équation générique, mais le serait aussi pour bien d'autres. Nous verrons plus bas où cette hypothèse est utile. Pour une discussion sur la différence que l'on fait aujourd'hui entre les mots générale et générique, voir [10] §8.

2) Un mot sur la présence de racines de l'unité. Là encore Abel ne dit pas explicitement qu'il suppose la présence de suffisamment de racines de l'unité, mais il les utilise dès le premier paragraphe. En réalité, ce point n'est pas essentiel, car si les racines de l'unité ne sont pas dans le corps de base, on peut toujours les y adjoindre, voir 3.9.

16. Par exemple le corps $\mathbf{C}$ des nombres complexes, mais il suffit de prendre une extension de $\mathbf{Q}$ contenant les racines k-ièmes de l'unité pour $k = 3$ et $k = 5$, voir 3.8 ci-dessous.

17. Précisément à racines génériques, mais c'est la même chose que des équations à coefficients génériques.

3.3 Une preuve moderne du théorème d'Abel

Je donne ici une preuve moderne, qui utilise la théorie de Galois (voir au besoin [11]), mais qui suit fidèlement la ligne de la démonstration d'Abel. Pour des détails sur ce que fait vraiment Abel, on se reportera au paragraphe suivant.

3.3.1 Une définition

Nous donnons ici la définition moderne du mot "résoluble par radicaux" et des extensions radicales :

3.3 Définition. *Soit K un corps (de caractéristique 0) et M une extension de K. On dit que M est* **radicale** *sur K s'il existe une suite de corps $K_0 = K \subset K_1 \subset \cdots \subset K_r = M$ telle que, pour chaque $i = 0, \ldots, r-1$, on ait $K_{i+1} = K_i(\alpha_i)$ avec $\alpha_i^{p_i} = a_i$, $p_i \in \mathbf{N}^*$ un nombre premier et $a_i \in K_i$.*

Une extension M de K est dite **résoluble** *si elle est contenue dans une extension radicale. Enfin, une équation $P(x) = 0$ avec $P \in K[X]$ est dite* **résoluble par radicaux** *si son corps de décomposition $L = D_K(P)$ (corps engendré par les racines de P) est résoluble sur K.*

3.4 *Remarque.* On peut donner cette définition sans supposer que les exposants p_i sont premiers. Cela revient au même en vertu du lemme suivant :

3.5 Lemme. *Soit $K \subset K(\alpha)$ une extension, avec $\alpha^n = a \in K$. Il existe une suite de corps $K = K_0 \subset K_1 \subset \cdots \subset K_s = K(\alpha)$ tel que chaque étage soit engendré par un radical de degré premier.*

Démonstration. On raisonne par récurrence sur le nombre k de facteurs premiers de n, le résultat étant évident si $k = 1$. Pour passer de k à $k+1$ on écrit $n = pm$ avec p premier, de sorte qu'on a $(\alpha^m)^p = a$. On a donc la suite de corps $K \subset K(\alpha^m) \subset K(\alpha)$ et il suffit d'appliquer l'hypothèse de récurrence à l'extension $K(\alpha^m) \subset K(\alpha)$.

La proposition suivante est immédiate :

3.6 Proposition. *Soient $K \subset L \subset M$ des extensions.*
1) Si M/K est radicale, M/L l'est aussi.
2) Si L/K et M/L sont radicales, M/K l'est aussi.

Nous utiliserons aussi la notion d'extension normale [18], essentielle en théorie de Galois, que nous détaillerons plus bas, voir §5.2.1. Voir aussi [11] ou [10].

18. En caractéristique zéro, cette notion est équivalente à celle d'extension galoisienne.

3.3.2 Le résultat de structure des extensions énoncé par Abel

Les notations sont celles de 3.1. En termes modernes, le théorème de structure énoncé par Abel est le suivant :

3.7 Théorème. *Soit K un corps contenant suffisamment de racines de l'unité. Soit $P \in K[X]$ un polynôme et $L = D_K(P)$ son corps de décomposition. On suppose que l'équation $P(x) = 0$ est résoluble par radicaux. Alors, il existe une suite de sous-corps $K \subset K_1 \subset \cdots \subset K_r = L$ où $K_{i+1} = K_i(\alpha_i)$ avec $\alpha_i^{p_i} = a_i \in K_i$, p_i premier.*

Commentaire. Autrement dit, on peut supposer que L est non seulement résoluble mais radicale, c'est-à-dire que l'extension M donnée par 3.3, qui contient L, lui est en fait égale. Du point de vue technique, ce résultat est le plus délicat de tout le texte d'Abel. Nous verrons plus loin comment il prétend le démontrer. Mon opinion est que sa preuve est pour le moins vague, sinon insuffisante. Je donne ci-dessous une preuve du résultat d'Abel qui utilise la théorie de Galois et la caractérisation des extensions résolubles par la résolubilité de leur groupe de Galois. C'est bien sûr une tricherie puisque ces notions ne sont pas connues avant Galois (et même dans Galois elles sont encore bien imprécises). C'est un aveu d'impuissance : je ne sais pas rendre correcte la preuve d'Abel. Voir ci-dessous §3.6 pour une tentative, plus proche des idées d'Abel, mais qui utilise aussi la théorie de Galois.

3.8 Proposition. *Soit $K \subset L$ une extension galoisienne résoluble de degré n. On suppose que, pour tout p premier diviseur de n, les racines p-ièmes de l'unité sont dans K. Alors, l'extension est radicale.*

Démonstration. Le cas où n est premier résulte de [10] 4.13 (c'est la résolvante de Lagrange). Pour le cas général, on raisonne par récurrence sur n. Si n n'est pas premier, le groupe de Galois $G := \mathrm{Gal}(L/K)$, qui est résoluble, voir [10] 4.1, admet un sous-groupe distingué non trivial H et on note M l'extension intermédiaire correspondante. On a $K \subset M \subset L$. Les deux extensions sont résolubles, de degrés diviseurs de n et plus petits que n, donc l'hypothèse de récurrence montre qu'elles sont radicales, donc aussi L/K en vertu de [10] 3.6.

Notons que la présence de racines de l'unité, si elle est techniquement importante, ne l'est pas fondamentalement, car on peut toujours les adjoindre [19] :

19. C'est le moment d'appliquer le principe de Jeanne d'Arc répondant à la question de ses juges : – *Jeanne, êtes-vous en état de grâce ?* – *Si je n'y suis, Dieu veuille m'y mettre, si j'y suis, Dieu veuille m'y tenir.*

3.9 Lemme. *Soit $K \subset L$ une extension galoisienne et $K \subset K(\zeta)$ une extension engendrée par une racine de l'unité. Alors, L est résoluble sur K si et seulement si $L(\zeta)$ l'est sur $K(\zeta)$.*

Démonstration. Cela résulte de [10] 3.13 et du fait que les extensions cyclotomiques sont résolubles. On a même une version forte où l'on n'utilise pas les racines de l'unité dans la tour radicale, voir ci-dessous 8.3.

3.3.3 Les résultats sur les groupes

On reprend les notations précédentes. Comme $K_1 = K(\alpha)$ est de degré p premier sur K, le groupe de Galois $\mathrm{Gal}(L/K_1)$ est un sous-groupe de $\mathfrak{S}_5$ d'indice p. Abel utilise alors le résultat suivant, dû à Cauchy [20] :

3.10 Lemme. *Soit n un entier, p le plus grand diviseur premier de n et soit H un sous-groupe de $\mathfrak{S}_n$. Alors H est d'indice 1, 2 ou $\geq p$. Si H est strictement contenu dans $\mathfrak{A}_n$ il est d'indice $\geq p$ dans $\mathfrak{A}_n$.*

On suppose $n = 5$. Un sous-groupe d'indice premier de $\mathfrak{S}_5$ (resp. $\mathfrak{A}_5$) est d'indice 2 ou 5 (resp. 5). L'unique sous-groupe d'indice 2 de $\mathfrak{S}_5$ est $\mathfrak{A}_5$.

Démonstration. Soit $H \subset \mathfrak{S}_n$ un sous-groupe d'indice $< p$. Alors, il contient tous les p-cycles (sinon, si σ est un p-cycle non dans H, le sous-groupe engendré $<\sigma>$ s'injecte dans l'ensemble quotient $\mathfrak{S}_n/H$). Alors, il contient les 3-cycles grâce à la formule $(1,3,2) = (1,p,p-1,\cdots,4,2,3)(1,2,\cdots,p)$. Il contient donc $\mathfrak{A}_n$, donc est d'indice 1 ou 2. Le même argument donne aussi le cas de $\mathfrak{A}_n$. Le cas $n = 5$ résulte du fait que l'indice divise 120, donc vaut $2, 3$ ou 5.

La version originelle de Cauchy est en termes d'orbites en non de sous-groupes :

3.11 Lemme. *Le nombre de valeurs différentes d'une fonction non symétrique de n quantités ne peut s'abaisser au-dessous du plus grand nombre premier p contenu dans n sans devenir égal à 2.*

(Ou encore : Une orbite de $\mathfrak{S}_n$ de cardinal > 2 est de cardinal $\geq p$.)

Tant qu'on y est, on a aussi le lemme suivant :

20. *Mémoire sur le nombre des valeurs qu'une fonction peut acquérir lorsqu'on y permute de toutes les manières les quantités qu'elle renferme*, 17-ième cahier du Journal de l'école polytechnique, 1815 ou Oeuvres, Série II, Tome 1, p. 64. On notera que, pour $n = 5$, Cauchy en attribue la paternité à Ruffini.

3.12 Lemme. *1) Tout sous-groupe d'indice* 5 *de* $\mathfrak{S}_5$ *(resp.* $\mathfrak{A}_5$*) est le stabilisateur d'un élément*[21].

2) Soit P *irréductible de degré* 5 *sur* K*, de groupe de Galois* $\mathfrak{S}_5$ *ou* $\mathfrak{A}_5$*, et soient* $x_1, \ldots, x_5$ *les racines de* P *dans* $L = D_K(P)$*. Si* $\alpha \in L$ *est de degré* 5 *sur* K*, il existe* i *tel que* $K(\alpha) = K(x_i)$*.*

Démonstration. 1) Soit $H \subset \mathfrak{S}_5$ (resp. $\mathfrak{A}_5$), de cardinal 24 (resp. 12). On considère l'opération de H sur $\{1, 2, \ldots, 5\}$. Elle ne peut être transitive car 5 ne divise pas 24 (resp. 12). Si elle fixe un point, H est contenu dans le stabilisateur de ce point, donc égal et on a gagné. Sinon, c'est qu'on a deux orbites de cardinaux 2 et 3. Mais, $\mathfrak{S}_5$ (resp. $\mathfrak{A}_5$) opère transitivement sur les 10 ensembles $\{i, j\}$, de sorte que le stabilisateur d'un tel ensemble est de cardinal 12 (resp. 6). Il ne peut donc contenir H !

2) Vu le point 1), la théorie de Galois assure que les seules extensions de degré 5 de K contenues dans L sont les $K(x_i)$ et c'est le cas de $K(\alpha)$.

3.3.4 La fin de la preuve

Revenons au théorème en supposant d'abord que l'indice de $\mathrm{Gal}(L/K(\alpha))$ est $p = 5$, de sorte que $K(\alpha)$ est de degré 5 sur K et égal à $K(x_i)$ en vertu de 3.12. Comme K contient les racines cinquièmes de l'unité, l'extension $K \subset K(\alpha)$ est galoisienne, donc si x_i est dans $K(\alpha)$, tous ses conjugués aussi, donc $L = K(\alpha)$ et c'est absurde car L est de degré 120.

Supposons maintenant $p = 2$. Le groupe $\mathrm{Gal}(L/K(\alpha))$ est donc $\mathfrak{A}_5$. On considère l'étage suivant de la tour : $K_1 \subset K_2 = K_1(\beta)$. Le groupe $\mathrm{Gal}(L/K_1)$ est un sous-groupe d'ordre premier de $\mathfrak{A}_5$, il est donc d'indice 5 et fixe un élément x_i. On a, comme ci-dessus, $K_1(x_i) = K_1(\beta)$. Mais, comme K_1 contient les racines cinquièmes de l'unité, l'extension $K_1 \subset K_1(\beta)$ est galoisienne et comme elle contient x_i, elle contient ses conjugués, donc est égale à L. Mais le degré de $K_1(\beta)$ sur K est 10 et c'est une contradiction.

3.3.5 Une variante avec les sous-groupes distingués

Si l'on dispose de cette notion[22], le théorème d'Abel est plus facile. Le lemme est le suivant :

3.13 Lemme. *Si* N *est un sous-groupe distingué de* $\mathfrak{S}_n$*,* $n \geq 5$*, de quotient abélien, on a* $N = \mathfrak{S}_n$ *ou* $\mathfrak{A}_n$*.*

21. Pour l'inciter à la prudence, le lecteur se souviendra que l'analogue de ce résultat dans $\mathfrak{S}_n$ est faux pour $n = 6$, voir [9] Ch.1 §8.

22. Essentiellement due à Galois, donc postérieure à Abel.

Démonstration. Tout cycle d'ordre 3 est un commutateur, donc dans N, cf. [9].

On considère la tour radicale $K \subset K_1 \subset K_2 \subset \cdots \subset K_r = L$. Comme les racines de l'unité sont dans K, l'extension $K \subset K_1$ est normale, donc $\mathrm{Gal}(K/K_1)$ est distingué dans $\mathfrak{S}_5$ (et distinct de $\mathfrak{S}_5$ car $K \neq K_1$). De plus, comme le quotient n'est autre que $\mathrm{Gal}(K_1/K) = \mathbf{Z}/p_1\mathbf{Z}$, donc abélien, le sous-groupe est donc $\{1\}$ ou $\mathfrak{A}_5$. Dans le premier cas on a $K_1 = L$, mais c'est absurde car L est de degré 120 et K_1 de degré premier. Dans le second, on a $p_1 = 2$. On considère alors K_2 qui est une extension normale non triviale de K_1. Le groupe $\mathrm{Gal}(L/K_2)$ est un sous-groupe distingué de $\mathrm{Gal}(L/K_1) = \mathfrak{A}_5$, c'est donc $\{1\}$, mais c'est encore absurde pour une raison de degré.

3.3.6 Annexe : un théorème d'irréductibilité

3.14 Lemme. *Soit K un corps de caractéristique nulle, p un nombre premier et a un élément de K qui n'est pas une puissance p-ième. Alors, le polynôme $X^p - a$ est irréductible sur K.*

Démonstration. On commence par un autre lemme :

3.15 Lemme. *Sous les hypothèses de 3.14, soit ζ une racine primitive p-ième de l'unité. Alors, a n'est pas une puissance p-ième dans $K(\zeta)$.*

Démonstration. Le groupe de Galois G de $K(\zeta)/K$ est cyclique d'ordre un diviseur d de $p-1$ (voir par exemple [10] Prop. 4.6). Supposons qu'on ait $a = b^p$ dans $K(\zeta)$. On calcule $\prod_{\sigma\in G}\sigma(b^p) = a^d = (\prod_{\sigma\in G}\sigma(b))^p := c^p$ et c est invariant par G, donc dans K. Comme d est premier avec p, on a une relation de Bézout $\lambda d + \mu p = 1$, d'où $a = (a^d)^\lambda (a^\mu)^p = (c^\lambda a^\mu)^p$ et a est une puissance p-ième dans K contrairement à l'hypothèse.

Revenons à 3.14. En vertu de 3.15, on peut supposer que K contient une racine primitive p-ième de l'unité ζ. Si $X^p - a$ est réductible, on a $X^p - a = PQ$ et les racines de P, Q sont des racines p-ièmes de a, donc de la forme $\zeta^i\alpha$ avec $\alpha^p = a$. En considérant le produit des racines de P on voit que K contient un élément de la forme $\zeta^j\alpha^k$ avec $1 \leq k < p$, qui est une racine p-ième de a^k. Mais si a^k est une puissance p-ième, on voit avec Bézout qu'il en est de même de a : c'est une contradiction.

3.4 Le mémoire de Crelle

Dans ce paragraphe, j'analyse ce que fait vraiment Abel dans le mémoire de Crelle.

3.4.1 Le paragraphe I

Abel précise dans ce paragraphe la forme des fonctions algébriques de n quantités $x_1, x_2, \ldots, x_n$. Rappelons qu'il entend par là les fonctions obtenues à partir de ses quatre opérations fondamentales : addition, multiplication, division, extraction de racines d'exposant premier. Il en distingue trois types : les fonctions entières, obtenues par addition et multiplication, les fonctions rationnelles, en ajoutant la division, et algébriques, avec en plus les racines. Il note que les fonctions entières sont des polynômes en les x_i et les rationnelles des fractions rationnelles en les x_i, autrement dit, il décrit l'anneau engendré $K[x_1, \ldots, x_n]$ et le corps $K(x_1, \ldots, x_n)$.

Plus importante est la description des fonctions algébriques générales. En termes modernes, celles-ci sont contenues dans une tour d'extensions $K \subset K_1 = K(\sqrt[n_1]{p_1}) \subset K_2 = K_1(\sqrt[n_2]{p_2}) \subset \ldots \subset K_{r-1}(\sqrt[n_r]{p_r})$. Abel introduit deux notions : le degré, qui est le nombre total de radicaux ajoutés, et l'ordre, qui est la hauteur des radicaux (i.e. le nombre de radicaux superposés).

Le lemme essentiel qu'il démontre est qu'on peut ramener les fonctions rationnelles en les radicaux à des fonctions polynomiales. Je le dis en termes modernes :

3.16 Lemme. *Soit K un corps, $a \in K$ et α tel que $\alpha^p = a$ avec p premier. On a $K[\alpha] = K(\alpha)$.*

Démonstration. Voici celle d'Abel. On considère un élément $\dfrac{P(\alpha)}{Q(\alpha)} \in K(\alpha)$. Soit ζ une racine p-ième primitive de l'unité. Alors le produit :

$$m := Q(\alpha)Q(\zeta\alpha)Q(\zeta^2\alpha)\cdots Q(\zeta^{p-1}\alpha)$$

est dans K. Abel considère ce résultat comme connu : "comme on sait" dit-il, mais l'argument pour prouver cela est le suivant. Le nombre m est un polynôme symétrique en les $\zeta^i\alpha$ à coefficients dans K. Le théorème fondamental des fonctions symétriques appliqué aux racines du polynôme $X^p - a$ montre que m est dans K. On a donc :

$$\frac{P(\alpha)}{Q(\alpha)} = \frac{1}{m}P(\alpha)Q(\zeta\alpha)Q(\zeta^2\alpha)\cdots Q(\zeta^{p-1}\alpha)$$

et cet élément est dans $K[\alpha]$.

3.17 *Remarques.* 1) On notera qu'Abel utilise déjà les racines de l'unité dans ce lemme.

2) On dispose aujourd'hui d'une preuve plus simple de ce résultat (et qui n'utilise pas les racines de l'unité). Il suffit de noter que $K[\alpha]$ est un K-espace vectoriel de dimension finie (car engendré par $1, \alpha, \ldots, \alpha^{p-1}$). Si $Q(\alpha)$

est non nul, la multiplication par $Q(\alpha)$ dans $K[\alpha]$ est K-linéaire injective, donc surjective, donc 1 est atteint et $Q(\alpha)$ est inversible dans $K[\alpha]$.

Abel précise ensuite que les éléments de $K[\alpha]$ sont de la forme $a_0 + a_1\alpha + \cdots + a_{p-1}\alpha^{p-1}$ avec des $a_i \in K$ (s'il y a des termes de degré $n \geq p$ il les ramène à cette forme en divisant n par p et en utilisant la relation $\alpha^p = a$). Enfin, il montre le lemme – un peu bizarre, mais essentiel – suivant :

3.18 Lemme. *Soit K un corps, $a \in K$ et α une racine p-ième de a avec p premier. Alors, si x est dans $K(\alpha)$ et pas dans K, on peut l'écrire sous la forme $x = b_0 + \beta + b_2\beta^2 + \cdots + b_{p-1}\beta^{p-1}$ où les b_i et $b := \beta^p$ sont dans K, mais où β n'est pas dans K. Nous dirons qu'une telle écriture est* **stricte**.

Démonstration. On peut écrire $x = a_0 + a_1\alpha + \cdots + a_{p-1}\alpha^{p-1}$ avec $a_i \in K$. Comme x n'est pas dans K, l'un des a_i, pour $i \geq 1$, est non nul et on prend celui de plus petit indice. On pose alors $\beta = a_i\alpha^i$, on a $\beta^p = a_i^p a^i \in K$. Pour voir que x s'écrit sous la forme annoncée, on utilise Bézout. Pour $k = i+1, \ldots, p-1$, il existe $u, v \in \mathbf{Z}$ avec $k = ui + vp$ et, quitte à diviser u par p, on peut supposer $1 \leq u < p$ et même $1 < u < p$. Alors, on a $\alpha^k = (\alpha^i)^u(\alpha^p)^v = (\frac{\beta}{a_i})^u a^v = b_u\beta^u$ avec $b_u \in K$ et on a gagné. Bien entendu, β n'est pas dans K, sinon α^i et α y seraient.

3.19 *Remarque.* Ce lemme, où le point essentiel est l'égalité à 1 du coefficient de β, joue un rôle technique important dans la suite du travail d'Abel, comme on le verra. Cela étant, il induit un certain nombre d'imprécisions quant à la possibilité de l'appliquer plusieurs fois, voir le commentaire qui suit la proposition 3.21.

3.4.2 Le paragraphe II

Dans ce paragraphe, Abel montre d'abord le résultat suivant, que je dis en termes modernes :

3.20 Proposition. *Soient p un nombre premier et K un corps contenant une racine primitive p-ième de l'unité ζ, K' une extension de K et $P(X)$ un polynôme de degré n à coefficients dans K. On considère une extension $K' \subset K'(\alpha)$ avec $\alpha^p = a \in K'$, $\alpha \notin K'$. Soit $x \in K'(\alpha) - K'$ un élément admettant une écriture stricte sur α : $x = a_0 + a_1\alpha + \cdots + a_{p-1}\alpha^{p-1}$ avec $a_1 = 1$. On a alors $P(x) = b_0 + b_1\alpha + \ldots + b_{p-1}\alpha^{p-1}$ avec $b_i \in K'$.*

On suppose que x est racine de P. On a les propriétés suivantes :

1) Les coefficients $b_0, \ldots, b_{p-1}$ sont nuls.

2) Les quantités $x_i = a_0 + a_1\zeta^i\alpha + \cdots + a_{p-1}\zeta^{i(p-1)}\alpha^{p-1}$ pour $i = 0, 1, \ldots, p-1$ sont aussi racines de P et sont toutes distinctes. On a $p \leq n$.

3) Le radical α est dans le corps de décomposition de P sur K c'est-à-dire le corps engendré sur K par les racines $x = x_1, \ldots, x_n$ de P.

Démonstration. 1) Ce point exprime que l'extension $K' \subset K'(\alpha)$ est de degré p et cela résulte de l'irréductibilité du polynôme $X^p - a$ sur K', voir 3.14. Voici comment Abel montre ce résultat.

Si les b_i sont non tous nuls, on a les deux relations $b_0 + b_1\alpha + \ldots + b_{p-1}\alpha^{p-1} = 0$ et $\alpha^p = a$. Le polynôme minimal[23] de α sur K' est donc un polynôme Q de degré $d \leq p-1$, qui divise les deux autres et on a $Q(\alpha) := c_0 + c_1\alpha + \ldots + c_d\alpha^d = 0$ avec $c_0 \neq 0$. Mais, les racines de Q sont des racines p-ièmes de a, donc de la forme $\zeta\alpha$ où ζ est une racine p-ième de l'unité. On a donc $Q(\zeta\alpha) = 0$, donc aussi $Q(\zeta\alpha) - \zeta^d Q(\alpha) = 0$. Mais ce dernier polynôme est de degré $< d$, donc nul puisque le polynôme minimal Q de α est de degré d. Il en résulte que le terme de degré 0 de $Q(\zeta\alpha) - \zeta^d Q(\alpha) = 0$ est nul : $c_0(\zeta^d - 1) = 0$, ce qui, comme on a $c_0 \neq 0$ et $d < p$, est absurde.

2) En termes modernes, le point 2) de 3.20 résulte du fait que l'extension $K' \subset K'(\alpha)$ est galoisienne et que son groupe de Galois est formé des transformations qui associent à α les $\zeta^i\alpha$. La preuve d'Abel utilise le point 1). Si l'on a $x = a_0 + a_1\alpha + \cdots + a_{p-1}\alpha^{p-1}$ et si ζ est une racine p-ième de l'unité, on pose $y = a_0 + a_1\zeta\alpha + \cdots + a_{p-1}\zeta^{p-1}\alpha^{p-1}$. On a $P(x) = b_0 + b_1\alpha + \ldots + b_{p-1}\alpha^{p-1}$ avec $b_i \in K$, donc $P(y) = b_0 + b_1\zeta\alpha + \ldots + b_{p-1}\zeta^{p-1}\alpha^{p-1}$. Si $P(x)$ est nul, le point 1) implique que les b_i sont tous nuls, donc aussi $P(y)$.

Par ailleurs, si deux des quantités du type y sont égales, en écrivant que leur différence est nulle et en divisant par α on obtient une équation vérifiée par α et de degré $< p$ ce qui est absurde. Les p quantités x_i sont des racines distinctes de P, ce qui prouve que p est $\leq n$.

Passons au point 3). On peut écrire $x = a_0 + a_1\alpha + \cdots + a_{p-1}\alpha^{p-1}$ avec $a_1 = 1$ et on a les x_i comme en 2). On vérifie qu'on a alors les formules $a_i\alpha^i = \frac{1}{p}(x_0 + \zeta^{(p-1)i}x_1 + \zeta^{(p-2)i}x_2 + \cdots + \zeta^i x_{p-1})$ (on inverse un système de type Vandermonde). Mais alors, comme on a $a_1 = 1$ et que les racines de l'unité sont dans K, on en déduit que α est dans $K(x_1, \ldots, x_n)$.

Jusque là, la preuve d'Abel est inattaquable et elle constitue un premier pas vers le théorème de structure 3.7. Pour obtenir ce résultat, Abel généralise le résultat précédent au cas où les racines $x_1, \ldots, x_n$ de P sont non plus dans une unique extension engendrée par un radical, mais dans une tour : $K \subset K_1 \subset \cdots \subset K_r$ dont chaque étage est engendré par un radical de degré premier : $K_{i+1} = K_i(\alpha_i)$ avec $\alpha_i^{p_i} = a_i \in K_i$. Ici, la rédaction d'Abel est nettement plus imprécise[24]. Voilà ce que j'en ai compris :

23. Abel ne dit pas cela, mais il prend le polynôme de degré minimal qui annule α.

24. On n'oubliera pas qu'il ne dispose pas des concepts et des notations modernes :

3.21 Proposition. *Soit K un corps contenant suffisamment de racines de l'unité, $P \in K[X]$, $L = D_K(P)$. On suppose que L est contenu dans une extension radicale au sens de 3.7. Alors, L lui-même est extension radicale de K et on peut écrire $K = L_0 \subset L_1 \subset \cdots \subset L_s = L$, où l'on a, pour tout i, $L_{i+1} = L_i(\beta_i)$ avec $\beta_i^{q_i} = b_i$, q_i premier, où b_i est dans L_i (donc dans L) et admet une écriture stricte au sens de 3.18 sur β_{i-1} et où x a une écriture stricte sur β_s.*

Démonstration. On sait que L est contenue dans une extension radicale M avec $K \subset K_1 \subset \cdots \subset K_r = M$ dont chaque étage est engendré par un radical de degré premier : $K_{i+1} = K_i(\alpha_i)$ avec $\alpha_i^{p_i} = a_i \in K_i$. On montre la proposition par récurrence descendante sur i. Cela revient essentiellement à montrer qu'on peut modifier les α_i pour qu'ils soient dans L. Soit x une racine de P. Elle est dans K_r et quitte à supprimer l'étage K_r, on peut supposer qu'elle n'est pas dans K_{r-1}. Quitte à changer α_r, on peut supposer que x admet une écriture stricte sur α_r. La proposition 3.20 montre alors que α_r est dans L.

Supposons la proposition établie jusqu'au rang $i+1$ et passons à i. On considère $a_i \in K_i$. Par l'hypothèse de récurrence, il est dans L ainsi que tous ses conjugués (car L est une extension normale). Bien entendu, Abel ne dit pas cela, je cite ce qu'il dit à propos de $v := a_i$ et de ses conjugués. *Soient $v_1, v_2, \ldots, v_{n'}$ les valeurs différentes de v qu'on trouve lorsqu'on échange entre elles les racines $x_1, \ldots, x_n$ de toutes les manières possibles. On peut donc former une équation de degré n' dont les coefficients sont des fonctions rationnelles et dont les racines sont les quantités $v_1, \ldots, v_{n'}$ qui sont des fonctions rationnelles des quantités $x_1, \ldots, x_n$.* Permuter les x_i c'est faire agir le groupe de Galois de L et les v_i sont alors exactement les conjugués de v comme on l'a dit [25].

De deux choses l'une : ou bien a_i est dans K_{i-1} et on supprime l'étage K_i, ou bien non et alors, quitte à changer α_{i-1}, on peut supposer que a_i a une écriture stricte sur α_{i-1} et, en appliquant 3.20 à a_i écrit sur α_{i-1} **et à ses conjugués**, on voit que α_{i-1} est dans L et on a franchi le pas de récurrence.

Commentaire. C'est ici que je conteste ce que fait Abel. En effet, s'il est vrai que a_i est dans $K(\alpha_{i-1})$, pour appliquer 3.20 on a besoin que ses conjugués aussi soient dans $K(\alpha_{i-1})$. Or *a priori* cette extension n'est pas normale sur K, de sorte que les conjugués des a_i ne sont pas nécessairement dedans. C'est un point subtil car les conjugués ne sont pas seulement obtenus en multipliant

corps, espaces vectoriels, etc.

25. D'ailleurs cet argument est dit de manière plus explicite dans le papier [13] de Wantzel dans lequel il reprend la preuve d'Abel mais – à mon avis – avec la même lacune.

par des racines de l'unité, il faut peut-être aller les chercher plus bas, voir la preuve de 3.28 ci-dessous. Je propose dans l'annexe 3.6 une manière de montrer le résultat d'Abel en utilisant un argument voisin du sien, mais en tenant compte de cette difficulté de non normalité. Le lecteur verra que, pour cela, j'utilise sans vergogne la théorie de Galois, ce qui est évidemment un anachronisme.

3.4.3 Le paragraphe III

3.22 *Remarque.* Dans ce paragraphe, Abel utilise systématiquement la notion de "valeurs différentes d'une fonction". Explicitons ce dont il s'agit. On est dans le corps $L = K(x_1, \ldots, x_n)$ engendré par les racines d'un polynôme P. Les éléments de L sont donc des fonctions rationnelles $f(x_1, \ldots, x_n)$. Les valeurs différentes des fonctions dont parle Abel sont celles obtenues par permutation des x_i : les $f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$. En termes modernes, il s'agit des conjugués de f (images de f par le groupe de Galois qui est ici le groupe $\mathfrak{S}_n$ des permutations des x_i). On sait que ce sont aussi les racines du polynôme minimal de f et dire qu'il y en a d signifie que le sous-corps $K(f)$ est de degré d (c'est-à-dire de dimension d comme K-espace vectoriel).

Abel commence par démontrer une variante du théorème dit de Lagrange[26]. On prend $v(x_1, \ldots, x_n) \in L = K(x_1, \ldots, x_n)$ et on considère les valeurs de v obtenues en permutant les x_i. Le résultat est que le nombre de valeurs différentes est un diviseur de $n!$ ("cela est connu" dit Abel). Il en donne une preuve qui ressemble beaucoup à la preuve maintenant classique de découpage en classes[27] d'équivalences.

Ensuite, il montre le lemme de Cauchy 3.10 sous la forme suivante (qui est la forme originelle de Cauchy, voir 3.11 ci-dessus) :

3.23 Lemme. *Avec les notations précédentes, on désigne par p le plus grand nombre premier qui divise n. Alors, le nombre de valeurs différentes de v obtenues en permutant les x_i est $1, 2$ ou $\geq p$. En particulier, pour $n = 5$, ce nombre ne peut être 3 ni 4.*

Démonstration. Supposons que v prenne moins de p valeurs et considérons une permutation σ d'ordre p. Il y a au moins deux valeurs égales parmi $v, \sigma(v), \ldots, \sigma^{p-1}(v)$ et on en déduit qu'il existe $r < p$ tel que $\sigma^r(v) = v$.

26. Dans la version d'Abel, comme dans Lagrange, le théorème ne porte pas sur le cardinal d'un sous-groupe (la notion n'existe pas) mais sur celui d'une d'une orbite.

27. Notons que, comme le fera aussi parfois Galois, il donne le nom de *groupes* aux classes d'équivalence : *... les valeurs de v au nombre de μ seront partagées en plusieurs groupes, dont chacun contiendra un nombre m de valeurs équivalentes.*

Comme on a aussi $\sigma^p(v) = v$, le théorème de Bézout montre qu'on a $\sigma(v) = v$. En appliquant cela à deux p-cycles comme dans la preuve de 3.10 on voit que v est invariant sous les 3-cycles [28] donc sous $\mathfrak{A}_n$ et on en déduit le résultat.

Abel montre ensuite le lemme :

3.24 Lemme. *Soit $f(x_1, \ldots, x_n)$ une fonction qui prend exactement deux valeurs, donc qui est invariante par les permutations paires et transformée en g par les permutations impaires des x_i. On pose $\delta = \prod_{i<j} x_i - x_j$. Alors, il existe des fonctions symétriques a, b des x_i telles que l'on ait $f = a + b\delta$.*

Démonstration. On note que l'on a $\sigma(\delta) = \epsilon(\sigma)\delta$ où ϵ désigne la signature. Il suffit alors de prendre $a = (f+g)/2$ et $b = (f-g)/(2\delta)$ et c'est essentiellement ce que fait Abel.

3.25 *Remarque.* Si l'on pose $\Delta = \delta^2$, on voit que Δ est un polynôme symétrique en les x_i, c'est le discriminant de l'équation donnée.

À partir de là on suppose $n = 5$.

Le lemme suivant est crucial (c'est essentiellement le lemme 3.12 ci-dessus) :

3.26 Lemme. *Soit $f(x_1, \ldots, x_5)$ une fonction rationnelle des x_i qui prend cinq valeurs (i.e de degré 5). Alors, il existe un x_i telle que l'on ait $K(f) = K(x_i)$.*

Démonstration. Il n'est pas si simple de comprendre ce que fait Abel. Premier point, disons $(*)$, il montre que si f est invariante par les permutations de $x_2, \ldots, x_5$, on peut l'écrire $f = r_0 + r_1 x_1 + \cdots + r_4 x_1^4$ où les r_i sont des fonctions symétriques de $x_1, \ldots, x_5$.

Ici, son raisonnement est un peu rapide. On peut écrire $f = P/Q$ avec P, Q des polynômes premiers entre eux. Par Gauss, l'invariance de f par $\mathfrak{S}_4$ implique la semi-invariance de P et Q : $\sigma(P) = \lambda(\sigma)P$ et $\sigma(Q) = \lambda(\sigma)Q$ avec $\lambda(\sigma) \in k^*$. De plus λ est alors un caractère de $\mathfrak{S}_5$ et il n'y a que le caractère 1 ou la signature ϵ. Mais, si λ est la signature, on montre qu'on a $P = P_1\delta$ et $Q = Q_1\delta$ où δ est la racine du discriminant vue en 3.24 et on peut simplifier par δ. On en déduit que P et Q sont invariants par $\mathfrak{S}_4$, ainsi que les coefficients de x_1^k dans ces polynômes. Ici, Abel montre que ces coefficients peuvent s'écrire comme polynômes en x_1 et en des polynômes symétriques en les cinq variables. C'est facile : on écrit $x_2 + \cdots + x_5 =$

28. Ce n'est visiblement pas un résultat connu du temps d'Abel que les 3-cycles engendrent $\mathfrak{A}_n$, c'est pourquoi il les décompose en produits de deux transpositions.

$(x_1+\cdots+x_5)-x_1$, $\sum_{2,\ldots,5} x_ix_j = \sum_{1,\ldots,5} x_ix_j - x_1^2 - x_1(x_2+\cdots+x_5)$, etc. On écrit le dénominateur comme ci-dessus, polynôme $G(x_1)$ avec des coefficients symétriques en les cinq. On multiplie haut et bas par les autres $G(x_i)$. En bas on a un polynôme symétrique, en haut un polynôme en x_1 à coefficients symétriques en $x_2,\ldots,x_5$ et on le remet sous la forme voulue. Bref, on a écrit $\alpha = a_0 + a_1x_1 + \ldots + a_4x_1^4$ avec des a_i rationnelles et symétriques : on a ainsi $K(\alpha) \subset K(x_1)$.

L'objectif est maintenant de montrer que toute fonction qui prend 5 valeurs est de du type $r_0 + r_1x_i + \cdots + r_4x_i^4$ où les r_k sont des fonctions symétriques de $x_1,\ldots,x_5$.

Soit v une fonction rationnelle de $x_1,\ldots,x_5$ qui prend cinq valeurs $v_1,\ldots,v_5$. Abel considère $x_1^m v$ (il ne dit pas pour quels m). Il permute $x_2,\ldots,x_5$ dans $x_1^m v$, obtenant les valeurs $x_1^m v_1,\ldots,x_1^m v_5$ et là, il dit qu'il y en a au plus quatre de distinctes, et cela vaut aussi pour les v_i.

Sinon, si les cinq sont différentes il regarde les autres $x_2^m v_i$, ..., $x_5^m v_i$, dit que toutes sont distinctes [29] et constate qu'il y en a 25, ce qui est interdit car 25 ne divise pas $5! = 120$.

En réalité, c'est plus simple : les valeurs en question, obtenues par permutation de quatre lettres forment une orbite sous $\mathfrak{S}_4$ dont le cardinal divise 4! *et ne peut donc valoir* 5.

Bref, le nombre de valeurs prises par les v_i lorsqu'on permute x_2, x_3, x_4, x_5 est donc $\mu = 1, 2, 3, 4$. Si $\mu = 1$ c'est gagné, on applique $(*)$. Si $\mu = 4$, on a 4 valeurs $v_1,\ldots,v_4$ sous l'action de $\mathfrak{S}_4$, donc $v_1+\cdots+v_4$ est invariante par $\mathfrak{S}_4$ et donc v_5 aussi car la somme est dans le corps de base. On a gagné avec v_5.

Vient ensuite $\mu = 2$, v prend deux valeurs v_1, v_2. Alors $v_1 + v_2$ est de la forme voulue, disons une fonction $\varphi(x_1)$. En permutant x_1 avec x_2 on a $v_2 + v_3 = \varphi(x_2)$ puis $v_3 + v_4 = \varphi(x_3)$, etc. $v_{m-1} + v_m = \varphi(x_{m-1})$, $v_m + v_1 = \varphi(x_m)$ avec $m = 2, 3, 4$ ou 5. Mais le cas $m = 2$ est impossible car $\varphi(x_1)$ ne prendrait que 2 valeurs au lieu de 5. Si c'est $m = 3$ on a $v_1 + v_2 = \varphi(x_1)$, $v_2 + v_3 = \varphi(x_2)$ et $v_3 + v_1 = \varphi(x_3)$, d'où $2v_1 = \varphi(x_1) + \varphi(x_3) - \varphi(x_2)$. Mais cette fonction prend plus que 5 valeurs (elle en prend 30 : 5 choix pour le signe $-$ et $6 = \binom{4}{2}$ pour les autres) et c'est absurde [30].

Le cas $\mu = 3$ se ramène au cas $\mu = 2$ en utilisant la somme des v_i.

Ensuite il montre :

3.27 Lemme. *Soit $v(x_1,\ldots,x_n)$ une fonction qui prend m valeurs distinctes quand on permute les x_i. Alors le polynôme minimal de v sur K est de degré m.*

29. Là, je ne comprends pas l'argument, peut-être faut-il supposer m assez grand ?

30. Au minimum cette démonstration est très compliquée, voire un peu incorrecte.

Démonstration. Appelons $v = v_1, \ldots, v_m$ les m valeurs de v. Le polynôme $(X - v_1) \cdots (X - v_m)$ est de degré m et il est invariant par permutation des x_i. Ses coefficients sont donc des fonctions symétriques des x_i, donc sont dans K. Inversement, si F est un polynôme de $K[X]$ tel que $F(v) = 0$, on voit, en permutant les x_i que F s'annule aussi en v_i donc est de degré $\geq m$. Voir aussi [9] Ch. 3.

3.4.4 Paragraphe IV : la fin de la preuve

On suppose $n = 5$. On reprend l'extension $L = K(x_1, \ldots, x_5)$, qui est de degré 120 sur K. On suppose P résoluble par radicaux. On a vu qu'alors l'extension est radicale, c'est-à-dire que le corps L est en haut d'une tour d'extensions engendrés par des radicaux d'ordre premier. On regarde le premier étage de cette tour, $K \subset K(\alpha)$, avec $\alpha^p = a \in K$ et $\alpha \notin K$. La fonction α prend alors p valeurs [31] et p est un diviseur premier de 120, donc $p = 2, 3$ ou 5 et le cas 3 est exclu par Cauchy.

Supposons $p = 5$. Alors, le lemme 3.26 montre qu'on a $K(\alpha) = K(x_i)$. Mais, comme K contient les racines cinquièmes de 1, $K(\alpha)$ contient non seulement x_i, mais aussi tous ses conjugués (voir 3.20), donc L, et c'est absurde pour une raison de degré (une fonction de α ne prend que 5 valeurs, alors que [32] $x_1 + \zeta x_2 + \zeta^2 x_3 + \zeta^3 x_4 + \zeta^4 x_5$ en prend 120).

Supposons $p = 2$. On a vu en 3.24 qu'on a $K(\alpha) = K(\delta)$ où δ est la racine du discriminant. Le corps L, qui est de degré 120, est strictement plus grand que $K(\alpha)$, de sorte qu'il y a un étage suivant dans la tour : $K_1 \subset K_1(\beta)$ avec $\beta^p = b \in K_1$, donc $b = u + v\delta$ avec $u, v \in K$. Soit σ une permutation impaire des x_i et posons $\overline{\beta} = \sigma(\beta)$. On a $\sigma(\delta) = -\delta$, donc $\overline{\beta}^p = \sigma(b) = \overline{b} = u - v\delta$. Considérons $\beta\overline{\beta}$ qui est une racine p-ième de $u^2 - \delta^2 v^2$. Comme u, v et δ^2 sont des fonctions symétriques, $u^2 - \delta^2 v^2$ aussi et on voit que $\beta\overline{\beta}$ "prend p valeurs" (est de degré p sur K). On a donc $p = 2$ ou $p = 5$ et le cas $p = 5$ a été exclu ci-dessus. Il reste donc $p = 2$, mais alors β est de degré 4 sur K et c'est exclu par 3.23.

3.5 Que retenir d'Abel ?

D'abord, il faut rendre à Abel ce qui est à Abel, savoir le grand mérite d'avoir, le premier, montré l'impossibilité de la résolution par radicaux des équations de degré 5, même si certaines preuves nous semblent compliquées,

31. Si l'on préfère, α est de degré p sur K.

32. La fonction citée est celle utilisée par Abel mais on aurait pu prendre aussi bien $x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5$.

voire rapides. Dans ce paragraphe, nous replaçons son travail par rapport à Galois et dans la perspective des progrès ultérieurs de l'algèbre.

Par rapport à Galois, il reste quelques étapes à franchir.

• Le résultat d'Abel ne vaut que si les racines sont des indéterminées (ou au moins si le groupe de Galois est $\mathfrak{S}_n$). Le travail de Galois donnera des méthodes pour aborder le cas général.

• Abel suppose systématiquement la présence de racines de l'unité. Galois éclaircira cette condition en parlant d'adjonction de manière générale.

• Surtout, Abel reste dans la droite ligne de Lagrange et de Cauchy en utilisant de manière essentielle le nombre de valeurs que prend une fonction lorsqu'on permute les variables. Autrement dit, il s'intéresse aux orbites d'un groupe (ici le groupe symétrique). Galois apportera une révolution en pensant au groupe plus qu'à son opération, et en considérant d'autres groupes que le groupe symétrique tout entier.

• Enfin, Galois introduira (implicitement) une notion essentielle, celle de sous-groupe distingué, qui aurait bien simplifié la preuve d'Abel.

Par rapport aux mathématiciens modernes, plusieurs notions font cruellement défaut à Abel (même s'il arrive à s'en passer), ce sont celles de corps, avec ses accessoires (corps engendré, corps de décomposition, etc.) et celles d'espace vectoriel et de dimension. Sur ce thème, voir §7 ci-dessous.

3.6 Annexe : retour sur le paragraphe II

Dans cette annexe, on reprend l'analyse du résultat annoncé [33] par Abel : en présence de racines de l'unité, une extension normale et résoluble est radicale. Comme on l'a dit, la preuve d'Abel est imprécise et, sans doute, incomplète. On en donne ici une version moderne, moins brutale que celle de 3.8, mais qui utilise cependant la théorie de Galois de manière essentielle [34]. Le défaut de la méthode d'Abel provient d'une difficulté incontournable de la théorie des corps : le problème de la normalité des extensions. Le point principal, pour surmonter cette difficulté, est de généraliser le résultat 3.20 d'Abel qui fonctionne dans le cas d'un groupe de Galois $\mathbf{Z}/p\mathbf{Z}$ à un groupe $(\mathbf{Z}/p\mathbf{Z})^m$, voir 3.31 ci-dessous.

3.6.1 Structure des extensions radicales

Rappelons qu'une clôture normale d'une extension $K \subset L$ est une extension $K \subset L \subset M$ telle que M soit normale sur K et minimale pour cette propriété. Les clôtures normales de L sont toutes isomorphes et on peut les

33. Voir 3.7 pour une formulation plus proche de celle d'Abel.

34. Je ne sais pas, sans ce recours, écrire de manière rigoureuse la preuve d'Abel.

construire comme suit. Si $L = K(x_1, \ldots, x_m)$, si l'on appelle P_i le polynôme minimal de x_i sur K et si l'on pose $P = P_1 \cdots P_m$, une clôture normale est un corps de décomposition $M = D_K(P)$.

Le résultat suivant est très important et sera utilisé aussi dans le paragraphe qui concerne Galois :

3.28 Théorème. *Soit $K \subset L$ une extension radicale. Cela signifie (cf. 3.3) qu'il existe une tour $K = K_0 \subset K_1 \subset \cdots \subset K_{n-1} \subset K_n = L$ avec $K_{i+1} = K_i(\alpha_i)$ où α_i vérifie $\alpha_i^{p_i} = a_i \in K_i$ avec des p_i premiers.*

Alors il existe une tour d'extensions $K = M_0 \subset M_1 \subset M_{n-1} \subset M_n = M$ vérifiant les propriétés suivantes :

1) Chaque M_i est une clôture normale de K_i sur K, de sorte que les extensions $K \subset M_i$ sont toutes **normales** *(et, a fortiori, les extensions $M_i \subset M_{i+1}$).*

2) Pour chaque $i = 0, \ldots, n-1$ on a $M_{i+1} = M_i(\alpha_{i,1}, \ldots, \alpha_{i,m_i})$ avec $\alpha_{i,k}^{p_i} = a_{i,k}$, $a_{i,k} \in M_i$, $\alpha_{i,k} \notin M_i$. On a $a_{i,1} = a_i$, $\alpha_{i,1} = \alpha_i$ et les $a_{i,k}$, pour i fixé, sont tous conjugués sur K. En particulier les extensions M_i sont toutes radicales sur K.

3) Le groupe de Galois de M_{i+1} sur M_i est de la forme $(\mathbf{Z}/p_i\mathbf{Z})^{m'_i}$ avec $m'_i \leq m_i$.

Démonstration. On raisonne par récurrence sur le nombre n d'étages de la tour. Pour $n = 0$ on a $K = L = M$ et le résultat est évident. Supposons donc le résultat établi pour $n - 1 \geq 0$ et passons à n. Posons $\alpha = \alpha_n$. On a $L = K_{n-1}(\alpha)$ avec $\alpha^p = a \in K_{n-1}$. Par l'hypothèse de récurrence on a une tour $K = M_0 \subset \cdots \subset M_{n-1}$ avec M_{n-1} normale et radicale qui s'écrit $M_{n-1} = D_K(Q)$

Soit P le polynôme minimal [35] de α sur K. On pose $M_n = M = D_K(PQ)$, de sorte que M_{n-1} se plonge dans M. Si $\alpha = \alpha_1, \ldots, \alpha_m$ sont les racines de P dans M, on a $M = M_{n-1}(\alpha_1, \ldots, \alpha_m)$. Comme le groupe de Galois $G := \mathrm{Gal}(M/K)$ opère transitivement sur les α_k (voir [10] 9.14), il existe $g_k \in G$ tel que $g_k(\alpha) = \alpha_k$. On a donc $\alpha_k^p = g_k(\alpha)^p = g_k(\alpha^p) = g_k(a)$ et comme a est dans M_{n-1} et que M_{n-1}/K est normale, le conjugué $a_k = g_k(a)$ est dans M_{n-1}. On voit que les α_k sont des radicaux d'éléments de M_{n-1}, de sorte que l'extension $M_{n-1} \subset M$ est radicale et donc aussi M/K en vertu de 3.6.

Il reste la description du groupe de Galois de M_n sur M_{n-1}. On peut supposer que a n'est pas une puissance p-ième dans M_{n-1} (sinon on a $M_n = M_{n-1}$ et le résultat est évident). Le polynôme $X^p - a$ est irréductible sur M_{n-1}

35. Attention, il faut prendre le polynôme minimal sur K sous peine de perdre des conjugués. C'est la fameuse difficulté qui concerne la normalité.

(voir 3.14) et comme M_n est normale sur M_{n-1}, toutes les racines p-ièmes de a sont dans M_n, donc aussi les racines p-ièmes de l'unité. Un élément de $\mathrm{Gal}(M_n/M_{n-1})$ fixe a_k, donc envoie α_k sur $\zeta^{r_k}\alpha_k$ avec $\zeta^p = 1$ et $r_k \in \mathbf{Z}/p\mathbf{Z}$. On a ainsi un homomorphisme $\varphi : \mathrm{Gal}(M_n/M_{n-1}) \to (\mathbf{Z}/p\mathbf{Z})^m$, injectif car les α_k engendrent M_n. Le résultat s'ensuit.

3.29 *Remarque.* Attention, l'homomorphisme φ n'est pas nécessairement surjectif comme en témoigne l'exemple suivant : $K = \mathbf{Q}$, $M_1 = \mathbf{Q}(\sqrt{3})$, $a_1 = 2 + \sqrt{3}$, $a_2 = 2 - \sqrt{3}$. Comme on a $(2 + \sqrt{3})(2 - \sqrt{3}) = 1$ l'extension $M_1(\alpha_1, \alpha_2)$ avec $\alpha_k^2 = a_k$ est seulement de degré 2 sur M_1.

3.6.2 Le point crucial de la preuve d'Abel

Il s'agit du résultat 3.20 que je redis en termes modernes :

3.30 Lemme. *Soit p un nombre premier, K un corps contenant les racines p-ièmes de l'unité, $L = D_K(P)$ une extension normale de K, distincte de K. On suppose $L \subset M = K(\alpha)$ où α vérifie $\alpha^p = a$, $a \in K$ et $\alpha \notin K$. Alors, on a $\alpha \in L$ (et donc $L = M$).*

Démonstration. Bien sûr, avec les notions d'espace vectoriel et de dimension, le résultat est trivial. En effet, le degré de M sur K est égal à p, premier, de sorte que l'extension intermédiaire L est de degré 1 ou p, donc p, donc est égale à M. Nous aurons cependant besoin d'une preuve plus explicite de ce résultat.

On appelle $x_1, \ldots, x_n$ les racines de P. On écrit $x_1 = a_0 + a_1\alpha + \cdots + a_{p-1}\alpha^{p-1}$ avec $a_i \in K$. Le groupe de Galois de M sur K est cyclique, isomorphe à $\mathbf{Z}/p\mathbf{Z}$, engendré par τ défini par $\tau(\alpha) = \zeta\alpha$ où ζ est une racine p-ième primitive de 1. Alors, les $\tau^i(x_1)$ sont racines de P et l'on a :

$$x_i = \tau^i(x_1) = a_0 + a_1\zeta^i\alpha + \cdots + a_{p-1}\zeta^{(p-1)i}\alpha^{p-1}.$$

On a donc un système d'équations qui donne les x_i en fonction des puissances de α. Tout le problème est d'inverser ce système. Il y a deux voies :

• **La voie Abel**

Voir 3.20. Elle consiste à montrer que l'on peut supposer $a_1 = 1$, quitte à modifier α. Alors, les $a_i\alpha^i$ sont solutions d'un système de type Vandermonde, donc on peut les calculer à partir des x_i. Comme $a_1\alpha$ n'est autre que α, on a gagné.

• **La voie Lagrange**

Comme Abel, on peut supposer $a_1 \neq 0$. On résout explicitement le système en calculant la somme des $\zeta^{-i}x_i$. On voit que tous les termes s'en

vont ou presque et l'on a $\sum_{i=0}^{p-1} \zeta^{-i} x_i = p a_1 \alpha$. On en déduit que α est dans L. On voit que les deux méthodes sont très voisines, la deuxième méthode donnant une solution explicite en utilisant les résolvantes de Lagrange.

3.6.3 Généralisation de la méthode d'Abel

On a vu en 3.30 que la preuve d'Abel de 3.20 revient essentiellement à montrer qu'une extension dont le groupe de Galois est $\mathbf{Z}/p\mathbf{Z}$ est engendrée par un radical. En fait, ce qui est nécessaire pour poursuivre cette preuve et montrer 3.21 est le résultat suivant :

3.31 Proposition. *Soit K un corps contenant suffisamment de racines de l'unité et soit M une extension galoisienne de K, de groupe de Galois $H = (\mathbf{Z}/p\mathbf{Z})^m$ avec p premier et $m \geq 1$. Alors l'extension $K \subset M$ est radicale.*

Démonstration. Comme l'extension $K \subset M$ est galoisienne de groupe H, on a $K = M^H$. On note $\tau_1, \ldots, \tau_m$ les éléments de H correspondant aux éléments $(1, 0, \ldots, 0)$ etc. de $(\mathbf{Z}/p\mathbf{Z})$. Appelons N le sous-corps de M invariant par $\tau_2, \ldots, \tau_m$. Il contient K et le groupe de Galois $\mathrm{Gal}(N/K)$ est le groupe cyclique engendré par τ_1. Soit $x \in N$, $x \notin K$, donc x non invariant par τ_1. L'élément $x_0 := x + \tau_1(x) + \cdots + \tau_1^{p-1}(x)$ est invariant par τ_1. Mais comme x est invariant par les τ_i, $i \geq 2$ et que les τ_i commutent à τ_1, x_0 est aussi invariant par τ_i, donc est dans K. Quitte à remplacer x par $x - x_0/p$ (qui n'est pas dans K) on peut supposer $x_0 = 0$.

On considère alors les résolvantes de Lagrange [36] $\beta_k := x + \zeta^k \tau_1(x) + \cdots + \zeta^{k(p-1)} \tau_1^{p-1}(x)$ qui sont dans N. On a $\tau_1(\beta_k) = \zeta^{-k} \beta_k$ et il en résulte qu'on a $\tau_1(\beta_k^p) = \beta_k^p$, de sorte que $b_k = \beta_k^p$ est invariant par τ_1. Par le même argument que ci-dessus, il est aussi invariant par les autres τ_i, donc est dans K. Si l'on montre que l'un des β_k n'est pas dans K, comme l'extension $K \subset N$ est de degré p premier, on aura $N = K(\beta_k)$. Comme on a $\tau_1(\beta_k) = \zeta^{-k} \beta_k$, il suffit de montrer que l'un des β_k n'est pas nul.

Mais, si toutes les résolvantes de Lagrange sont nulles, le système d'équations (on a posé $\tau = \tau_1$) :

$$x + \tau(x) + \cdots + \tau^{p-1}(x) = 0$$

$$x + \zeta\tau(x) + \cdots + \zeta^{p-1}\tau^{p-1}(x) = 0$$

$$x + \zeta^2\tau(x) + \cdots + \zeta^{2(p-1)}\tau^{p-1}(x) = 0$$

$$\ldots$$

36. On retrouve un des protagonistes de notre histoire.

$$x + \zeta^{p-1}\tau(x) + \cdots + \zeta^{(p-1)^2}\tau^{p-1}(x) = 0$$

admet la solution non nulle $x, \tau(x), \ldots, \tau^{p-1}(x)$, ce qui implique que son déterminant est nul. Or, ce déterminant est le déterminant de Van der Monde [37] associé à $1, \zeta, \ldots, \zeta^{p-1}$ qui est non nul !

Si l'on définit α_1 comme l'un des β_k non nul on a $N = K(\alpha_1)$ et $a_1 = \alpha_1^p$ est dans K.

On construit les α_i, $i \geq 2$ de la même manière. Chaque α_i est invariant par les τ_j, $j \neq i$, mais pas par τ_i. Il en résulte que les corps $K(\alpha_i)$ se coupent seulement sur K et que le corps M est engendré par les α_i.

3.6.4 Rectification de la preuve d'Abel

On peut maintenant prouver le résultat d'Abel :

3.32 Théorème. *Soit K un corps contenant suffisamment de racines de l'unité et L une extension normale et résoluble de K. Alors L est radicale sur K.*

Démonstration. On raisonne par récurrence sur le degré de L sur K, le cas $n = 1$ étant trivial.

Comme L est résoluble, elle est plongée dans une extension radicale, que l'on peut supposer normale en vertu de 3.28 et que l'on suppose minimale pour cette propriété. En vertu de 3.28 on a une tour d'extensions normales et radicales $M_0 = K \subset M_1 \subset \cdots \subset M_{n-1} \subset M_n$ et on peut supposer $M_{n-1} \neq M_n$, de sorte que L n'est pas contenue dans M_{n-1}. Toujours par 3.28, on sait que le groupe de Galois $H_0 := \mathrm{Gal}(M/M_{n-1})$ est isomorphe à $(\mathbf{Z}/p\mathbf{Z})^{m'}$.

Comme L est une sous-extension normale de M, le groupe $\mathrm{Gal}(L/K)$ est un quotient de $G := \mathrm{Gal}(M/K)$, de noyau $H' = \mathrm{Gal}(M/L)$ et H' est distingué dans G. L'image de H_0 dans $\mathrm{Gal}(L/K)$ n'est pas triviale (sinon on aurait $H_0 \subset H'$, donc $L \subset M_{n-1}$). C'est donc un sous-groupe distingué H de $\mathrm{Gal}(L/K)$, de la forme $(\mathbf{Z}/p\mathbf{Z})^m$. On considère alors $L' = L^H$. C'est un sous-corps strict de L, $K \subset L'$ est résoluble, donc radicale par l'hypothèse de récurrence. Mais $L' \subset L$ est radicale en vertu de 3.31, donc L/K est radicale.

37. Et en voici un autre.

4 Introduction aux mémoires de Galois

4.1 Les textes

Nous en arrivons au personnage principal de l'histoire, celui dont le nom est devenu synonyme de la théorie des équations, Évariste Galois (1811-1832). Durant sa brève et romantique existence [38], celui-ci parvient essentiellement à résoudre le problème de la résolubilité par radicaux des équations et introduit pour cela, parfois de manière implicite, des notions nouvelles, dont l'importance s'avérera capitale. Les œuvres de Galois sont évidemment limitées et nous nous intéresserons à trois d'entre elles qui portent sur le sujet des équations, voir [4] :

• Le "premier mémoire", intitulé *Sur les conditions de résolubilité des équations par radicaux*, soumis à l'Académie des sciences en 1830 et rejeté par celle-ci, que Galois reprend en janvier 1831. Il traite essentiellement des équations de degré premier.

• Le "second mémoire", en fait un fragment de mémoire, qui traite des équations primitives résolubles par radicaux.

• La "lettre de la veille", écrite à son ami Auguste Chevalier le 29 mai 1832, la veille de sa mort tragique en duel. C'est un texte absolument extraordinaire, qui renferme nombre d'idées fulgurantes, à peine ébauchées, mais qui justifient que le nom de Galois ait pris une telle place dans les mathématiques.

Dans ce texte j'étudie principalement le premier mémoire et un peu la lettre de la veille. Pour le second mémoire, voir Annexe 2, §9. Je suppose que le lecteur connaît les rudiments de théorie des corps et de théorie de Galois, pour lesquels je le renvoie à [9], [11], [5]. Une première approche rapide pourra être trouvée dans [10].

4.2 Une citation

La citation suivante de Galois, qui figure dans l'introduction aux deux mémoires évoqués ci-dessus, est emblématique de la modernité de sa pensée :

Depuis Euler les calculs sont devenus de plus en plus nécessaires et aussi de plus en plus difficiles à mesure qu'ils s'appliquaient à des objets de science plus avancés. Dès le commencement de ce siècle, l'algorithme avait atteint un degré de complication tel que tout progrès était devenu impossible par ce moyen, sans l'élégance que les géomètres modernes ont dû imprimer à leurs recherches et au moyen de laquelle l'esprit saisit promptement et d'un seul coup un grand nombre d'opérations.

38. Ce n'est pas mon propos de revenir sur cet aspect, que l'on trouvera partout.

Or je crois que les simplifications produites par l'élégance des calculs (simplifications intellectuelles s'entend, de matérielle il n'y en a pas) ont leurs limites ; je crois que le moment arrivera où les transformations algébriques prévues par les spéculations des analystes ne trouveront ni le temps ni la place de se produire ; à tel point qu'il faudra se contenter de les avoir prévues. Je ne veux pas dire qu'il n'y a plus rien de nouveau pour l'analyse sans ce secours : mais je crois qu'un jour sans cela tout serait épuisé.

Et il ajoute une sorte de profession de foi :

Sauter à pieds joints sur les calculs ; grouper les opérations, les classer suivant leurs difficultés et non suivant leurs formes ; telle est, suivant moi, la mission des géomètres futurs ; telle est la voie où je suis entré dans cet ouvrage.

4.3 Le rôle des permutations

Avant d'étudier le premier mémoire, essayons de comprendre l'un des outils essentiels introduits par Galois, à savoir le groupe qui porte son nom. Il faut pour cela revenir à la problématique de Lagrange, voir §2.2.2 : étant donnée une équation algébrique $P(x) = 0$ à coefficients dans K, de racines $x_1, \ldots, x_n$, on cherche à exprimer les x_i en fonction des racines $y_1, \ldots, y_m$ d'une équation auxiliaire (dite "réduite") $Q(y) = 0$, aussi à coefficients dans K, avec $m = \deg Q < n = \deg P$ (sinon, on n'a pas avancé d'un pouce). Dans le cas de l'équation de degré 3, les y_j sont les quantités u^3 et v^3 qui sont racines d'une équation du second degré à coefficients dans K et dont les racines cubiques u et v permettent d'exprimer rationnellement les x_i (par les formules $x_1 = u + v$, $x_2 = j^2u + jv$ et $x_3 = ju + j^2v$).

On cherche les y_j dans le corps des racines $L = K(x_1, \ldots, x_n)$ donc sous la forme $y_j = f_j(x_1, \ldots, x_n)$ où f_j est une fonction rationnelle. Les permutations des x_i vont alors induire des permutations des y_j et le degré de l'équation vérifiée par les y_j est égal au nombre de "valeurs" prises par les y_j ou encore au nombre total de permutations divisé par le cardinal de celles qui laissent y_j invariant [39]. Par exemple, pour une équation de degré 5, on peut considérer l'élément :

$$u = (x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1) - (x_1x_3 + x_2x_4 + x_3x_5 + x_4x_1 + x_5x_2)$$

qui est invariant par les permutations (12345) et (25)(34). L'argument qui conduit Lagrange à penser que l'équation générale de degré 5 n'est pas résoluble par radicaux est que le degré de l'élément u est encore plus grand

39. En termes modernes, le cardinal de l'orbite est le quotient du cardinal du groupe par celui du stabilisateur.

que 5. Cet argument est parfaitement valable si toutes les permutations de cinq lettres sont pertinentes (c'est le cas étudié par Abel). Par exemple, dans le cas $P(X) = X^5 + pX + q$ l'équation vérifiée par u est :

$$R(X) = X^6 - 20pX^4 + 240p^2X^2 - 32\delta X + 320p^3$$

où δ est la racine carrée du discriminant Δ de l'équation, de sorte que u est racine d'un polynôme de degré 6 ou 12 (selon que Δ est, ou non, un carré de K) à coefficients dans le corps de base. On voit que cette équation est de degré > 5. Dans le cas d'une équation "générale" [40], le polynôme R est irréductible, mais il peut ne pas l'être dans certains cas. Ainsi, si l'on regarde l'équation $X^5 - 5X + 12$, on a $\delta = 8000$ et l'équation R admet la racine rationnelle $u = 10$ et cette remarque permet de résoudre cette équation par radicaux, voir [10]§7. Cet exemple est intéressant car il comporte trois caractéristiques qui témoignent que l'équation n'est pas générale :

• On peut la résoudre par radicaux, contrairement au résultat d'Abel.

• Les racines sont liées par une relation supplémentaire (à côté des relations triviales liant racines et coefficients), à savoir $u = 10$.

• Seules les permutations des x_i qui conservent cette relation doivent être considérées, les autres n'ayant pas de sens par rapport à l'équation. Cette idée est exactement celle du groupe de Galois : parmi les permutations des racines, toutes ne sont pas pertinentes, seules le sont celles qui conservent les relations entre les racines.

4.4 Relations entre les racines et groupe de Galois

4.4.1 Relations entre les racines d'un polynôme : une approche théorique

On considère un polynôme $P(X) = X^n - a_1X^{n-1} + \cdots + (-1)^{n-1}a_{n-1}X + (-1)^n a_n$ à coefficients dans un corps [41] K et son corps de décomposition $L = D_K(P) = K(x_1, \ldots, x_n)$ où les x_i sont les racines de P. On sait que L est aussi égal à l'anneau engendré $K[x_1, \ldots, x_n]$. On a un donc homomorphisme surjectif d'anneaux $\Phi : R = K[X_1, \ldots, X_n] \to L$, qui à X_i associe x_i. Son noyau $\mathfrak{M}$ est un idéal maximal qui décrit les relations entre les x_i.

L'homomorphisme Φ s'étend de manière évidente en $\widehat{\Phi} : R[X] \to L[X]$ et l'image du polynôme générique :

$$\mathbf{P}(X) = \prod_{i=1}^{n}(X - X_i) = X^n + \sum_{i=1}^{n}(-1)^i\Sigma_i(X_1, \ldots, X_n)X^{n-i}$$

40. Ici cela signifie, en anticipant, que le groupe de Galois de P est le groupe symétrique tout entier.

41. Disons de caractéristique 0.

(où les Σ_i sont les polynômes symétriques élémentaires) est égale à P.

L'idéal $\mathfrak{M}$ contient déjà les polynômes $P(X_i)$ et $\Sigma_i(X_1,\ldots,X_n)-a_i$ correspondant aux relations évidentes $P(x_i)=0$ et $\Sigma_i(x_1,\ldots,x_n)=a_i$. Appelons I l'idéal engendré par les $\Sigma_i(X_1,\ldots,X_n)-a_i$ et posons $A=R/I$. On note déjà que les relations $P(x_i)=0$ sont superflues :

4.1 Proposition. *Les polynômes $P(X_i)$ sont dans l'idéal I.*

Démonstration. Notons $\overline{X_i}$ l'image de X_i dans A. Dans $A[X]$ on a $\overline{\mathbf{P}(X)}=P(X)$ car Σ_i est égal à a_i dans A. Mais, comme $\mathbf{P}(X_i)=0$ dans R, *a fortiori* on a $P(\overline{X_i})=0$ dans A, donc $P(X_i)$ est dans I.

4.2 Proposition. *Avec les notations précédentes, l'anneau $A=R/I$ est un K-espace vectoriel de dimension $n!$.*

Démonstration. Voir [10] th. 8.4.

4.3 *Remarque.* La proposition précédente montre que l'idéal I n'est pas l'idéal engendré par les $P(X_i)$. En effet, A est un K-espace vectoriel de dimension $n!$ alors que le quotient B de R par l'idéal J engendré par les $P(X_i)$ est de dimension n^n (par division euclidienne, on voit qu'une base de R/J est formée des $\overline{X_1}^{\alpha_1}\cdots\overline{X_n}^{\alpha_n}$ avec $0\leq\alpha_i\leq n-1$).

4.4 Corollaire. *Le corps L est de degré*[42] *$n!$ sur K si et seulement si l'idéal $\mathfrak{M}$ est égal à I i.e. s'il n'y a pas de relations entre les x_i autres que les triviales.*

Démonstration. On a l'homomorphisme surjectif $\psi: A=R/I\to L=R/\mathfrak{M}$ et, comme A est de dimension $n!$ sur K, L est de degré $n!$ si et seulement si ψ est un isomorphisme autrement dit si $\mathfrak{M}=I$.

4.4.2 Les relations et le groupe de Galois

On note qu'une permutation σ de l'ensemble $\{1,2,\ldots,n\}$ définit un automorphisme u_σ (qu'on dira associé à σ) de l'anneau $R=K[X_1,\ldots,X_n]$ en posant $u_\sigma(\lambda)=\lambda$ pour $\lambda\in K$ et $u_\sigma(X_i)=X_{\sigma(i)}$. On peut alors expliciter le lien entre l'idéal des relations et le groupe de Galois :

4.5 Proposition-Définition. *Les deux groupes suivants sont isomorphes :*

1) Le groupe des K-automorphismes[43] *d'anneaux de R associés à une permutation des X_i, qui laissent stable l'idéal $\mathfrak{M}$.*

2) Le groupe des K-automorphismes de corps de L.

Ce groupe est appelé le **groupe de Galois** *de L sur K et noté* $\mathrm{Gal}(L/K)$.

42. Il en résulte que son groupe de Galois est $\mathfrak{S}_n$, voir [10].

43. C'est-à-dire des automorphismes qui fixent les éléments de K.

Démonstration. Soit u un K-automorphisme de R qui laisse stable $\mathfrak{M}$. Il induit un automorphisme $\overline{u}$ de $L = R/\mathfrak{M}$ qui fixe K. Inversement, si on a un automorphisme g de L qui fixe K, il permute les x_i (appelons encore g la permutation), donc définit un automorphisme $\widehat{g}$ de R. Soit $F(X_1, \ldots, X_n)$ un élément de $\mathfrak{M}$. On a $F(x_1, \ldots, x_n) = 0$ dans L, donc aussi $F(x_{g(1)}, \ldots, x_{g(n)}) = 0$ car g est un homomorphisme de corps, mais cet élément est l'image de $\widehat{g}(F(X_1, \ldots, X_n))$ et ce polynôme est donc dans $\mathfrak{M}$.

4.6 *Remarque.* Attention, il y a d'autres automorphismes de R que ceux associés aux permutations.

4.7 Scolie. *On voit que le groupe de Galois de L sur K est formé des permutations qui conservent les relations polynomiales entre les racines (définies par l'idéal $\mathfrak{M}$). Parmi ces relations il y a les relations triviales mais il peut y en avoir d'autres, auquel cas le groupe de Galois est strictement plus petit que $\mathfrak{S}_n$.*

4.4.3 Exemple 1 : groupe symétrique ou alterné

On a vu qu'une équation de groupe $\mathfrak{S}_n$ est caractérisée par le fait qu'il n'y a pas d'autres relations que les triviales entre les racines. Par exemple, comme le groupe de Galois de l'équation $x^4 - x - 1 = 0$ est $\mathfrak{S}_4$, les seules relations entre les 4 racines sont les triviales : $x_1+x_2+x_3+x_4 = 0$, $x_1x_2+\cdots+x_3x_4 = 0$, $x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 = 1$ et $x_1x_2x_3x_4 = -1$.

Pour le groupe alterné, il y a juste une relation supplémentaire, qui exprime que le discriminant Δ est un carré dans K et qui s'écrit alors $\prod_{i<j}(x_i - x_j) = \delta = \sqrt{\Delta}$.

4.4.4 Exemple 2 : l'extension cyclotomique d'ordre 5

Considérons l'exemple de l'extension cyclotomique $\mathbf{Q} \subset \mathbf{Q}(\zeta)$ avec $\zeta^5 = 1$. Il y a quatre racines primitives $x_1 = \zeta$, $x_2 = \zeta^2$, $x_3 = \zeta^{-2}$ et $x_4 = \zeta^{-1}$. En plus des relations triviales on a, par exemple, $x_1x_4 = 1$ et $x_2x_3 = 1$. On peut calculer l'idéal $\mathfrak{M}$:

4.8 Proposition. *L'idéal $\mathfrak{M}$ des relations est engendré par l'idéal I des relations triviales et par les deux éléments $X_1X_4 - 1$ et $X_1^2 - X_2$.*

Démonstration. Appelons J l'idéal engendré par les éléments indiqués. Il est clair qu'on a $J \subset \mathfrak{M}$. Si l'on pose $B = R/J$ on a un homomorphisme surjectif de B sur L. Appelons $\overline{X_i}$ les images des X_i dans B. Il suffit de montrer que $1, \overline{X_1}, \overline{X_1}^2, \overline{X_1}^3$ et $\overline{X_1}^4$ engendrent B comme K-espace vectoriel et on conclura par un argument de dimension que B est isomorphe à L.

Mais les relations triviales donnent $\overline{X_1}^5 = 1$ et les autres donnent $\overline{X_2} = \overline{X_1}^2$, puis $\overline{X_4} = 1/\overline{X_1} = \overline{X_1}^4$. Comme on a aussi $\overline{X_1X_2X_3X_4} = 1$, on en déduit $\overline{X_2X_3} = 1$, donc $\overline{X_3} = \overline{X_1}^3$.

Une fois listées ces relations, on peut déterminer le groupe : parmi les permutations, seules celles qui conservent $\mathfrak{M}$ sont acceptables. Ici, on voit qu'on peut envoyer x_1 sur n'importe quel x_i mais qu'alors les images des autres sont déterminées. On obtient le groupe $\mathbf{Z}/4\mathbf{Z}$ engendré par (1243).

4.4.5 Exemple 3 : l'équation $x^4 - 2 = 0$

Elle admet les racines $x_1 = \sqrt[4]{2} := \alpha$, $x_2 = ix_1 = i\alpha$, $x_3 = -x_1 = -\alpha$ et $x_4 = -ix_1 = -i\alpha$. On a les relations $x_1 + x_3 = 0$, $x_2 + x_4 = 0$. Le corps $D_{\mathbf{Q}}(X^4 - 2)$ est égal à $\mathbf{Q}(i, \alpha)$.

4.9 Proposition. *Le groupe de Galois conserve la partition*[44] $\{1,3\}\cup\{2,4\}$. *C'est le groupe diédral, engendré*[45] *par* (1234) *et par* (24) *(conjugaison complexe). Précisément, le groupe contient l'identité et les permutations* (1234), (13)(24) *et* (1432) *(rotations*[46]*) et* (12)(34), (14)(23), (13) *et* (24) *(symétries).*

Démonstration. Soit σ conservant la partition. Quitte à composer par (12)(34) on peut supposer que σ conserve à la fois $\{1,3\}$ et $\{2,4\}$. Quitte à composer avec (13) on peut supposer qu'il fixe 1 et 3. Il ne reste que deux possibilités : Id et (24).

4.10 *Remarques.* 1) Il y a *a priori* une autre relation : $x_1^2 + x_2^2 = 0$. Mais elle est conséquence de $x_3 = -x_1$. En effet, de la nullité des deux premières fonctions symétriques on déduit $x_1^2+x_2^2+x_3^2+x_4^2 = 0$, d'où $x_1^2+x_2^2 = -x_3^2-x_4^2$. Mais on a aussi $x_1^2 = x_3^2$ et $x_2^2 = x_4^2$, d'où le résultat.

2) On note que, bien que l'équation soit résoluble par radicaux, $\mathbf{Q}(x_1, x_3)$ n'est pas égal à L contrairement à ce qui se passe dans le cas étudié par Galois[47], cf. 5.1.

On peut expliciter un élément primitif (le calcul a été effectué avec le logiciel *xcas*) :

4.11 Proposition. *1) Une base sur* $\mathbf{Q}$ *de* $D_{\mathbf{Q}}(X^4-2)$ *est formée des éléments* $1, \alpha, \sqrt{2}, \alpha\sqrt{2}, i, i\alpha, i\sqrt{2}, i\alpha\sqrt{2}$.

44. Il est donc non primitif.

45. Cet automorphisme est défini sur $\mathbf{Q}(i)$ par $\alpha \mapsto i\alpha$. Attention, la multiplication par un scalaire $\neq 1$ n'est jamais un automorphisme de corps !

46. On notera que les rotations ne coïncident pas avec les permutations paires.

47. Pas de doute : 4 n'est pas premier !

2) Soit $x = \alpha+i$. On a $D_{\mathbf{Q}}(X^4-2) = \mathbf{Q}(x)$. On a les formules suivantes :

$$x^2 = -1+\sqrt{2}+2i\alpha, \quad x^3 = -3\alpha+\alpha\sqrt{2}-i+3i\sqrt{2}, \quad x^4 = 3-6\sqrt{2}-4i\alpha+4i\alpha\sqrt{2},$$

$$x^5 = 7\alpha - 10\alpha\sqrt{2} + 11i - 10i\sqrt{2}, \quad x^6 = -31 + 17\sqrt{2} + 18i\alpha - 20i\alpha\sqrt{2},$$

$$x^7 = -49\alpha + 37\alpha\sqrt{2} - 71i + 35i\sqrt{2}, \quad x^8 = 145 - 84\sqrt{2} - 120i\alpha + 72i\alpha\sqrt{2}.$$

On a l'équation :

$$x^8 = -1 - 28x^2 - 2x^4 - 4x^6.$$

Les nombres α et $i\alpha$ se calculent à partir de x :

$$\alpha = F(x) := \frac{151}{24}x + \frac{5}{24}x^3 + \frac{19}{24}x^5 + \frac{5}{24}x^7,$$

$$i\alpha = \frac{29}{24} + \frac{13}{24}x^2 + \frac{5}{24}x^4 + \frac{1}{24}x^6.$$

3) Les conjugués de x sont $\alpha + i$, $\alpha - i$, $i\alpha + i$, $i\alpha - i$, $-\alpha + i$, $-\alpha - i$, $-i\alpha + i$ et $-i\alpha - i$. Ils correspondent aux huit éléments du groupe de Galois, respectivement à Id, (24), (1234), (12)(34), (13)(24), (13), (1432) *et* (14)(23).

L'élément du groupe de Galois qui transforme $\alpha + i$ en $\alpha - i$ consiste à fixer α et à changer i en $-i$. Il fixe donc α et $-\alpha$ et échange $i\alpha$ et $-i\alpha$, c'est la transposition (24).

4.12 *Remarques.* 1) Cet exemple permet d'éclaircir la notion de "valeurs prises par une fonction" chère à Abel, Cauchy, etc. Rappelons qu'une fonction des x_i est un élément x de $\mathbf{Q}(x_1, \ldots, x_4)$. Pour les valeurs de x, il y a deux notions *a priori*. La bonne c'est que les valeurs de x sont les conjugués de x (i.e. ses transformés par le groupe de Galois). Mais il y a une autre possibilité qui est de regarder les transformés de x par **toutes** les permutations. Ce n'est pas la même chose. Ici, si l'on regarde $x = \alpha+i = x_1+\dfrac{x_2}{x_1}$, on a 8 transformés par le groupe de Galois, mais si l'on applique la transposition $\sigma = (14)$ on a $\sigma(x) = x_4 + x_2/x_4 = -i\alpha - 1$ qui n'est pas un conjugué. Cet exemple est un peu subtil car certains transformés par des permutations qui ne sont pas dans Galois sont tout de même des conjugués. Par exemple c'est le cas avec (12). En fait, c'est normal, car le stabilisateur de x contient (34), donc les transformés de x par les $\tau(34)$ avec τ dans Galois sont des conjugués. En particulier, on a $(12) = (12)(34) \circ (34)$. On note qu'on obtient seulement 4 valeurs avec les permutations restantes ($\alpha - 1, -\alpha - 1, i\alpha - 1$ et $-i\alpha - 1$).

2) Si l'on a un corps de décomposition $L = D_K(P) = K(x_1, \ldots, x_n)$, on pourrait être tenté de faire opérer le groupe $\mathfrak{S}_n$ sur L par la formule $\sigma(f(x_1, \ldots, x_n)) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$, mais si σ ne conserve pas les relations

entre les racines, cette définition n'a pas de sens. Ainsi, dans l'exemple de $X^4 - 2$ avec $\sigma = (12)$, l'image de $x_1 + x_3 = 0$ est-elle $x_2 + x_3 = \alpha(i-1)$ ou 0 ?

Il semble bien qu'avant Galois, les gens n'avaient pas une claire conscience qu'il fallait parfois éliminer certaines permutations. En tous cas Abel, qui travaille avec une extension générique, n'évoque rien de tel.

4.4.6 La définition de Galois

Voici la définition donnée par Galois (Proposition I, p. 421 du premier mémoire) :

4.13 Théorème. *Soit une équation donnée, dont $a, b, c, \ldots$ sont les m 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 ;

2) Réciproquement, que toute fonction des racines, déterminable rationnellement, soit invariable par les substitutions.

4.14 *Remarques.* 1) Galois n'explicite pas la conservation des relations par le groupe, mais elle est évidente. En effet, si l'on a $y := f(x_1, \ldots, x_n) = 0$ avec f polynomiale, si σ est une permutation du groupe elle transforme $f(x_1, \ldots, x_n)$ en $f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ et comme $y = 0$ est dans K on a $\sigma(y) = y = 0$, de sorte que σ conserve bien la relation.

2) Par exemple, dans le cas de l'équation $x^4 - 2 = 0$, la transposition $\tau = (12)$ n'est pas dans le groupe de Galois. En effet, si l'on considère la fonction des racines $x_1 + x_3$, elle est "déterminable rationnellement" comme dit Galois, puisqu'elle est nulle. Si τ était dans le groupe de Galois elle devrait donc être invariable par τ, ce qui n'est pas le cas puisque $\tau(x_1 + x_3) = x_2 + x_3 \neq 0$.

Voici la traduction moderne de ce théorème :

4.15 Théorème. *Soit $P \in K[X]$ de racines $x_1, \ldots, x_n \in L = K(x_1, \ldots, x_n)$. Il y a un sous-groupe G de $\mathfrak{S}_n$ qui opère sur L par automorphismes de corps et qui est tel que tout $y \in L$ fixe par G est dans K et réciproquement.*

C'est un des résultats de base de la théorie de Galois, voir par exemple [10] 9.13.

5 Le premier mémoire de Galois

Rappelons qu'il s'agit du mémoire intitulé : *Sur les conditions de résolubilité des équations par radicaux.*

5.1 Le résultat principal

Le théorème principal de cet article est le suivant :

5.1 Théorème. *Soient K un corps de caractéristique zéro*[48]*, $F \in K[X]$ un polynôme irréductible* **de degré** *p* **premier***, L son corps de décomposition, $x_1, \ldots, x_p$ ses racines dans L. L'équation $F(x) = 0$ est résoluble par radicaux si et seulement si l'on a, pour tous i, j, $L = K(x_i, x_j)$.*

Dans le cas des coefficients rationnels on en déduit un corollaire :

5.2 Corollaire. *Soit P un polynôme irréductible de degré p premier à coefficients rationnels. On suppose l'équation $P(x) = 0$ résoluble par radicaux. Alors, si P a deux racines réelles, elles le sont toutes.*

Variante : *Si P admet au moins deux racines réelles et au moins une racine non réelle, il n'est pas résoluble.*

Ce corollaire permet d'exhiber nombre d'équations de degré premier non résolubles par radicaux :

5.3 Théorème. *Soit p un nombre premier ≥ 5 et posons $P(X) = X^p - p^2X + p$. Alors, P est irréductible sur $\mathbf{Q}$ et l'équation $P(x) = 0$ n'est pas résoluble par radicaux.*

Démonstration. L'irréductibilité vient du critère d'Eisenstein. Pour l'assertion sur la solvabilité, il suffit de montrer que P admet exactement 3 racines réelles x_1, x_2, x_3. En effet, il a alors aussi des racines non réelles et le corps de décomposition de P n'est pas égal à $\mathbf{Q}(x_1, x_2) \subset \mathbf{R}$.

Pour cela, on note que $P'(X) = pX^{p-1} - p^2$ est une fonction décroissante puis croissante qui prend des valeurs négatives, de sorte que P croît, puis décroît, puis croît et n'a pas plus de trois racines réelles. Pour voir qu'il en a trois on note, outre les valeurs à l'infini, qu'on a $P(0) = p > 0$ et $P(1) = p + 1 - p^2 < p + 1 - 2p < 0$.

5.4 *Exemple.* Plus généralement, l'équation $f(x) = x^p + ax + b$, avec $a, b \in \mathbf{Q}$ et p premier ≥ 5, si elle est irréductible, ne sera pas résoluble si $a < 0$, $b > 0$ et $-a > 1 + b$. En effet, la dérivée est positive, puis négative, puis positive, de sorte qu'il y a au plus trois racines réelles et il y en a trois car $f(0) = b > 0$ et $f(1) = 1 + a + b < 0$.

5.5 *Remarque.* L'hypothèse que p est premier est indispensable pour le sens direct de 5.1. Par exemple, si $F(X) = X^4 - X - 1 \in \mathbf{Q}[X]$, le groupe de Galois de F est $\mathfrak{S}_4$ donc le corps L est de degré 24 sur $\mathbf{Q}$. L'équation est résoluble et pourtant le corps $\mathbf{Q}(x_1, x_2)$ est de degré 12, donc strictement plus petit que L. Pour un contre-exemple à la réciproque, voir ci-dessous 5.19.

48. Nous garderons cette hypothèse tout au long de ce texte.

5.2 Une preuve moderne du résultat de Galois

Comme dans le cas d'Abel, nous commençons par donner une preuve actuelle du théorème, mais en restant le plus possible fidèle à la ligne de démonstration de Galois. Nous reviendrons dans les paragraphes suivants sur ce que fait exactement Galois.

On renvoie à 3.3 ci-dessus pour la définition des extensions radicales.

5.2.1 Un mot sur les extensions normales

Une des notions essentielles de la théorie de Galois est celle d'extension normale, voir [10] ou [11]. Rappelons la propriété caractéristique de ces extensions :

5.6 Proposition. *Une extension $K \subset M$ est normale*[49] *si et seulement si M est le corps de décomposition d'un polynôme à coefficients dans K.*

Le théorème essentiel est alors le suivant :

5.7 Théorème. *Soit $K \subset L$ une extension normale et $K \subset M \subset L$ une extension intermédiaire. Posons $G = \mathrm{Gal}(L/K)$ et $H = \mathrm{Gal}(L/M)$ (c'est un sous-groupe de G). Alors, si M/K est normale, on a les propriétés suivantes :*

1) On a $g(M) = M$ pour tout $g \in G$.

2) Le sous-groupe H est distingué dans G.

Démonstration. 1) On écrit $M = D_K(F)$ avec F à coefficients dans K. Alors, g permute les racines de F donc laisse stable M.

2) C'est une conséquence du principe de conjugaison (voir [9] Ch. 1) : un conjugué ghg^{-1} est du même type que h et ses éléments géométriques sont ceux de h transportés par g. Ici, si h est dans H il fixe M, donc, par le principe de conjugaison, ghg^{-1} fixe $g(M)$ et comme $g(M) = M$, ghg^{-1} est dans H.

5.2.2 Structure des extensions radicales

5.8 *Remarque.* **Attention**, même si l'on dispose de toutes les racines de l'unité, une extension radicale n'est pas nécessairement normale, voir ci-dessous paragraphe 8.2. On renvoie au théorème 3.28 pour le théorème de structure des extensions radicales. En voici un corollaire :

5.9 Corollaire. *Soit $K \subset M$ une extension normale et radicale. Il existe une suite de sous-corps $K = K_0 \subset K_1 \subset \cdots \subset K_n = M$ avec $K_{i+1} = K_i(\alpha_i)$,*

49. Ici, comme on est en caractéristique 0, ce mot est synonyme de *galoisienne*.

$\alpha_i^{p_i} = a_i$ avec $a_i \in K_i$ et $\alpha_i \notin K_i$ telles que les extensions $K_i \subset K_{i+1}$ soient normales. On pose $G_i = \mathrm{Gal}(M/K_i)$. Alors, les G_i sont des sous-groupes de $G_0 = \mathrm{Gal}(M/K)$, G_{i+1} est un sous-groupe distingué de G_i de quotient cyclique d'ordre premier.

Démonstration. Cela résulte de 3.28. Il suffit de décomposer l'extension $M_i \subset M_{i+1} = M_i(\alpha_{i,1}, \ldots, \alpha_{i,m_i})$ en introduisant les corps $M_i(\alpha_{i,1}, \ldots, \alpha_{i,k})$, $1 \leq k \leq m_i$.

5.10 Corollaire. *Soit K un corps et soit P un polynôme irréductible de degré > 0 à coefficients dans K. On note $L = D_K(P)$ un corps de décomposition de P. On suppose que l'équation $P(x) = 0$ est résoluble par radicaux. Alors, le groupe de Galois $G = \mathrm{Gal}(L/K)$ admet une suite de sous-groupes $\{1\} = H_s \subset H_{s-1} \subset \cdots \subset H_1 \subset H_0 = G$, avec H_{i+1} distingué dans H_i, de quotient cyclique d'ordre premier*[50].

Démonstration. Le corps L se plonge dans une extension radicale et on obtient une extension normale radicale M/K par 3.28. On a un homomorphisme surjectif de $G_0 = \mathrm{Gal}(M/K)$ sur $G = \mathrm{Gal}(L/K)$. Les images H_i des sous-groupes G_i de G_0 donnés par 5.9 sont des sous-groupes distingués les uns dans les autres, à quotients d'ordre premier ou triviaux. On peut supprimer ces derniers et comme le degré de L/K est > 0, tous ne le sont pas.

5.11 *Remarque.* **Attention**, dans 5.9, si chaque K_{i+1} est normal sur K_i il ne l'est pas, en général, sur K. C'est une grande différence avec 3.28 où les extensions M_i/K sont toutes normales. Cela signifie que, si le sous-groupe G_{i+1} est distingué dans G_i, il ne l'est pas dans G en général et c'est la même chose pour le sous-groupe[51] H_i de 5.10.

5.2.3 La preuve du théorème de Galois : les résultats sur les groupes

On reprend la situation de 5.1. On suppose que l'équation $P(x) = 0$ est résoluble. En vertu de 5.10, on a une suite de sous-groupes $\{1\} = H_s \subset H_{s-1} \subset \cdots \subset H_1 \subset H_0 = G = \mathrm{Gal}(L/K)$, avec H_{i+1} distingué dans H_i, de quotient cyclique d'ordre premier. Le groupe G permute les racines de P, fidèlement (car les racines engendrent L), de sorte que c'est un sous-groupe de $\mathfrak{S}_p$, et transitivement (car P est irréductible), donc il est d'ordre multiple de p. De plus, comme p est premier et $|\mathfrak{S}_p| = p!$, on a $|G| = pm$ avec $p \wedge m = 1$.

50. Le lecteur instruit aura reconnu un groupe résoluble.

51. Un groupe résoluble G n'admet pas, en général, une suite de sous-groupes G_i distingués dans G à quotients cycliques d'ordre premier comme le montre l'exemple de $\mathfrak{A}_4$.

Comme Galois, on note $\{0, 1, \ldots, p-1\}$ l'ensemble sur lequel $\mathfrak{S}_p$ opère et on l'identifie à $\mathbf{Z}/p\mathbf{Z}$.

On a un premier lemme :

5.12 Lemme. *Soit G un sous-groupe de $\mathfrak{S}_p$, p premier, transitif sur $X = \{0, 1, \ldots, p-1\}$ et soit N un sous-groupe distingué de G, distinct de $\{1\}$. Alors N opère transitivement sur X.*

Démonstration. C'est le principe de conjugaison, pris sous la forme :

5.13 Lemme. *Si G opère sur X, si N est un sous-groupe de G, et si Y est une orbite sous N, gY est une orbite sous gNg^{-1}.*

Démonstration. Il faut voir que si y, z sont dans Y, donc gy et gz dans gY, gy est transformé en gz par gNg^{-1}. Mais on a $z = ny$ avec $n \in N$, donc $gz = gny = (gng^{-1})gy$.

Alors, si N est distingué et a des orbites $X_1, \ldots, X_r$, gX_i est une orbite sous $gNg^{-1} = N$ et c'est donc un X_j. Les orbites ont donc même cardinal, qui ne peut être que 1 ou p car p est premier et 1 n'est pas possible car N est différent de $\{1\}$.

5.14 Corollaire. *Le sous-groupe H_{s-1} est d'ordre p et il est distingué dans G.*

Démonstration. On est dans les conditions d'applications de 5.12, donc on montre successivement en descendant que chaque H_i opère fidèlement transitivement sur X, en particulier H_{s-1}. Comme H_{s-1} est de cardinal premier et multiple de p, il est de cardinal p. Montrons que H_{s-1} est distingué [52] dans G. Comme p ne divise pas m, H_{s-1} est un sous-groupe de Sylow de H_{s-2}, donc caractéristique. Mais alors, on en déduit, par récurrence, que H_{s-1} est distingué dans chaque H_i et qu'il en est un Sylow. Pour $i = 0$ on a le résultat. Pour une autre preuve de ce fait, voir 5.16.1 ci-dessous.

Le résultat crucial est alors le suivant :

5.15 Lemme. *Soient p un nombre premier et G un sous-groupe de $\mathfrak{S}_p$ de cardinal multiple de p. On suppose que G contient un sous-groupe distingué N d'ordre p. On identifie $\{0, 1, \ldots, p-1\}$ avec $\mathbf{Z}/p\mathbf{Z}$. Alors, si $g \in G$ on a les propriétés suivantes :*

1) g est affine : on a $g(s) = a + ks$ pour tout s, avec $a, k \in \mathbf{Z}/p\mathbf{Z}$ et $k \neq 0$.

2) Si $g \neq \mathrm{Id}$, g admet au plus un point fixe.

3) Si g n'est pas dans N, g est d'ordre diviseur de $p-1$. Il en résulte que N est l'unique sous-groupe d'ordre p de G.

52. Attention, bien sûr, le fait d'être distingué n'est pas transitif.

Démonstration. Comme N est un sous-groupe cyclique d'ordre p de $\mathfrak{S}_p$ il est engendré par un p-cycle, disons $\sigma = (0, 1, 2, \ldots, p-1)$. On a $\sigma(i) = i+1$ et $\sigma^k(i) = i+k$ modulo p. Soit $g \in G$, on considère $g\sigma g^{-1}$ et on en note deux propriétés :

i) c'est $(g(0), g(1), \ldots, g(p-1))$ par le principe de conjugaison,

ii) c'est une puissance de σ, disons σ^k, avec $k = 1, \ldots, p-1$.

On a donc $g(1) = g(0) + k$, $g(2) = g(1) + k = g(0) + 2k$, etc. $g(s) = g(0) + ks := a + ks$ ce qui donne le point 1).

Si s est fixe on a $a + ks = s$ donc $s(1-k) = a$. Si $k \neq 1$ il y a un unique point fixe[53] $f = a/(1-k)$, si $k = 1$ il n'y en a pas sauf si $a = 0$ auquel cas g est l'identité.

Enfin, si $k \neq 1$, on a $g^n(s) = a + ka + \cdots + k^{n-1}a + k^n s$ et, pour $n = p-1$, on a $g^{p-1}(s) = s$, ce qui montre que l'ordre de g divise $p-1$. (Ou encore : si f est l'unique point fixe de g on a $g(s) - f = k(s-f)$, donc $g^{p-1} = \mathrm{Id}$).

5.16 *Remarques.* 1) Le lemme ci-dessus permet de montrer que H_{s-1} est distingué dans G sans utiliser le théorème de Sylow. En effet, à chaque cran il est l'unique sous-groupe d'ordre p de H_i.

2) Le lemme montre que G est contenu dans le groupe affine $\mathbf{A}_1(\mathbf{F}_p)$ des transformations de $\mathbf{F}_p$ du type $x \mapsto ax + b$ avec $a \in \mathbf{F}_p^*$ et $b \in \mathbf{F}_p$. Ce groupe est isomorphe au produit semi-direct $(\mathbf{Z}/p\mathbf{Z}) \rtimes (\mathbf{Z}/p\mathbf{Z})^*$ et il est de cardinal $p(p-1)$. On voit que les sous-groupes résolubles de $\mathfrak{S}_p$ sont beaucoup plus petits que $\mathfrak{S}_p$ qui est de cardinal $p!$.

5.2.4 La preuve du théorème de Galois 5.1 (suite et fin)

En vertu de 5.10, le groupe G possède une suite de sous-groupes H_i distingués les uns dans les autres et à quotients d'ordre premier. En vertu de 5.14 et 5.15, on voit que les éléments non triviaux de G ont au plus un point fixe. Si l'on considère l'extension $K(x_i, x_j) \subset L$ les éléments du groupe de Galois $\mathrm{Gal}(L/K(x_i, x_j))$ fixent x_i et x_j, donc ce groupe est réduit à l'identité et on a $L = K(x_i, x_j)$.

5.2.5 La réciproque de 5.1

5.17 Proposition. *On reprend les notations de 5.1. On suppose qu'on a, pour tous i, j distincts $K(x_i, x_j) = L$. Alors, l'équation $P(x) = 0$ est résoluble.*

53. On utilise ici le fait que $\mathbf{Z}/p\mathbf{Z}$ est un corps, bien connu de Galois. N'oublions pas qu'il est aussi l'inventeur de la théorie des corps finis.

Démonstration. On suppose qu'on connaît le théorème fondamental sur les extensions résolubles (l'équivalence entre équation résoluble et groupe résoluble), voir [54] [10]. Il reste donc à montrer :

5.18 Lemme. *Soit G un sous-groupe transitif de $\mathfrak{S}_p$ dont les éléments non triviaux ont au plus un point fixe. Alors G est d'ordre $\leq p(p-1)$ et il est résoluble.*

Démonstration. Comme G opère sans point fixe sur les couples (i,j) avec $i \neq j$ et que ces couples sont en nombre $p(p-1)$ on a aussitôt l'assertion sur le cardinal.

On en déduit que G a un unique sous-groupe d'ordre p, qui est donc distingué. En effet, si l'on a deux sous-groupes A, B d'ordre p distincts, leur intersection est réduite à l'élément neutre, donc l'ensemble $AB = \{ab \mid a \in A, b \in B\}$ est de cardinal p^2 (on peut aussi invoquer Sylow).

Le lemme 5.15 et la remarque 5.16.2 montrent alors que G est inclus dans $\mathbf{A}_1(\mathbf{F}_p)$ qui est résoluble comme extension de $\mathbf{Z}/p\mathbf{Z}$ par $(\mathbf{Z}/p\mathbf{Z})^*$.

5.19 *Remarque.* L'hypothèse que p est premier est essentielle pour avoir le sens réciproque dans 5.1. On obtient un contre-exemple comme suit. On considère $L = D_{\mathbf{Q}}(X^5 - 6X + 3)$, dont on sait que le groupe de Galois est $\mathfrak{S}_5$ (voir [10]). Soit x un élément primitif de L, qui est donc de degré 120, soit F son polynôme minimal et soient $x = x_1, x_2, \ldots, x_{120}$ ses racines. Comme toutes sont de degré 120 on a $L = K(x_i)$ pour tout i, pourtant l'équation $F = 0$ n'est pas résoluble par radicaux car $L/\mathbf{Q}$ n'est pas résoluble.

5.3 Le mémoire original de Galois : les préliminaires

5.3.1 Principes

Galois commence par un paragraphe intitulé "Principes" dans lequel il précise certaines définitions, notamment les mots irréductible et rationnel. Sur ce point, Galois a une claire conscience des choses [55], même s'il ne dispose pas du vocabulaire adéquat pour le dire et notamment de la notion de corps. Voilà ce qu'il dit :

il faudra entendre ... par quantité rationnelle, une quantité qui s'exprime en fonction rationnelle des coefficients de la proposée.

En langage moderne, si l'on a une équation $x_n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, les quantités rationnelles sont celles qui sont dans le corps $\mathbf{Q}(a_0, \ldots, a_{n-1})$,

54. Le point crucial est de montrer qu'en présences de racines p-ièmes de l'unité, une extension de groupe $\mathbf{Z}/p\mathbf{Z}$ est engendrée par une racine p-ième. C'est essentiellement la résolvante de Lagrange, voir 3.31.

55. C'était déjà le cas d'Abel, voir ci-dessus §3.4.1.

voire dans le corps obtenu en adjoignant (il utilise explicitement ce mot) des quantités auxiliaires. Il dit explicitement :

Il y a plus : on pourra convenir de regarder comme rationnelle toute fonction rationnelle d'un certain nombre de quantités déterminées, supposées connues a priori. Par exemple, on pourra choisir une certaine racine d'un nombre entier, et regarder comme rationnelle toute fonction rationnelle de ce radical.

Le mot rationnel a donc bien le sens moderne de : "élément du corps de base", qui peut être étendu par rapport au corps $\mathbf{Q}$ des nombres rationnels par adjonction de certains éléments et notamment de radicaux.

Il note que l'irréductibilité peut se perdre par une telle adjonction et donne l'exemple du polynôme cyclotomique Φ_n qui devient réductible quand on adjoint les racines d'une "équation de Gauss", voir ci-dessous §8.1.

Ensuite il précise les notions de substitution et de permutation (la permutation est un état, la substitution une application passant d'un état à un autre). Il note que l'ensemble des substitutions est un groupe [56] (en tous cas qu'il est stable par composition : *... si dans un pareil groupe on a les substitutions S et T, on est sûr d'avoir la substitution ST.*).

5.3.2 Préparatifs

Galois propose une suite de quatre lemmes (qui sont "tous connus", dit-il). Nous les examinons soigneusement ci-dessous [57].

5.20 Lemme. (Lemme I) *Si P est irréductible sur K et s'il a une racine commune avec $Q \in K[X]$, alors P divise Q.*

Démonstration. En effet, on regarde $D = \operatorname{pgcd}(P, Q)$, il est de degré ≥ 1, à coefficients dans K et divise P, c'est donc P.

Galois ne fait que suggérer la méthode, la preuve se termine par "donc etc."

5.21 Lemme. (Lemme II) *Si P admet les racines $x_1, \ldots, x_n$ distinctes, il existe une fonction rationnelle (et même linéaire à coefficients entiers) $y = f(x_1, \ldots, x_n)$ telle que tous ses transformés par $\mathfrak{S}_n$ soient distincts.*

Commentaire. *C'est le pas décisif vers le théorème de l'élément primitif. Par rapport à Abel qui travaille avec des racines indéterminées c'est plus*

56. Il est indéniable que Galois est vraiment l'inventeur de la notion de groupe, même si parfois il utilise encore le mot pour des choses qui n'en sont pas (par exemple des classes à gauche).

57. Je traduis les énoncés en langage moderne et je complète au besoin les preuves de Galois qui sont souvent elliptiques. Mes commentaires apparaissent en italiques.

difficile (dans le cas d'Abel $x_1 + 2x_2 + \cdots + nx_n$ convient). Voici une preuve (Galois n'en donne pas).

Démonstration. On suppose que les x_i sont dans $\mathbf{C}$. On pose $m = \mathrm{Min}_{i\neq j}|x_i - x_j|$ et $M = \mathrm{Max}_{i\neq j}|x_i - x_j|$, on choisit un entier $N > M/m$, on pose $c_k = k!N^k$ (suite croissante) et $y = c_1x_1 + \cdots + c_nx_n$. Alors, si σ, τ sont deux permutations distinctes des x_i, on a $\sigma(y) \neq \tau(y)$. Il suffit de montrer que, si σ n'est pas l'identité, on a $\sigma(y) \neq y$. Sinon, on a $c_1(x_1 - x_{\sigma(1)}) + \cdots + c_n(x_n - x_{\sigma(n)}) = 0$. Soit k le plus grand indice tel que $k \neq \sigma(k)$. On a donc $c_1(x_1 - x_{\sigma(1)}) + \cdots + c_k(x_k - x_{\sigma(k)}) = 0$, d'où $c_k(x_{\sigma(k)} - x_k) = c_1(x_1 - x_{\sigma(1)}) + \cdots + c_{k-1}(x_{k-1} - x_{\sigma(k-1)})$. En passant aux modules, on en déduit $c_k m \leq (k-1)c_{k-1}M$, donc $k!N^k m \leq (k-1)!(k-1)N^{k-1}M$, d'où $kN \leq (k-1)M/m$ et c'est absurde.

En fait, on a mieux et c'est important pour la suite :

5.22 Lemme. *Avec les notations de la preuve précédente, si l'on a une égalité $\sum_{i=1}^n c_i(x_{\alpha_i} - x_{\beta_i}) = 0$, avec $\alpha_i, \beta_i \in \{1, 2, \ldots, n\}$, c'est que, pour tout i, on a $\alpha_i = \beta_i$.*

Démonstration. Sinon, on appelle k le plus grand i tel que $\alpha_i \neq \beta_i$ et on conclut comme ci-dessus.

5.23 Lemme. (Lemme III) *Avec les notations et les hypothèses de 5.21, on a $L = K(x_1, \ldots, x_n) = K(y)$ (théorème de l'élément primitif[58]).*

Démonstration. Donnons d'abord un argument de théorie de Galois moderne. Soit N le degré de l'extension, qui est aussi le cardinal de son groupe de Galois G. On considère les conjugués de y, i.e. les $g(y)$ avec $g \in G$. Comme les g permutent les x_i, les N conjugués de y sont[59] distincts, donc y est de degré N et engendre L.

Analysons maintenant l'argument de Galois. On a $y = f(x_1, \ldots, x_n) = c_1x_1 + \cdots + c_nx_n$. On regarde $F(y, x_1, \ldots, x_n) := \prod_\sigma y - f(x_1, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$, produit étendu aux permutations qui fixent 1. Ce produit est nul et il est de la forme $g(y, x_1)$ où g est un polynôme à coefficients dans K. En effet, c'est un polynôme symétrique en $x_2, \ldots, x_n$ et on conclut avec le lemme suivant :

5.24 Lemme. *On suppose que $x_1, \ldots, x_n$ sont les racines du polynôme $P(X) = \sum_{i=0}^n (-1)^i a_i X^{n-i}$. Alors, tout polynôme symétrique de $x_2, \ldots, x_n$ s'écrit comme polynôme en les a_i et x_1.*

58. Galois signale que cette proposition est énoncée (sans démonstration) par Abel dans un mémoire posthume sur les fonctions elliptiques.

59. Qui sont parmi les permutés, mais pas tous les permutés *a priori*.

Démonstration. Il suffit de montrer que les fonctions symétriques élémentaires $\Sigma_i(x_2, \ldots, x_n)$ s'expriment en fonction de x_1 et des a_i. On procède par récurrence sur i. Pour $i = 1$ on a $x_2 + \cdots + x_n = a_1 - x_1$, et ensuite $\Sigma_i(x_2, \ldots, x_n) = a_i - x_1\Sigma_{i-1}(x_2, \ldots x_n)$.

On en déduit que x_1 est racine d'un polynôme Q à coefficients dans $K(y)$. Mais, les x_i, pour $i \geq 2$ ne sont pas racines de Q. En effet, on aurait, sinon, $y = c_1x_1 + \cdots c_nx_n = c_1x_i + c_2x_{\sigma(2)} + \cdots + c_nx_{\sigma(n)}$ et cela contredit 5.22.

Galois semble dire que c'est une conséquence du lemme 5.21, ce qui est sans doute incorrect car $c_1x_i+c_2x_{\sigma(2)}+\cdots+c_nx_{\sigma(n)}$ n'est pas une permutation de $c_1x_1 + \cdots c_nx_n$. En vérité, sa rédaction est scandaleusement elliptique ici, mais l'idée de la preuve est correcte.

Alors, le *pgcd* D de P et Q est de degré 1 et x_1, qui est racine de P et Q, donc de D, est rationnel en y, donc dans $K(y)$ et le même argument vaut pour tous les x_i.

5.25 *Remarque.* Ce résultat est une belle illustration de la phrase de Galois citée au début de cette section (voir §4.2) sur les calculs qu'il faut se contenter d'imaginer. En effet, si le résultat affirme que les x_i s'écrivent rationnellement en fonction de y, il n'est pas du tout évident de le faire explicitement. Nous l'avons vu ci-dessus avec l'équation, pourtant très simple, $x^4 - 2 = 0$, voir 4.11, et encore, par rapport à Galois, les résultats ont-ils été obtenus avec l'aide d'un logiciel de calcul formel.

Galois en est parfaitement conscient, voici ce qu'il dit en note : *Il est remarquable que, de cette proposition, on peut conclure que toute équation dépend d'une équation auxiliaire telle que toutes les racines de cette nouvelle équation soient des fonctions rationnelles les unes des autres ; car l'équation auxiliaire en V est dans ce cas.*

Au surplus, cette remarque est purement curieuse. En effet, une équation qui a cette propriété n'est pas, en général, plus facile à résoudre qu'une autre.

La première phrase formule le théorème de l'élément primitif : $K[y]$ est une extension normale, donc les conjugués de y sont dedans. La deuxième phrase explique que ce n'est qu'un résultat théorique [60] !

Vient ensuite le lemme IV :

5.26 Lemme. (Lemme IV) *Avec les notations de 5.21 et 5.23, soit Q le polynôme minimal*[61] *de l'élément primitif y. Alors, si $x = F(y)$ est une racine de P et si z est une autre racine de Q, $F(z)$ est une racine de P.*

60. Mais on sait bien qu'il est précieux, voir par exemple [10] §9.6.

61. Galois n'utilise pas ce mot mais parle d'un facteur irréductible d'une équation vérifiée par y, ce qui revient au même.

Démonstration. C'est clair avec la vision moderne du groupe de Galois. En effet, comme Q est irréductible, il existe $\sigma \in \mathrm{Gal}(L/K)$ tel que $\sigma(y) = z$. On a $x = F(y)$ avec F à coefficients dans K, donc $\sigma(x) = F(\sigma(y)) = F(z)$ et, comme x est racine de P, $\sigma(x) = F(z)$ l'est aussi.

Voici l'argument originel de Galois : si $y = f(x_1, \ldots, x_n)$, on écrit $R(Y) = \prod_{\sigma \in \mathfrak{S}_n} Y - f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$. On a $R(y) = 0$, avec R à coefficients dans K, donc le polynôme minimal Q de y divise R et les autres racines de Q sont aussi de la forme $f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$, en particulier z.

On considère ensuite, comme au lemme III :

$$g(y, x_1) = \prod_{\tau \in \mathfrak{S}_{n-1}} y - f(x_1, x_{\tau(2)}, \ldots, x_{\tau(n)}) = 0.$$

Appliquant $\sigma \in \mathfrak{S}_n$ on a aussi $g(\sigma(y), x_{\sigma(1)}) = 0$. Mais, par le raisonnement du lemme III qui a donné $x = x_1 = F(y)$, on obtient, en permutant les x_i, $x_{\sigma(1)} = F(\sigma(y)) = F(z)$.

5.27 *Remarque.* Les preuves de ces deux derniers lemmes sont un bon exemple des simplifications apportées par la notion de corps et de groupe de Galois.

5.28 *Remarque.* Le théorème de l'élément primitif permet de mieux comprendre la notion de goupe de Galois vu comme groupe des "bonnes permutations". En effet, si le corps $L = K(x_1, \ldots, x_n)$ est engendré par les racines du polynôme irréductible P, on a vu qu'il existe un élément primitif y tel que $L = K(y)$. Cet élément est de degré N et ses conjugués $y = y_1, \ldots, y_N$, racines de son polynôme minimal Q, sont aussi dans L car l'extension est normale. On peut donc s'intéresser aussi aux permutations des y_i et la question est de savoir si une permutation des y_i induit une permutation des x_i. Ce n'est évidemment pas vrai en général. On pensera au cas où P est de degré 4 avec un groupe de Galois $\mathfrak{S}_4$, auquel cas y est de degré 24 et les 24! permutations de ses racines ne sont évidemment pas toutes bonnes à prendre. Un autre exemple est celui de $P(X) = X^4 - 2$, voir 4.11. On voit que la seule permutation des 8 conjugués de l'élément primitif $\alpha + i$ qui l'échange avec $\alpha - i$ et qui est dans le groupe de Galois est (12)(38)(47)(56) avec l'ordre des racines donné en 4.11. En particulier la transposition (12) n'est pas pertinente.

La détermination des "bonnes permutations", i.e. celles qui sont dans le groupe de Galois, est facile si l'on pense en termes d'automorphismes de corps et c'est l'un des progrès essentiels amenés par cette vision des choses.

5.4 Le mémoire original de Galois : suite, les quatre propositions

5.4.1 La proposition I ou l'acte de naissance du groupe de Galois

On l'a déjà évoquée ci-dessus :

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

1) Que toute fonction des racines, invariable par les substitutions de ce groupe, soit rationnellement connue ;

2) Réciproquement, que toute fonction des racines, déterminable rationnellement, soit invariable par les substitutions.

Rappelons aussi sa traduction :

5.30 Théorème. *Soit $P \in K[X]$ de racines $x_1, \ldots, x_n \in L = K(x_1, \ldots, x_n)$. Il y a un sous-groupe G de $\mathfrak{S}_n$ tel que tout $y \in L$ fixe par G est dans K et réciproquement.*

Il s'agit bien du groupe de Galois $G = \mathrm{Gal}(L/K)$ qui admet exactement K comme corps fixe, voir [10] 9.13.

5.31 *Remarques.* 1) Galois affirme, dans une parenthèse, que *dans le cas des équations algébriques* le groupe est $\mathfrak{S}_n$. Le sens du mot *équations algébriques* n'est évidemment pas le nôtre. Peut-être faut-il entendre *équations générales* ?

2) Il dit aussi, dans une autre parenthèse, que, dans le cas de $\dfrac{X^n - 1}{X - 1} = 1 + X + \cdots + X^{n-1}$, le groupe considéré est cyclique. Ce n'est pas vrai en général, même si l'on prend le polynôme Φ_n (c'est vrai si n est premier et presque seulement dans ce cas, voir [10] 4.7 et [9] Ch. 3, th. 4.14). Il dit aussi que si les racines sont toutes des fonctions rationnelles de l'une d'entre elles, i.e. si $L = K(x_1)$, le cardinal du groupe est le degré du polynôme, ce qui est exact.

Démonstration. (du théorème) Galois considère un élément primitif y de L et ses conjugués $y = y_1, \ldots, y_N$ et il écrit les racines de P comme polynômes en y : $x_1 = f_1(y)$, ..., $x_n = f_n(y)$, puis il écrit les mêmes appliquées aux conjugués de y. Cela permute les x_i (lemme IV) : si $x_i = f_i(y)$, on pose $\sigma_j(x_i) = f_i(y_j)$, et on obtient ainsi N permutations des x_i qui forment le groupe cherché [62].

62. La théorie moderne confirme que c'est effectivement le groupe de Galois car son cardinal est le degré de L sur K, donc le degré N de y.

En lisant un peu entre les lignes, on rétablit la démonstration de Galois :

1) Si $z = f(y_1)$ est invariant par le groupe, cela signifie qu'on a $f(y_1) = f(y_2) = \ldots = f(y_N)$, donc, dit-il, que z est dans K. L'argument de Galois n'est pas clair, mais voilà ce qu'on peut dire. On a $z = a_0 + a_1 y_i + \cdots + a_r y_i^r$ pour tout $i = 1, \ldots, N$. On somme toutes ces relations et on obtient $Nz = Na_0 + a_1(y_1 + \cdots + y_N) + \cdots + a_r(y_1^r + \cdots + y_N^r)$. Comme les sommes de Newton (somme des y_i^k) sont des polynômes symétriques en les y_i, elles s'écrivent comme des polynômes en les coefficients de l'équation minimale de y qui sont dans K.

2) Réciproquement, si $x = f(y)$ est dans K, on peut supposer que le degré de f est $< N$. Mais alors, si f n'est pas une constante, cette égalité est une équation vérifiée par y et de degré plus petit que celui de Q, ce qui est absurde.

5.32 *Remarque.* On notera à la suite de cette proposition la scolie 2, un peu mystérieuse :

Les substitutions sont indépendantes même du nombre des racines.

Cette remarque est troublante, car Galois a tout fait avec les permutations des racines, mais il a manifestement l'intuition d'un groupe indépendant de cela (peut-être en voyant le groupe agir aussi sur l'élément primitif y et ses conjugués qui sont généralement en nombre plus grand que les x_i). L'avenir lui donne raison puisqu'on sait que ce groupe peut être vu comme celui des automorphismes du corps L qui fixent K, indépendamment des racines de P. Sur ce point, d'autres interprétations, peut-être bien plus profondes, sont possibles, comme me l'a suggéré Ricardo Perez-Marco lors de l'exposé oral.

5.4.2 La proposition II

Précisons, une fois pour toutes, les notations valables dans toute la suite :

5.33 Notations. On considère un corps K, un polynôme $P \in K[X]$, irréductible, de degré n, on désigne par L un corps de décomposition [63] de P, $L = K(x_1, \ldots, x_n)$, L est donc une extension normale de K. On note y un élément primitif de L. On a donc $L = K(y)$, on appelle Q le polynôme minimal de y sur K et on note N son degré. On pose $G = \mathrm{Gal}(L/K)$.

Voici, citée très exactement, la proposition II de Galois :

5.34 Théorème. *Si l'on adjoint à une équation donnée la racine r d'une équation auxiliaire irréductible, il arrivera de deux choses l'une : ou bien le groupe de l'équation ne sera pas changé, ou bien il se partagera en p groupes*

63. On supposera toujours que les racines des polynômes sont dans $\mathbf{C}$.

appartenant chacun à l'équation proposée respectivement quand on lui adjoint chacune des racines de l'équation auxiliaire ; ces groupes jouiront de la propriété remarquable, que l'on passera de l'un à l'autre en opérant dans toutes les permutations une même substitution de lettres.

Voici une tentative de traduction de cette proposition en termes modernes :

5.35 Théorème. *Les notations sont celles de 5.33. On considère un polynôme R irréductible sur K et on adjoint à K toutes les racines*[64] *$\alpha_1, \ldots, \alpha_r$ de R, on obtient $M = K(\alpha_1, \ldots, \alpha_r) = D_K(R)$. On considère le corps LM engendré par L et M. On a $LM = K(\alpha_1, \ldots, \alpha_r, y) = L(\alpha_1, \ldots, \alpha_r) = D_M(P)$.*

Il y a deux cas :

1) Le polynôme Q est encore irréductible sur M. On a $\mathrm{Gal}(LM/M) = \mathrm{Gal}(L/K)$.

2) Le polynôme Q est réductible sur M. Alors, ses facteurs sont tous de même degré. Les r sous-groupes de $\mathrm{Gal}(LM/K)$ *du type* $\mathrm{Gal}(LM/K(\alpha_i))$ *sont conjugués.*

Démonstration. L'extension $K \subset LM = D_K(QR)$ est normale donc galoisienne et on peut appliquer la théorie de Galois (voir [10] §9).

1) Comme L/K est normale, on a un homomorphisme Φ de restriction $\sigma \mapsto \sigma|_L$ de $\mathrm{Gal}(LM/K)$ dans $\mathrm{Gal}(L/K)$, que l'on restreint au sous-groupe $\mathrm{Gal}(LM/M)$, et, comme L et M engendrent LM, le noyau de Φ est trivial. Comme Q est irréductible sur M et de degré N, on a $[LM : M] = N = [L : K]$ et comme ces degrés sont les cardinaux des groupes de Galois, Φ est un isomorphisme.

Pour toute démonstration, Galois se contente de dire : *il est clair que le groupe de l'équation ne sera pas changé.*

2) On écrit $Q = Q_1 \cdots Q_s$ dans $M[X]$. Si y et z sont des racines de Q_i et Q_j, comme Q est irréductible sur K, il existe $\sigma \in \mathrm{Gal}(L/K)$ qui envoie y sur z et, comme $LM = D_L(R)$, on peut prolonger σ en un automorphisme σ' de LM (qui fixe encore K), voir [9] Ch. III lemme 1.31. Comme M/K est normale aussi car $M = D_K(R)$, σ' laisse stable M, donc Q_i se transforme en un polynôme à coefficients dans M, de même degré, et irréductible. Comme on a $Q_i(y) = 0$, donc, par σ', $\sigma'(Q_i)(z) = 0$, on a $\sigma'(Q_i) = Q_j$, d'où l'assertion sur le degré.

Montrons l'assertion sur les conjugués. Soient α_i et α_j deux racines de R. Comme R est irréductible, il existe $\sigma \in \mathrm{Gal}(M/K)$ tel que $\sigma(\alpha_i) = \alpha_j$

64. Rappelons qu'on les suppose dans **C**.

et, comme LM/M est normale, σ se prolonge en un automorphisme de LM, noté encore σ. Soit $g \in \mathrm{Gal}(LM/K(\alpha_i)) \subset \mathrm{Gal}(LM/K)$. Alors $\sigma g \sigma^{-1}$ est dans $\mathrm{Gal}(LM/K(\alpha_j))$ et inversement.

Commentaire. J'ai eu beaucoup de mal à comprendre cette proposition et j'en ai proposé d'abord plusieurs traductions fausses [65]. Un point essentiel est qu'il ne suffit pas d'adjoindre à K une racine de l'équation R, mais qu'il faut les ajouter toutes afin de préserver la normalité des extensions. C'est ce que dit Galois avec la phrase : *chacune des racines de l'équation auxiliaire.* C'est d'ailleurs beaucoup plus clair dans la lettre de la veille (voir §6 ci-dessous) où il dit : *on voit une grande différence entre adjoindre à une équation une des racines d'une équation auxiliaire ou les adjoindre toutes.*

L'assertion de conjugaison de 5.35 est la traduction de : *on passera de l'un à l'autre en opérant dans toutes les permutations une même substitution de lettres.* En effet, si g est dans un sous-groupe, c'est une permutation, donc un produit de cycles $(a_1 \dots a_r)(b_1 \dots b_s) \dots$ et, en vertu du principe de conjugaison, on passe au groupe conjugué en faisant $\sigma g \sigma^{-1}$, donc $(a_{\sigma(1)} \dots a_{\sigma(r)})(b_{\sigma(1)} \dots b_{\sigma(r)}) \dots$, c'est-à-dire en effectuant la même substitution σ sur les éléments du groupe comme le dit Galois.

Galois considère comme évident que les degrés des facteurs sont les mêmes et en déduit que les groupes ont un même nombre d'éléments : *... puisqu'à chaque valeur de V* (l'élément primitif) *correspond une permutation.* Il explique ensuite (avec les notations ci-dessus) que si y est une racine de Q_i, si $z = F(y)$ en est une autre et si y' est une racine de Q_j, $z' = F(y')$ est racine de Q_j. Bien qu'il n'y ait pas d'allusion aux permutations, il semble bien que ce soit cet argument qui soit derrière cette assertion. De même le point sur les conjugués, s'il est clairement énoncé, n'est – à mon avis – pas vraiment établi [66].

5.4.3 Les Proposition III et IV

Voici la version de Galois :

5.36 Théorème. *Si l'on adjoint à une équation toutes les racines d'une équation auxiliaire, les groupes dont il est question dans le théorème II joui-*

65. Les mathématiciens actuels ont tendance à considérer que les académiciens (notamment Poisson) qui ont rejeté le mémoire de Galois étaient des incompétents. À lire ce mémoire dans le détail, je serais assez enclin à leur trouver des excuses.

66. Il est clair que Galois a écrit très rapidement ce texte et il est conscient qu'il y a des points obscurs. D'ailleurs sur le manuscrit originel on trouve la mention : *Il y a quelque chose à compléter dans cette démonstration. Je n'ai pas le temps.* De même, pour la proposition III ci-dessous, il se contente de dire *On trouvera la démonstration.*

ront de plus de cette propriété, que les substitutions seront les mêmes dans chaque groupe.

Ce théorème n'est vraiment pas clair. Dans l'édition de Liouville des œuvres de Galois, il est accompagné d'une note d'Auguste Chevalier, qui évoque une première version de ce théorème, plus compréhensible. Voici d'abord ce que dit Auguste Chevalier :

5.37 Proposition. *Si l'équation en r est de la forme $r^p = A$, et que les racines p-ièmes de l'unité se trouvent au nombre des quantités précédemment adjointes, les p groupes dont il est question dans le théorème II jouiront de plus de cette propriété, que les substitutions de lettres par lesquelles on passe d'une permutation à l'autre dans chaque groupe soient les mêmes pour tous les groupes.*

En voici une traduction en termes modernes :

5.38 Théorème. *Les notations sont celles de 5.33. Soit p un nombre premier*[67]*. On suppose que K contient une racine p-ième primitive de l'unité ζ. On ajoute à K une racine p-ième α d'un élément $a \in K$. Alors, le corps $K(\alpha)$ est une extension normale de K, il est égal à tous les $K(\zeta^i\alpha)$ et le groupe de Galois* $\mathrm{Gal}(L/K(\alpha))$ *est un sous-groupe distingué de* $\mathrm{Gal}(L/K)$ *de quotient* $\mathrm{Gal}(K(\alpha)/K)$*.*

En effet, dire que le groupe $\mathrm{Gal}(L/K(\alpha))$ est distingué signifie que les groupes $\mathrm{Gal}(L/K(\alpha_i)) = \mathrm{Gal}(L/K(\zeta^i\alpha))$ sont tous égaux.

La proposition IV, elle, est bien claire dans sa traduction moderne :

5.39 Proposition. *On adjoint à K un élément $z \in L$. Alors le groupe de Galois de L sur $K(z)$ est le sous-groupe de* $\mathrm{Gal}(L/K)$ *qui fixe z.*

5.5 Le problème de la résolution par radicaux

5.5.1 Préliminaires

On conserve les notations de 5.33.

Dans la proposition V, Galois pose le problème : *Dans quels cas une équation est-elle soluble par de simples radicaux* et il décrit une méthode pour ce faire : *... il faut successivement abaisser son groupe jusqu'à ne contenir plus qu'une seule permutation.*

Autrement dit, si l'équation $P(x) = 0$ est résoluble par radicaux, il existe un polynôme R du type $X^n - a$ tel que l'adjonction d'une de ses racines α

67. Ce point n'est pas précisé dans Galois.

diminue le groupe. Le groupe $\mathrm{Gal}(L(\alpha)/K(\alpha))$ est donc strictement inclus dans $G := \mathrm{Gal}(L/K)$.

5.40 *Remarques.* 1) Bien entendu, diminuer le groupe de Galois ne signifie pas que dans le corps obtenu en adjoignant les racines de R le polynôme P admet une racine. Par exemple si $P(X) = X^3 + X - 1$, l'adjonction de $\sqrt{\Delta} = \sqrt{23}$ fait passer le groupe de $\mathfrak{S}_3$ à $\mathfrak{A}_3$ sans ajouter de racine de P.

2) La diminution du groupe de Galois ne signifie pas non plus que R admet une racine dans L, voir le cas "irréductible" de l'équation de degré 3, par exemple avec $P(X) = X^3 - 3X + 1$ où le corps L est inclus dans $\mathbf{R}$, mais où la résolution nécessite d'introduire des radicaux complexes, cf. [10] 5.6.

Le point suivant est de montrer qu'on peut supposer une adjonction de degré premier. Le lemme suivant précise 3.5 ci-dessus :

5.41 Lemme. *Soit $K \subset L$ une extension galoisienne, $a \in K$, α une racine n-ième de a dans une extension. Soit $L(\alpha)$ le corps engendré. Le groupe* $\mathrm{Gal}(L(\alpha)/K(\alpha))$ *s'injecte dans* $\mathrm{Gal}(L/K)$ *et on suppose que cette inclusion est stricte. Alors, il existe une puissance b de α, un facteur premier p de n et une racine p-ième β de b avec $K(b) \subset K(\beta) \subset K(\alpha)$ tels que l'on ait* $\mathrm{Gal}(L(b)/K(b)) = \mathrm{Gal}(L/K)$ *et que* $\mathrm{Gal}(L(\beta)/K(\beta))$ *soit strictement inclus dans* $\mathrm{Gal}(L/K)$.

Démonstration. On raisonne par récurrence sur le nombre de facteurs premiers de n. Le résultat est clair si n est premier. Sinon, on pose $n = pm$ et on considère la racine p-ième $\gamma = \alpha^m$ de a. Si $\mathrm{Gal}(L(\gamma)/K(\gamma))$ est plus petit que $\mathrm{Gal}(L/K)$ on a gagné. Sinon, on considère l'extension $K(\gamma) \subset L(\gamma)$ et son groupe diminue par adjonction de la racine m-ième α de $\gamma = \alpha^m$. Comme m a moins de facteurs premiers que n on a gagné par l'hypothèse de récurrence.

5.42 *Remarques.* 1) Attention, l'exemple de $X^3 - 3X + 1$ montre que l'on ne peut pas supposer que le groupe diminue par une seule extension de degré premier du corps de base. Ici, il faut rajouter une racine 9-ième de l'unité, donc d'abord une racine cubique j (qui ne change pas le groupe), puis une racine cubique de j (qui trivialise le groupe).

2) Galois choisit un tel p minimal et il suppose aussi qu'on a adjoint une racine p-ième de l'unité. Il note que cette adjonction n'altère pas le groupe. En effet, on sait depuis Gauss que l'équation cyclotomique de degré p se résout avec des équations de degré plus petit (voir ci-dessous 8.1), de sorte que si le groupe changeait en ajoutant la racine de l'unité il aurait changé par une adjonction de degré $< p$.

5.5.2 Résoluble implique sous-groupe distingué

Voilà ce que dit Galois à ce moment du texte :

... d'après les théorèmes II et III, le groupe de l'équation devra se décomposer en p groupes jouissant les uns par rapport aux autres de cette double propriété : 1) que l'on passe de l'un à l'autre par une seule et même substitution ; 2) que tous contiennent les mêmes substitutions.

Pour bien comprendre le sens de ces assertions, il faut d'abord noter le lemme suivant [68], qui montre que tout se passe dans l'extension L :

5.43 Lemme. *Soit K un corps, P un polynôme irréductible sur K, $L = D_K(P)$, $G = \mathrm{Gal}(L/K)$ et soit p un nombre premier. On suppose que K contient les racines p-ièmes de l'unité. Soit $a \in K$ et α une racine p-ième de a. On suppose que le groupe de Galois de $L(\alpha)$ sur $K(\alpha)$ (qui s'injecte dans G) est strictement plus petit que G. Alors, α est dans L.*

Démonstration. Le résultat est évident si α est dans K. Sinon, le polynôme $X^p - a$ est irréductible sur K (voir 3.14) et on a $[K(\alpha) : K] = p$. Posons $N = [L : K]$, $N' = [L(\alpha) : K(\alpha)]$ et $q = [L(\alpha) : L]$, de sorte qu'on a $Nq = pN'$. Comme N' est un diviseur strict de N (car le groupe de Galois correspondant est un sous-groupe strict de G), on a $N = N'm$ avec $m > 1$ et $mq = p$. Comme m est un diviseur de p et que m est plus grand que 1 on a $m = p$, donc $q = 1$.

5.44 *Remarque.* Ici, l'apport des notions modernes est évident, notamment la notion de dimension et le théorème de la base télescopique.

Le résultat suivant est un corollaire de 5.43 et 5.38 :

5.45 Corollaire. *Dans la situation précédente, si l'on pose $M = K(\alpha)$, M est inclus dans L et $\mathrm{Gal}(L/M)$ est un sous-groupe distingué de G, de quotient $\mathrm{Gal}(K(\alpha)/K) \simeq \mathbf{Z}/p\mathbf{Z}$.*

5.5.3 Réciproque

Voici le résultat de Galois :

5.46 Proposition. *Les notations sont toujours celles de 5.33. On suppose que G contient un sous-groupe distingué H d'indice premier p et que K contient une racine primitive p-ième de l'unité ζ. Alors, l'extension $K \subset M := L^H$ est radicale (engendrée par une racine p-ième) et le groupe $\mathrm{Gal}(L/M)$ strictement plus petit que G.*

68. Ce lemme n'est pas dans Galois mais, à mon sens, il éclaircit la situation.

Démonstration. Pour une preuve en termes modernes, voir [10] 4.13 ou s'inspirer de 3.31 ci-dessus.

Galois considère un élément θ "invariable par toutes les substitutions de l'un des groupes partiels" mais qui "varie pour toute autre substitution". En clair, un élément qui est invariant par H, donc qui est dans M, mais pas dans K. Il donne une recette pour faire cela qui est de prendre un élément primitif ("invariable par aucune substitution") et d'en considérer une fonction symétrique par H (par exemple $\theta = \sum_{g\in H} g(y)$).

Il applique alors à θ une "substitution du groupe total qui ne lui sont point communes avec les groupes partiels", autrement dit un élément τ de $\mathrm{Gal}(M/K)$, puis ses itérés. Il note alors que, comme p est premier, la suite des $\tau^i(\theta)$ s'arrête à $p-1$ (le groupe $\mathrm{Gal}(M/K)$ est d'ordre p, donc cyclique engendré par τ). Il considère alors la résolvante de Lagrange[69] $x := \theta + \zeta\tau(\theta) + \zeta^2\tau^2(\theta) + \cdots + \zeta^{p-1}\tau^{p-1}(\theta)$. On a $\tau(x) = \zeta^{-1}x$, donc $\tau(x^p) = x^p$ et $x^p \in K$.

Galois considère comme évident que l'on a alors $M = K(x)$. (On sait qu'il faut vérifier que x n'est pas dans K, ce qui revient à voir que x est non nul, voir [10] *loc. cit.*)

5.5.4 Conclusion

Une fois ce résultat établi, il conclut par récurrence ("ainsi de suite") que l'on va pouvoir ramener le groupe donné à ne contenir plus qu'une permutation par adjonctions successives de radicaux.

Il explique sa démarche sur l'équation de degré 4. Il part de $\mathfrak{S}_4$, énumère d'abord les éléments de $\mathfrak{A}_4$, puis ceux du groupe de Klein $\mathbf{V}_4$ des doubles transpositions.

Arrivé là, il partage ce groupe en deux "groupes" (*sic*), $\{\mathrm{Id}, (ab)(cd)\}$ et $\{(ac)(bd), (ad)(bc)\}$. On notera que le second n'est évidemment pas un groupe (c'est une classe à gauche). Mais c'est juste une question de langage et Galois a parfaitement dévissé le groupe symétrique dans ce cas.

5.6 Le cas de degré premier

Il s'agit maintenant de prouver le théorème principal de l'article, voir 5.1. On se reportera au paragraphe 5.2 pour comparer avec la preuve moderne.

69. Galois ne cite pas Lagrange. Voir à ce sujet l'exposé de Massimo Galuzzi *Équations et substitutions avant Galois : Lagrange et Cauchy.*

5.6.1 Préliminaires

On reprend les notations de 5.33, mais on suppose que le degré de P est un nombre premier p. On suppose l'équation résoluble par radicaux. Cela signifie, en termes modernes, qu'il existe une extension radicale M qui contient L. Dans M, le polynôme P est scindé. L'extension M contient une tour de K_i (et on peut supposer que les radicaux qui interviennent sont de degrés premiers) et on considère le premier indice i tel que P soit réductible sur K_{i+1} et pas sur K_i. On en déduit que le radical de K_i à K_{i+1} est de degré p, c'est la Proposition VI de Galois :

5.47 Lemme. *Une équation irréductible de degré premier ne peut devenir réductible par l'adjonction d'un radical dont l'indice serait autre que le degré même de l'équation.*

Démonstration. Galois utilise sa proposition II (voir 5.35) : si P devient irréductible ses facteurs sont tous de même degré, à savoir celui du radical ajouté [70], lequel divise ainsi p, donc lui est égal.

Voici la version moderne de ce lemme :

5.48 Lemme. *Soient n et p des nombres premiers et soit $P \in K[X]$ irréductible de degré p. On adjoint à K un radical α vérifiant $\alpha^n = a$ avec $\alpha \notin K$, on pose $M = K(\alpha)$ et on suppose que P devient réductible sur M. Alors on a $n = p$.*

Démonstration. L'extension M/K étant de degré n en vertu de 3.14, on conclut avec [9] 3.14 : si n est distinct de p il est premier avec p et le polynôme P reste irréductible dans l'extension. Rappelons la preuve de ce point : on suppose $P = QR$ avec Q irréductible de degré $q < p$ et on considère un corps de rupture $M(x)$ de Q. Il est de degré q sur M et contient $K(x)$ corps de rupture de P qui est de degré p sur K. On a donc, par multiplicativité des degrés : $[M(x) : M] \times [M : K] = [M(x) : K(x)] \times [K(x) : K]$ soit $qn = mp$ et, comme p est premier avec q il divise n donc lui est égal.

5.49 *Remarques.* 1) On a encore ici un bel exemple de l'apport, dans la version moderne, des notions d'espace vectoriel et de dimension.

2) Ce lemme montre quelque chose de plus subtil. En effet, si P est résoluble, il y a un étage de la tour au passage duquel P cesse d'être irréductible et le degré de cet étage est égal à p d'après le lemme. Cela montre qu'il y a dans le sous-groupe correspondant (et donc dans le groupe de Galois total) un élément d'ordre p, donc un p-cycle, et cela assure la transitivité du groupe de Galois sur l'ensemble des racines de P.

70. Ce point n'est pas tout à fait évident. Il n'est correct que parce que l'on suppose que le radical adjoint est de degré premier, voir 5.48.

5.6.2 Le sens direct : un bilan

Il est temps de faire un bilan, en termes modernes :

5.50 Corollaire. *On reprend les notations de 5.33, mais avec un polynôme P de degré p premier et on suppose que les racines q-ièmes de l'unité, pour tout q premier $\leq p$, sont dans K. On suppose l'équation $P(x) = 0$ résoluble par radicaux. En vertu de 3.8, on sait qu'il existe une tour $K \subset K_1 \subset \cdots \subset K_s = L = D_K(P)$ telle que chaque extension soit engendrée par un radical de degré premier. On désigne par $K_{r+1} = K_r(\alpha)$ le premier étage de la tour sur lequel P est réductible. On a les résultats suivants :*

1) On a $[K_{r+1} : K_r] = p$ et α est racine p-ième d'un élément de K_r.

2) Le polynôme P est scindé sur K_{r+1} et on a $L = K_{r+1}$.

3) Les degrés des extensions $K_j \subset K_{j+1}$ pour $j < r$ sont $< p$.

4) Le groupe $H = \mathrm{Gal}(L/K_r)$ est un sous-groupe distingué d'ordre p de $\mathrm{Gal}(L/K)$.

Démonstration. Le point 1) a été vu en 5.48. La preuve du point 2) est analogue à celle de 5.35. On considère l'extension $K_r \subset D_{K_r}(P) = LK_r$. On écrit $P = P_1 \cdots P_s$ sur K_{r+1}. Soit x une racine de P_1 et y une racine de P_i. Comme P est irréductible sur K_r, il existe $\sigma \in \mathrm{Gal}(LK_r/K_r)$ tel que $\sigma(x) = y$. Comme les racines p-ièmes de l'unité sont dans K, l'extension $K_r \subset K_{r+1}$ est normale, donc K_{r+1} est stable par σ. Il en résulte que $\sigma(P_1)$ est à coefficients dans K_{r+1}, irréductible et qu'il admet y comme racine, c'est donc P_i et les facteurs de P ont tous même degré. Mais comme P est de degré p premier, tous sont de degré 1 et P est scindé sur K_{r+1} (ce qui donne $L = D_K(P) = K_{r+1}$)

Montrons le point 3). Le degré $[K_{j+1} : K_j]$ est un nombre premier q_j qui divise $N = [L : K]$. Mais comme N divise $p!$ le seul facteur premier égal à p dans N est $[L : K_{r+1}]$. Il en résulte que K_r est engendré sur K par des radicaux de degrés premiers $q < p$.

Une conséquence de cette remarque c'est que l'extension $K \subset K_r$ est normale. En effet, sinon, il y aurait un élément $\sigma \in \mathrm{Gal}(L/K)$ tel que $\sigma(K_r) := M \neq K_r$, de sorte que K_rM serait strictement plus grand que K_r et comme $[L : K_r] = p$ premier, cela imposerait $L = K_rM$. Mais M, qui est image de K_r, est engendré par des radicaux de degrés $q < p$, donc L serait engendré sur K_r par ces mêmes radicaux et c'est absurde.

Il en résulte que $\mathrm{Gal}(L/K_r)$ est un sous-groupe distingué d'ordre p de $\mathrm{Gal}(L/K)$.

5.51 *Remarque.* Galois considère comme évident que le groupe $\mathrm{Gal}(L/K)$ a

un sous-groupe distingué[71] d'ordre p. Certes c'est vrai, mais il est vraiment un peu rapide ici.

5.6.3 Le sens direct : la fin de la preuve

C'est essentiellement celle que nous avons donnée en 5.15.

Galois considère *le plus petit groupe possible avant celui qui n'a qu'une permutation*, c'est-à-dire ici $H = \mathrm{Gal}(L/K_r)$ et dit qu'il a p éléments. C'est bien ce qui a été vu en 5.50. Il applique alors un lemme de Cauchy :

5.52 Lemme. *Soit p un nombre premier et soit H un sous-groupe d'ordre p de $\mathfrak{S}_p$. Alors H est cyclique engendré par un p-cycle.*

Il écrit les racines $x_0, x_1, \ldots, x_{p-1}$ et énumère les éléments du groupe H qui sont les permutations circulaires des x_i. Il considère ensuite le groupe *qui précédera immédiatement celui-ci* (ici, il faut comprendre $G = \mathrm{Gal}(L/K)$) et affirme qu'il *devra se composer d'un certain nombre de groupes ayant tous les mêmes substitutions que celui-ci* (c'est la façon de dire que H est distingué dans G, voir 5.50).

Galois décrit la permutation g engendrant le groupe cyclique H comme $x_k \mapsto x_{k+c}$ (indices pris modulo p, c constant non nul), c'est-à-dire qu'il voit le groupe H comme[72] $\mathbf{Z}/p\mathbf{Z}$.

Puis il dit : *l'un quelconque des groupes semblables devra s'obtenir en opérant partout dans ce groupe une même substitution*, disons f. Cela signifie que l'on passe d'un groupe à l'autre en appliquant le principe de conjugaison : $(x_0, \ldots, x_{p-1})$ devient $(x_{f(0)}, \ldots, x_{f(p-1)})$. Et ensuite : *les substitutions de ces nouveaux groupes devant être les mêmes*[73] *que celles du groupe H on devra avoir $f(k+c) = f(k) + C$, C constant.* En fait, il écrit $h = fgf^{-1}$, avec $g, h \in H$, donc données par $g(k) = k + c$ et $h(k) = k + C$, soit $hf = fg$, $hf(k) = fg(k)$, $hf(k) = f(k+c) = f(k) + C$.

Il peut maintenant calculer f comme permutation de $\mathbf{Z}/p\mathbf{Z}$:

5.53 Lemme. *Soit $f : \mathbf{Z}/p\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$ une application. On suppose qu'il existe c, C, avec $c \neq 0$, tels que l'on ait, pour tout k, $f(k+c) = f(k) + C$. Alors, il existe $a, b \in \mathbf{Z}/p\mathbf{Z}$ avec $a \neq 0$ tels que $f(k) = ak + b$.*

Démonstration. On pose $g(k) = ak + b$ avec $a = \dfrac{f(c) - f(0)}{c}$ et $b = f(0)$ et on vérifie qu'on a $g(0) = f(0)$ et que g vérifie la relation $g(k+c) = g(k) + C$, d'où le résultat.

71. Bien entendu, il ne formule pas les choses ainsi.

72. On pourrait presque dire qu'il le voit comme le corps $\mathbf{F}_p$ à p éléments et c'est d'ailleurs sans doute à partir de là qu'il a introduit les corps finis.

73. Autrement dit, H est distingué dans G.

Commentaire. Ce que Galois a montré c'est que le groupe de Galois $G = \mathrm{Gal}(L/K)$ est formé des permutations de la forme $k \mapsto ak + b$ (donc qu'il est contenu dans le groupe affine de $\mathbf{Z}/p\mathbf{Z}$). C'est évidemment le point crucial de son résultat.

5.6.4 La réciproque

Réciproquement, si $\mathrm{Gal}(L/K)$ est contenu dans le groupe affine de $\mathbf{Z}/p\mathbf{Z}$, l'équation est résoluble par radicaux.

Galois reprend ici la résolvante de Lagrange. Il considère une racine p-ième primitive ζ de 1 et un entier a, générateur de $(\mathbf{Z}/p\mathbf{Z})^*$, (il dit *racine primitive de p*) et les éléments (pour $k = 1, \ldots, p-1$) :

$$X_1 = (x_0 + \zeta x_1 + \zeta^2 x_2 + \cdots + \zeta^{p-1} x_{p-1})^p$$

$$X_{a^k} := (x_0 + \zeta x_{a^k} + \zeta^2 x_{2a^k} + \cdots + \zeta^{p-1} x_{(p-1)a^k})^p$$

Il dit : *il est clair que toute fonction invariable par les substitutions circulaires des quantités $X_1, X_a, \ldots$ sera immédiatement connue.* Autrement dit, ces éléments sont dans K. On peut donc calculer les X_i à partir des coefficients de P, puis leurs racines p-ièmes et en déduire les x_i en résolvant un système linéaire [74].

5.54 *Exemple.* On peut illustrer cette méthode sur l'exemple de l'équation $x^5 - 5x + 12 = 0$, voir [10] §7.4. En effet, on pose

$$y_1 = x_1 + \zeta x_2 + \zeta^2 x_3 + \zeta^{-2} x_4 + \zeta^{-1} x_5, \quad y_4 = x_1 + \zeta^{-1} x_2 + \zeta^{-2} x_3 + \zeta^2 x_4 + \zeta x_5,$$

$$y_2 = x_1 + \zeta^2 x_2 + \zeta^{-1} x_3 + \zeta x_4 + \zeta^{-2} x_5, \quad y_3 = x_1 + \zeta^{-2} x_2 + \zeta x_3 + \zeta^{-1} x_4 + \zeta^2 x_5$$

et c'est exactement ce que dit Galois avec $a = 3$ modulo 5 !

5.6.5 Le théorème des deux racines

Voici le résultat final (Proposition VIII) :

5.55 Théorème. *Pour qu'une équation irréductible de degré premier soit soluble par radicaux, il faut et il suffit que deux des racines étant connues, les autres s'en déduisent rationnellement.*

74. Cela ressemble fort à la preuve usuelle. Il faut simplement ajouter l'équation $x_0 + \cdots + x_{p-1} = c$ où c est connu.

Avec les notations de 5.33, la condition de solubilité est donc $L = K(x_i, x_j)$ pour tous i, j, voir 5.1.

Démonstration. Si l'équation est résoluble, on a vu que $\mathrm{Gal}(L/K)$ est isomorphe un sous-groupe du groupe affine de $\mathbf{Z}/p\mathbf{Z}$, c'est-à-dire des applications $k \mapsto ak + b$, et on vérifie aussitôt que les éléments distincts de l'identité de ce groupe ont un unique point fixe (si $a \neq 1$), voire aucun (si $a = 1$). Comme le groupe $\mathrm{Gal}(L/K(x_i, x_j))$ est formé des éléments qui fixent x_i et x_j (pour cela, Galois invoque sa proposition IV, voir 5.39), il est réduit à l'identité, ce qui montre que l'on a $L = K(x_i, x_j)$.

Réciproquement, comme le groupe ne fixe pas deux racines son cardinal est $\leq p(p-1)$ (comme on le voit en le faisant opérer sur les couples (i, j)) et il contient donc un seul sous-groupe d'ordre p (sinon il y a au moins p^2 éléments), qu'il normalise, et il est donc inclus dans le groupe affine de $\mathbf{Z}/p\mathbf{Z}$ en vertu de 5.53. On conclut [75] par §5.6.4.

5.56 *Exemple.* Galois donne un exemple avec $p = 5$, qui est exactement le groupe affine du corps $\mathbf{F}_5$. C'est un groupe d'ordre 20 qui contient le cycle $(abcde)$, dix 4-cycles, dont $(abdc)$ et cinq doubles transpositions dont $(ad)(bc)$. Ce groupe est produit semi-direct de $\mathbf{Z}/5\mathbf{Z}$ par $\mathbf{Z}/4\mathbf{Z}$. Il ne donne pas d'équation admettant ce groupe, mais il suffit de prendre une équation binôme, par exemple $X^5 - 2$. Pour un exemple explicite avec un groupe de Galois d'ordre 10 isomorphe à $\mathbf{D}_5$, voir [10] §7.4.

5.7 Annexe : une fausse piste sur la structure des extensions radicales

On peut facilement dire des bêtises sur les extensions et les groupes résolubles. Par exemple qu'un groupe résoluble admet toujours un sous-groupe distingué d'ordre premier, assertion immédiatement démentie par $\mathfrak{A}_4$. Voici [76] une autre tentative avortée.

5.57 Conjecture. *(??) Soit $K \subset M_0$ une extension radicale. Il existe une suite de corps $K_0 = K \subset K_1 \subset \cdots \subset K_r = M$, avec $M_0 \subset M$, vérifiant les propriétés suivantes :*

1) Pour chaque $i = 0, \ldots, r-1$, on a $K_{i+1} = K_i(\alpha_i)$ avec $\alpha_i^{p_i} = a_i$ où p_i est premier, $a_i \in K_i$ mais $\alpha_i \notin K_i$.

2) L'extension $K \subset K_i$ est normale pour tout $i = 1, \ldots, r$.

On dira alors que l'extension $K \subset M$ est **hautement radicale**.

75. *Donc etc.* dit-il !

76. Ce paragraphe n'est présent que pour éviter au lecteur de dire les mêmes bêtises que l'auteur !

La conjecture 5.57 est fausse, voici comment bâtir un contre-exemple.

5.58 Définition. *Un groupe G est dit* **hautement résoluble** *s'il existe une suite de sous-groupes $G_0 = \{1\} \subset G_1 \subset \cdots \subset G_r = G$ tels que chaque G_i soit distingué dans G et chaque quotient G_{i+1}/G_i soit d'ordre premier.*

5.59 *Remarques.* Le groupe de Galois d'une extension hautement radicale est hautement résoluble.

2) Un groupe nilpotent est hautement résoluble, $\mathfrak{S}_3$ est hautement résoluble non nilpotent, $\mathfrak{A}_4$ est résoluble mais pas hautement résoluble.

Le lemme crucial est alors :

5.60 Lemme. *Un quotient d'un groupe hautement résoluble l'est aussi.*

Démonstration. Soit $p : G \to H$ surjectif. Alors les $p(G_i) = H_i$ distincts donnent la suite cherchée pour H.

5.7.1 Un contre-exemple

On considère le polynôme $P(X) = X^4 - 8X + 12$. On sait, voir [10] 6.11, que le groupe de Galois sur $\mathbf{Q}$ de ce polynôme est $\mathfrak{A}_4$. On considère le corps de décomposition de ce polynôme sur $\mathbf{Q}(j)$. Le polynôme P est encore irréductible sur $\mathbf{Q}(j)$ (voir lemme ci-dessous) ainsi que la résolvante $R(X) = X^3 - 48X - 64$ (elle l'est sur $\mathbf{Q}$, voir *loc. cit.* et le reste après une extension de degré 2). Le groupe de Galois de P sur $\mathbf{Q}(j)$ est donc encore $\mathfrak{A}_4$, l'extension est résoluble, elle contient les racines cubiques de 1, donc elle est radicale. Pourtant, elle ne peut se plonger dans une extension hautement radicale, sinon son groupe serait hautement résoluble.

5.61 Lemme. *Le polynôme $X^4 - 8X + 12$ est irréductible sur $\mathbf{Q}(j)$.*

Démonstration. Comme $\mathbf{Z}[j]$ est principal, il suffit de voir que le polynôme est irréductible sur $\mathbf{Z}[j]$. Montrons d'abord qu'il n'a pas de racine $a + bj$, $a, b \in \mathbf{Z}$. Sinon, on aurait les deux équations :

$$a^4 - 6a^2b^2 + 4ab^3 - 8a + 12 = 0 \quad \text{et} \quad 4a^3b - 6a^2b^2 + b^4 - 8b = 0.$$

Comme P n'a pas de racine dans $\mathbf{Q}$ on a $b \neq 0$ ce qui donne $4a^3 - 6a^2b + b^3 - 8 = 0$. La première équation montre que a est pair, la seconde que b l'est aussi. Mais alors 12 serait multiple de 16 ce qui est absurde.

Supposons que P soit de la forme QR avec $Q, R \in \mathbf{Z}[j][X]$ de degré 2. On réduit modulo 5. Comme 5 n'est pas de la forme $x^2 + x + 1$, il est premier dans $\mathbf{Z}[j]$, donc $\mathbf{Z}[j]/(5)$ est le corps $\mathbf{F}_{25}$. Mais, P admet la racine 1 dans $\mathbf{F}_5$

et on a $P(X) = X^4 + 2X + 2 = (X-1)(X^3 + X^2 + X - 2)$. On vérifie que ce dernier polynôme n'a pas de racine dans $\mathbf{F}_5$, donc est irréductible et il le reste sur $\mathbf{F}_{25}$. Mais cela contredit l'existence d'une décomposition $P = QR$ avec des polynômes de degré 2 sur $\mathbf{F}_{25}$.

6 La lettre de la veille

Il s'agit de la lettre écrite par Galois à son ami Auguste Chevalier le 29 mai 1832, c'est-à-dire la veille de sa mort. C'est un texte absolument extraordinaire. Comme il le dit par un doux euphémisme : *J'ai fait en analyse plusieurs choses nouvelles.*

6.1 Le début

Il revient sur la résolution des équations par radicaux et notamment sur les propositions II et III du premier mémoire (voir ci-dessus 5.35 et 5.38) en notant qu'il y a une grande différence entre adjoindre une racine d'une équation auxiliaire et les adjoindre toutes. Je cite *in extenso* ce qu'il dit :

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 $G = H + HS + HS' + \cdots$. Et aussi il peut se décomposer en groupes qui ont tous les mêmes substitutions, en sorte que $G = H + TH + T'H + \cdots$. Ces deux genres de décompositions ne coïncident pas ordinairement. Quand ils coïncident, la décomposition est dite propre.

Voilà ce que je comprends. On a la situation de 5.33 : $K \subset L = D_K(P) = K(x_1, \ldots, x_n)$, $G = \mathrm{Gal}(L/K)$ et on adjoint une racine[77] α d'une équation auxiliaire Q. On obtient une extension intermédiaire $K \subset M \subset L$. À une telle extension est associée le sous-groupe $H = \mathrm{Gal}(L/M)$ de G.

77. Il y a là un point qui n'est pas clair : α peut être dans L ou non. Nous supposerons ici que α est dans L (et donc aussi les autres racines de Q puisque L/K est normale), voir ci-dessus 5.43. Sinon il faudrait considérer l'extension composée LM.

Galois considère alors les deux décompositions de G en classes à droite et à gauche selon H : $G = H + HS + HS' + \cdots$ et $G = H + TH + T'H + \cdots$. Trois remarques ici.

1) Il appelle "groupes " les classes. Du point de vue actuel c'est au moins un abus de langage, mais cela montre bien que les notions ne sont pas encore complètements stabilisées pour lui.

2) Il note + la réunion.

3) Il a deux vocables pour désigner ces classes. Pour les classes à droite : *on passe de l'un à l'autre par une même substitution*, on passe de H à HS en appliquant S, c'est bien normal. Pour les classes à gauche : *il peut se décomposer en groupes qui ont tous les mêmes substitutions*. J'avoue que je ne comprends pas exactement le sens de ces mots.

Ce qui est clair, en revanche, c'est ce que signifie *décomposition propre* : cela signifie que les classes à gauche et à droite sont égales, donc que H est un sous-groupe distingué de G et Galois a parfaitement compris [78] que cela correspond au fait que M est une extension normale de K donc que l'on adjoint **toutes** les racines de Q.

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 transformations.

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 groupe de N permutations.

Ici Galois évoque le dévissage de l'extension en deux extensions galoisiennes $K \subset M$ et $M \subset L$ lorsque H est distingué et note que ce n'est pas possible si le groupe est **simple** (c'est-à-dire n'a pas de sous-groupe distingué ou encore aucune décomposition propre) .

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.

En quelques lignes il énonce le résultat essentiel : l'équation est résoluble si et seulement si, lorsqu'on dévisse son groupe de Galois au moyen de sous-groupes distingués, on finit à des groupes d'ordre premier. En termes mo-

78. Tous ceux qui ont enseigné la théorie de Galois savent que ces questions de normalité sont une difficulté importante pour les étudiants.

dernes : si le groupe de Galois est un groupe résoluble !

Il conclut en donnant le plus petit exemple de groupe non résoluble :

Le plus petit nombre de permutations que puisse avoir un groupe indécomposable, quand ce nombre n'est pas premier est 3.4.5.

Il s'agit bien sûr du groupe alterné $\mathfrak{A}_5$.

6.2 Les équations primitives

On renvoie au §9 pour des précisions sur ce thème. Galois annonce deux résultats :

1) *Pour qu'une équation primitive soit soluble par radicaux, elle doit être du degré p^ν, p premier.* Voir ci-dessous 9.10.

2) Il donne ensuite la forme du groupe d'une équation primitive. En termes modernes, il est plongé dans le groupe affine $GA(\nu, \mathbf{F}_p)$, dont il donne le cardinal, produit de p^ν (les translations) par $(p^\nu - 1)(p^\nu - p)\cdots(p^\nu - p^{\nu-1})$ (le groupe $GL(\nu, \mathbf{F}_p)$).

Il dit simplement que les équations de ce type ne sont pas toutes résolubles et que la condition donnée dans le *Bulletin de Férussac* est trop restreinte.

6.3 Le groupe $PGL(2, \mathbf{F}_p)$

Galois évoque ensuite les extensions (provenant des équations liées aux fonctions elliptiques) dont le groupe est formé des transformations $\dfrac{az+b}{cz+d}$ avec $z = 0, 1, \ldots, p-1, \infty$, le tout pris modulo p, c'est-à-dire le groupe qu'on note aujourd'hui $PGL(2, \mathbf{F}_p)$ et qui est bien de cardinal $p(p^2-1)$ comme il le dit.

Il décompose ce groupe en utilisant son sous-groupe $PSL(2, \mathbf{F}_p)$, de cardinal moitié (il explique que ce sont les homographies dont le déterminant $ad - bc$ est un résidu quadratique, c'est vrai !). Il dit ensuite (évidemment sans démonstration) que ce groupe n'est plus décomposable, sauf si $p = 2$ ou 3, autrement dit, il annonce que $PSL(2, \mathbf{F}_p)$ est simple sauf pour $p = 2$ ou 3 ! ! ! Là encore, c'est le bon résultat.

Il étudie alors la question suivante : le degré de ce groupe peut-il s'abaisser à p (autrement dit, ce groupe peut-il opérer sur un ensemble de cardinal p ?). Dans ce cas les stabilisateurs seraient de cardinal $(p^2-1)/2$. C'est ce que dit Galois : *il faut pour cela que le groupe se décompose (improprement s'entend) en p groupes de $(p+1)(p-1)/2$ permutations chacun.*

Pour voir cela, il regarde le stabilisateur commun de 0 et de ∞, ce sont les homothéties $z \mapsto a^2 z$. Il dit ensuite que cette réduction n'est possible que pour $p = 5, 7, 11$. Je ne comprends pas tout à fait son argument, mais il a

raison ! Dans le cas $p = 5$ on sait que le groupe $PSL(2, \mathbf{F}_5)$ est isomorphe à $\mathfrak{A}_5$ et il opère bien sur 5 éléments. Dans le cas $p = 7$, le groupe $PSL(2, \mathbf{F}_7)$ à 168 éléments est isomorphe à $PSL(3, \mathbf{F}_2)$ qui opère sur $\mathbf{F}_2^3 - \{0\}$, de cardinal 7. Enfin, $PSL(2, \mathbf{F}_{11})$ opère aussi sur un ensemble à 11 éléments. En effet, c'est un groupe de cardinal 660 qui admet des sous-groupes d'ordre 60 isomorphes à $\mathfrak{A}_5$, voir :

`https://groupprops.subwiki.org/wiki/Subgroup_structure_of_projective_special_linear_group:PSL(2,11)`

En revanche, pour $p = 13$, le groupe est d'ordre $1092 = 2^2 \times 3 \times 7 \times 13$ et il n'a pas de sous-groupe d'ordre 84.

Là encore, on ne peut qu'admirer la profondeur de vues de Galois.

7 Abel, Galois et l'algèbre moderne

7.1 Une liste de notions actuelles absentes

Parmi les notions familières aux mathématiciens actuels, beaucoup sont absentes des œuvres d'Abel et de Galois (ce qui rend d'autant plus remarquable leur travail). Nous allons les énumérer puis analyser si elles sont présentes de manière implicite et si elles sont essentielles.

• **Corps**

Cette notion est implicite dans toute l'œuvre d'Abel et de Galois, voir les détails ci-dessous.

• **Corps de rupture, de décomposition**

Le fait de disposer du corps $\mathbf{C}$ des nombres complexes permet souvent de se passer de ces notions. Voir cependant le travail de Galois sur les corps finis.

• **Groupes**

Abel n'utilise pas cette notion, sauf, de manière implicite, avec le groupe des permutations. Galois introduit le mot, même si sa signification exacte n'est pas toujours claire. On peut aussi repérer dans Galois de manière implicite les notions de sous-groupe distingué (avec la notion de décomposition propre) et de groupe résoluble (notamment dans la lettre de la veille), voir §6.1.

• **Homomorphismes, automorphismes**

Ces notions ne sont vraiment pas présentes chez Galois. Elles permettent pourtant une définition plus conceptuelle du groupe de Galois.

• **Classes**

Galois utilise des classes à gauche et à droite, notamment dans la fameuse lettre (en les appelant "groupes"). La notion de conjugaison est aussi sous-

jacente, mais pas formulée comme telle.

• **Espaces vectoriels**

Ni l'un ni l'autre n'ont cette notion, ni celle de dimension. C'est sans doute l'un des points qui permettrait d'éclaircir nombre de résultats, voir plusieurs exemples ci-dessous.

• **Extensions normales**

Dans la théorie de Galois moderne, c'est une notion essentielle. Ici, comme les extensions dont s'occupe Galois sont essentiellement engendrées par des radicaux, elle est souvent occultée par l'hypothèse implicite de présence de suffisamment de racines de l'unité. Cependant, dans la lettre de la veille, il est parfaitement clair sur ce point, voir §6.1, ainsi que sur le lien de cette notion avec les sous-groupes distingués.

7.2 Discussion

7.2.1 Corps *versus* quantités rationnelles

Le mot corps ne fait pas partie du vocabulaire d'Abel et Galois, mais la notion est bien présente. C'est particulièrement clair dans le mémoire d'Abel au Journal de Crelle. Voilà ce qu'il dit :

Soient $x', x'', x''', \ldots$ un nombre fini de quantités quelconques. On dit que v est une fonction algébrique de ces quantités, s'il est possible d'exprimer v en $x', x'', x''', \ldots$ à l'aide des opérations suivantes. 1. par l'addition ; 2. par la multiplication soit des quantités dépendantes de $x', x'', x''', \ldots$ soit des quantités qui n'en dépendent pas ; 3. par la division ; 4. par l'extraction des racines avec des exposants premiers. Parmi ces opérations nous n'avons pas compté la soustraction, l'élévation à des puissances entières et l'extraction des racines avec des exposants composés, car elles sont évidemment comprises dans les quatre opérations mentionnées.

Il distingue ensuite trois types de fonctions : les fonctions entières, obtenues par addition et multiplication, les fonctions rationnelles, en ajoutant la division, et algébriques, avec en plus les racines, autrement dit l'anneau engendré par $x', x'', x''', \ldots$, le corps engendré, puis une extension de celui-ci.

Galois ajoute à cela la nécessité de préciser un "corps de base" : *Il y a plus : on pourra convenir de regarder comme rationnelle toute fonction rationnelle d'un certain nombre de quantités déterminées, supposées connues a priori. Par exemple, on pourra choisir une certaine racine d'un nombre entier, et regarder comme rationnelle toute fonction rationnelle de ce radical.* Il explicite aussi la notion d'adjonction : *Lorsque nous conviendrons de regarder ainsi comme connues de certaines quantités, nous dirons que nous les adjoignons à l'équation qu'il s'agit de résoudre. ...*

Cela posé nous appellerons rationnelle toute quantité qui s'exprimera en fonction rationnelle des coefficients de l'équation et d'un certain nombre de quantités adjointes à l'équation ...

L'exemple type de cette démarche est son résultat sur les équations de degré premier :

Pour qu'une équation irréductible de degré premier soit résoluble par radicaux, il faut et il suffit que deux des racines étant connues, les autres s'en déduisent rationnellement.

En termes modernes, si $x_1, \ldots, x_p$ sont les racines du polynôme et si x_i, x_j en sont deux particulières, le corps de décomposition $L = D_K(P) = K(x_1, \ldots, x_p)$ est égal à $K(x_i, x_j)$.

7.2.2 Le groupe de Galois

Nous avons vu en 5.29 la définition du groupe de Galois d'une équation, comme le groupe de permutations dont (en termes modernes) le corps fixe est le corps de base. La scolie 2 qui suit cette introduction (*Les substitutions sont indépendantes même du nombre des racines*) semble bien montrer que Galois a l'intuition d'un groupe qui ne dépend pas de l'équation. Ici, c'est évidemment la notion d'automorphisme du corps qui est pertinente, mais elle n'est pas du tout présente dans le travail de Galois.

L'un des intérêts majeurs de l'utilisation du groupe de Galois sous la forme automorphismes apparaît dans la fin de la preuve d'Abel. Il a écrit une racine x du polynôme P grâce à un radical α avec $\alpha^p = a$, $a \in K$: $x = a_0 + a_1\alpha + \cdots + a_{p-1}\alpha^{p-1}$ et il s'agit de montrer que, si ζ désigne une racine primitive p-ième de 1, $x' = a_0 + a_1\zeta\alpha + \cdots + a_{p-1}\zeta^{p-1}\alpha^{p-1}$ est une autre racine de P. Avec le groupe de Galois c'est évident : les racines de P sont les conjugués de x, donc de la forme $\sigma(x)$ avec $\sigma \in \mathrm{Gal}(L/K)$ et, comme σ est un automorphisme, il vérifie $\sigma(\alpha^p) = \sigma(\alpha)^p = \sigma(a) = a$ puisque a est fixe par σ (et aussi $\sigma(a_i) = a_i$). On a donc $\sigma(\alpha) = \zeta\alpha$ et le résultat. On comparera avec la preuve d'Abel, voir ci-dessus 3.20.

7.2.3 La notion d'espace vectoriel

Il faut se souvenir que la notion d'espace vectoriel n'existe pas à l'époque d'Abel et de Galois : c'est Grassmann qui l'introduira le premier (dans l'*Ausdehnunglehre*, 1862), mais son travail sera peu connu de ses contemporains. Il semble bien que la notion ne s'imposera vraiment qu'au début du XX-ième siècle avec Emmy Noether. Cependant, guère plus tard que Galois, Riemann manipulait les notions d'indépendance linéaire et de base (sans aucune formalisation) à propos des solutions d'équations différentielles.

Ces notions, que l'on peut considérer comme l'essentiel de l'algèbre linéaire, n'étaient donc pas si éloignées de nos héros.

En plusieurs endroits, l'utilisation de ces notions eut grandement simplifié leurs preuves. Par exemple, dans le mémoire d'Abel, pour montrer que si α est un radical toute fraction rationnelle en α est aussi un polynôme, la voie moderne consiste à regarder la multiplication par un élément non nul de $K(\alpha)$ comme une application linéaire et à utiliser le fait qu'en dimension finie, injectif implique surjectif, voir 3.17.

De même, la preuve (que d'ailleurs Galois ne donne pas) du fait que si le groupe de Galois de P diminue par adjonction d'un radical, ce radical est dans le corps de décomposition de P, est immédiate avec le théorème de la base télescopique (ou de multiplicativité des degrés, c'est-à-dire des dimensions), résultat très simple d'algèbre linéaire, voir 5.43.

Enfin, c'est encore le cas de la preuve de 5.48, qui repose aussi sur la base télescopique.

7.2.4 Les corps finis

Le travail de Galois sur les corps finis apparaît dans le texte *Sur la théorie des nombres* paru en juin 1830 dans le *Bulletin des Sciences Mathématiques* de M. Férussac. Le but de Galois dans ce texte est de donner des outils pour l'étude des équations primitives, voir ci-dessous §9. Dans ce travail Galois montre que si une équation primitive est résoluble par radicaux, son degré est une puissance de nombre premier (voir ci-dessous 9.10). Son but est d'avoir un ensemble d'indices de cardinal p^n et il lui sera donné, en termes modernes, par le corps $\mathbf{F}_{p^n}$, le groupe de Galois, dans le cas considéré, étant le groupe affine de ce corps, isomorphe à $\mathbf{F}_{p^n} \rtimes (\mathbf{F}_{p^n})^*$. Voilà ce que dit Galois :

C'est surtout dans la théorie des permutations, où l'on a sans cesse besoin de varier la forme des indices, que la considération des racines imaginaires des congruences paraît indispensable.

La question traitée est la suivante. On travaille modulo un nombre premier p avec une équation (polynomiale) dont on cherche les solutions en termes de congruences [79] : $F(x) \equiv 0 \pmod{p}$, essentiellement dans le cas où il n'y a pas de solutions "commensurables" (i.e. pas de solutions dans $\mathbf{Z}/p\mathbf{Z}$). Autrement dit, il regarde $F \in \mathbf{F}_p[X]$ irréductible de degré n. Il dit :

Il faut donc regarder les racines de cette congruence comme des espèces de symboles imaginaires, puisqu'elles ne satisfont pas aux questions des nombres entiers, symboles dont l'emploi, dans le calcul, sera souvent aussi utile que celui de l'imaginaire $\sqrt{-1}$ dans l'analyse ordinaire.

79. La notation $a \equiv b \pmod{p}$ est due à Gauss.

Si i est l'une des racines de la congruence, il regarde les expressions :

$$\alpha = a + a_1 i + a_2 i^2 + \cdots + a_{n-1} i^{n-1}.$$

C'est bien sûr ce qu'on appelle aujourd'hui le corps de rupture de F, qui doit plus ou moins exister à l'époque sous forme de "théorie des résidus de puissances". En particulier, il dit un peu plus loin que toute expression polynomiale (par exemple α élevé à une certaine puissance) peut de ramener au degré $n-1$ "parce que toute fonction de i peut se réduire au $(n-1)$-ième degré".

Notons $\mathbf{F}_{p^n}$ l'ensemble de ces symboles "imaginaires". Galois regarde ensuite le groupe multiplicatif $\mathbf{F}_{p^n}^*$ et dit qu'il existe N tel que $\alpha^N = 1$ pour tout α et démontre (comme on montre le théorème de Lagrange) que N divise $p^n - 1$, donc qu'on a $\alpha^{p^n} = \alpha$ pour tout α. Il affirme aussi l'existence de racines primitives (donc le fait que ce groupe est cyclique) et le fait que tous les éléments de $\mathbf{F}_{p^n}$ vérifient $x^{p^n} = x$. Il note aussi que cette équation n'a pas de racines multiples [80] en invoquant la dérivée (dans un cadre inhabituel à l'époque).

Il donne l'exemple de $\mathbf{F}_{7^3}$ qui est le corps de rupture de $x^3 - 2$. Si x est une racine, il dit que $x - x^2$ est d'ordre 342 (x est d'ordre 9, -1 d'ordre 2 et $x - 1$ d'ordre 19 et $9 \times 2 \times 19 = 342$).

Tout de même, ce Galois, quel homme !

8 Annexe 1 : quelques questions subsidiaires

8.1 Éliminer les extensions cyclotomiques

Bien sûr, s'agissant des équations cyclotomiques $x^n = 1$, on pourrait se contenter de dire qu'elles sont résolubles par radicaux, les racines de l'unité elles-mêmes étant des radicaux. En fait, on a un résultat plus précis [81].

8.1 Définition. *Soit K un corps de caractéristique zéro et $K \subset L$ une extension. On dit que l'extension est* **fortement résoluble** *si L est contenue dans une extension radicale dont tous les étages $K_i \subset K_{i+1}$ sont engendrés par des radicaux α_i avec $\alpha_i^{p_i} = a_i$, $a_i \in K_i$, $a_i \neq 1$ et $p_i \leq n$.*

8.2 Proposition. *Soit K un corps de caractéristique zéro et $K \subset L$ une extension galoisienne résoluble. Alors elle est fortement résoluble.*

80. Donc qu'elle est séparable.

81. Dû sans doute à Gauss dans le cas cyclotomique et important dans le travail de Galois, voir 5.42 ci-dessus.

8.3 Corollaire. *Soient n un entier ≥ 1 et ζ une racine n-ième primitive de l'unité dans $\mathbf{C}$. Alors l'extension $\mathbf{Q} \subset \mathbf{Q}(\zeta)$ est fortement résoluble (et les hauteurs p_i des étages au sens de 8.1 sont $< n$).*

Démonstration. (de la proposition) On raisonne par récurrence sur le degré n de l'extension. Le résultat est évident pour $n = 2$. Pour le pas de récurrence, il y a deux cas. Si le groupe de Galois $G := \mathrm{Gal}(L/K)$ n'est pas simple on a un corps intermédiaire M et on applique l'hypothèse de récurrence aux extensions $K \subset M$ et $M \subset L$. Si G est simple, comme il est résoluble, il est cyclique d'ordre premier p. Si K contient les racines p-ièmes de l'unité on conclut par [10] 4.13. Sinon, on adjoint une racine primitive p-ième ζ et, comme elle est de degré $\leq p-1$, on conclut grâce à l'hypothèse de récurrence.

8.4 *Exemples.* Prenons les n dans l'ordre. Pour $n = 1, 2$ on a $\mathbf{Q}(\zeta) = \mathbf{Q}$, pour $n = 3$, $\mathbf{Q}(j) = \mathbf{Q}(\sqrt{-3})$, pour $n = 4$ c'est $\mathbf{Q}(\sqrt{-1})$. Pour $n = 5$ on a une tour à deux étages : $\mathbf{Q} \subset \mathbf{Q}(\sqrt{5}) \subset \mathbf{Q}(\zeta)$ et, si l'on pose $\alpha = \frac{-1+\sqrt{5}}{2}$, le deuxième étage est engendré par $\sqrt{\alpha^2 - 4}$. Pour $n = 6$, on a $\mathbf{Q}(\zeta) = \mathbf{Q}(\sqrt{-3})$. Pour $n = 7$, les choses se compliquent. On pose $\alpha = \zeta + \zeta^{-1}$. On a l'équation $\alpha^3 + \alpha^2 - 2\alpha - 1 = 0$. On pose $\beta = \alpha + 1/3$ et on obtient $\beta^3 - \frac{7}{3}\beta - \frac{7}{27} = 0$. On résout par Cardan en posant $x = u + v$ avec $uv = 7/9$ et on obtient $u^3 = \dfrac{7 + 21i\sqrt{3}}{2 \times 27}$ de sorte que la tour pertinente est la suivante : $\mathbf{Q} \subset \mathbf{Q}(\sqrt{-3}) \subset \mathbf{Q}(u) = \mathbf{Q}(\beta) = \mathbf{Q}(\alpha) \subset \mathbf{Q}(\alpha, \sqrt{\alpha^2 - 4})$.

Pour $n = 8$, on a $\zeta = \dfrac{(1+i)\sqrt{2}}{2}$ et la tour est $\mathbf{Q} \subset \mathbf{Q}(\sqrt{2}) \subset \mathbf{Q}(\sqrt{2}, i) = \mathbf{Q}(\zeta)$.

Le cas de $n = 11$ est intéressant. En posant $\alpha = \zeta + \zeta^{-1}$ on obtient une équation de degré 5 en α dont le groupe de Galois est $\mathbf{Z}/5\mathbf{Z}$ et qui est donc résoluble. Voici cette équation : $\alpha^5 + \alpha^4 - 4\alpha^3 - 3\alpha^2 + 3\alpha + 1 = 0$. Mais trouver la résolvante et la racine cinquième correspondante est une autre histoire.

8.2 Sur la normalité des extensions radicales

La question est la suivante. On suppose que K contient toutes les racines de l'unité. Une extension radicale de K est-elle automatiquement normale ? Il n'en est rien comme le montre l'exemple suivant.

8.5 *Exemple.* On considère le sous-corps K_0 de $\mathbf{C}$ engendré par toutes les racines de l'unité et le corps $K = K_0(x)$ engendré par un élément transcendant x de $\mathbf{C}$ (par exemple π). On considère l'extension radicale $K \subset L$ obtenue en prenant d'abord $K_1 = K(\sqrt{x})$, puis $L = K_1(\sqrt{1 + \sqrt{x}})$. Alors, l'extension $K \subset L$ n'est pas normale. En effet, posons $t = \sqrt{x}$. Comme t

est transcendant sur $\mathbf{Q}$, donc aussi sur K, le corps $K(t)$ est le corps des fractions rationnelles en t et $1+t$ n'est pas un carré de $K(t)$. L'extension $K(t) \subset K(\sqrt{1+t})$ est donc de degré 2 et le polynôme minimal de $\sqrt{1+t}$ sur K est $X^4 - 2X^2 + 1 - x$ et il est irréductible. Le nombre $\sqrt{1-t}$ est un des conjugués de $\sqrt{1+t}$ et il n'est pas dans L. En effet, dire que $1-t$ est un carré de $L = K(\sqrt{1+t})$ signifie que $1-t$ ou $(1+t)(1-t)$ est un carré de $K(t)$ et ce n'est pas le cas.

9 Annexe 2 : Les équations primitives

Ce sujet est essentiellement abordé dans le (fragment du) second mémoire, p. 434-444 des œuvres (non daté). Mais, avant cela, p. 395-397 des œuvres, il y a un article publié en avril 1830 dans le *Bulletin des sciences mathématiques* de M. Férussac que je résume ci-dessous.

9.1 L'article de 1830

Il commence ainsi :

On appelle équations non primitives les équations qui étant, par exemple, du degré mn, se décomposent en m facteurs du degré n au moyen d'une seule équation du degré m. Ce sont les équations de M. Gauss.

Pour une explication, voir 9.6.

Dans cet article Galois énonce, sans démonstration, les résultats suivants sur les équations primitives :

1) Pour qu'une équation de degré premier soit résoluble par radicaux il faut et il suffit que deux quelconques de ses racines étant connues, les autres s'en déduisent rationnellement.

2) Pour qu'une équation primitive du degré m soit résoluble par radicaux, il faut que $m = p^\nu$, p étant un nombre premier.

3) À part les cas mentionnés ci-dessous, pour qu'une équation primitive du degré p^ν soit résoluble par radicaux, il faut que deux quelconques de ses racines étant connues, les autres s'en déduisent rationnellement.

À la règle précédente échappent les cas particuliers suivants : $m = p^\nu = 9$ ou 25, le cas $m = 4$ et généralement celui où, a^α étant un diviseur de $\dfrac{p^\nu - 1}{p-1}$ on aurait a premier et $\dfrac{p^\nu - 1}{a^\alpha(p-1)}\nu \equiv p \pmod{a^\alpha}$.

On reconnaît le point 1) qui est le résultat principal du premier mémoire, le point 2) qui est dans le second. Le point 3) (notamment le cas avec a^α)

est obscur pour moi [82].

9.2 La notion de groupe primitif

9.2.1 La définition

9.1 Définition. *Soit G un groupe opérant sur un ensemble X de manière transitive. On dit que l'opération est* **imprimitive** *s'il existe une partition $X = X_1 \cup \cdots \cup X_r$ non triviale (i.e. non réduite à un élément et dont les composants ne sont pas tous des singletons) stable par G (autrement dit, si $g \in G$, pour chaque $i = 1, \ldots, r$ il existe j tel que $g(X_i) = X_j$). Dans le cas contraire on dit que l'opération est* **primitive**.

9.2 *Remarques.* 1) Si le groupe est imprimitif, les composants X_i ont tous même cardinal car le groupe opère transitivement sur l'ensemble X, donc aussi sur $Y := \{X_1, \ldots, X_r\}$.

2) Soit $x \in X_i$, S le stabilisateur de x et H celui de X_i. On a $S \subset H \subset G$ et $S \neq H \neq G$. La dernière assertion résulte de $X \simeq G/S$, $Y \simeq G/H$ et des hypothèses de non trivialité.

9.2.2 L'exemple générique

En fait, une opération imprimitive correspond exactement à la situation ci-dessus :

9.3 Lemme. *Soit G un groupe, S un sous-groupe non maximal et H un sous-groupe contenant S et distinct de S et de G. Alors l'opération de G sur $X := G/S$ est imprimitive et l'ensemble Y des sous-ensembles de la partition est isomorphe à G/H. Toute opération imprimitive est isomorphe à une opération de ce type.*

Démonstration. En effet, une partition stable de X s'obtient ainsi. On considère G/H et on écrit $G/H = \{g_1H = H, g_2H, \ldots, g_rH\}$. On considère ensuite $H/S = \{h_1S, \ldots, h_sS\}$. La partition de X est formée par les ensembles $X_i = \{g_ih_1S, \ldots, g_ih_sS\}$. C'est une partition de G/S car les X_i sont formés de classes modulo S et si $g_ih_jS = g_kh_lS$, comme h_jS et h_lS sont contenus dans H, dire que les éléments sont égaux oblige $g_i = g_k$. Il reste $h_jS = h_lS$ et cela impose $h_j = h_l$.

82. Il est d'ailleurs incorrect, comme le note Jordan, voir [6] : *Galois avait annoncé que les équations primitives et solubles par radicaux rentreraient dans un type unique, sauf pour le neuvième et le vingt-cinquième degré, qui présenteraient certains types exceptionnels. On voit par les énoncés qui précèdent qu'il faut prendre presque exactement le contre-pied de cette assertion.*

Soit g dans G. On sait que g permute les classes modulo H : pour tout i il existe k tel que $gg_iH = g_kH$. Soit g_ih_jS un élément de X_i. Alors, pour tout j, gg_ih_jS est une des classes modulo S et elle est dans g_kH, donc dans X_k : la partition est stable.

L'assertion d'universalité résulte de la remarque 9.2.2.

9.4 *Remarque.* Dans la situation précédente, une question importante est de savoir si le stabilisateur d'un X_i est distingué. Comme G est transitif sur les X_i, les stabilisateurs sont conjugués et ils ne peuvent être distingués que s'ils sont égaux, auquel cas ils sont égaux au stabilisateur de **tous** les X_i. Manifestement, Galois n'examine que ce cas, voir ci-dessous.

Voici deux exemples qui éclairent cette question.

9.5 *Exemples.* 1) On prend $G = \mathfrak{A}_5$, S l'un de ses 5-Sylow, engendré par $\sigma := (12345)$ et pour H le normalisateur $\mathbf{D}_5$ de S dans $\mathfrak{A}_5$, qui est engendré par σ et par $(25)(34)$. C'est un exemple où H n'est pas distingué.

2) On pourrait se demander si, lorsque G est un groupe résoluble et S un sous-groupe non maximal, il existe toujours H avec $S \subset H \subset G$ et H distingué dans G. Il n'en est rien. En effet, on considère $G = \mathfrak{S}_4$ et le sous-groupe $S = \{\mathrm{Id}, (13), (24), (13)(24)\}$. C'est un groupe de Klein, contenu dans $\mathfrak{S}_4$, non maximal car il est contenu dans le groupe diédral :

$$\mathbf{D}_4 = \{\mathrm{Id}, (1234), (13)(24), (1432), (12)(34), (14)(23), (13), (24)\}$$

et non contenu dans un sous-groupe distingué. On verra ci-dessous ce que donne cet exemple sur les extensions. Un autre exemple est le sous-groupe cyclique d'ordre 4 engendré par (1234).

9.3 Traduction sur les extensions

9.3.1 La situation évoquée par Galois

Nous tentons d'expliquer dans ce paragraphe la phrase par laquelle commence l'article de 1830 (voir 9.1) : *On appelle équations non primitives les équations qui étant, par exemple, du degré mn, se décomposent en m facteurs du degré n au moyen d'une seule équation du degré m. Ce sont les équations de M. Gauss.* On a, en tous cas, le théorème suivant :

9.6 Théorème. *Soit K un corps, P un polynôme irréductible de degré n à coefficients dans K, $L = D_K(P)$ le corps engendré par les racines $x_1, \ldots, x_n$ de P, G le groupe de Galois de L sur K. Soit M une extension* **normale** *de K. On suppose que P est réductible sur M. On a vu en 5.35 qu'il est alors décomposé en $P = P_1 \cdots P_r$ avec des $P_i \in M[X]$, tous de même degré d.*

Alors, si les P_i ne sont pas de degré 1, l'opération de G sur $X = \{x_1, \ldots, x_n\}$ est imprimitive et la partition associée est formée des racines de chaque P_i.

Démonstration. Soit X_i l'ensemble des racines de P_i et soient $x, y \in X_i$. Soit $g \in G$. On suppose que $g(x)$ est dans X_j (donc racine de P_j) et il s'agit de montrer que $g(y)$ est aussi dans X_j.

Pour cela, on considère $LM = D_M(P)$. Le groupe G est un quotient de $\mathrm{Gal}(LM/K)$ tandis que $\mathrm{Gal}(LM/M)$ en est un sous-groupe distingué (car M est normale). On relève g en $\widehat{g} \in \mathrm{Gal}(LM/K)$ et on a donc $\widehat{g}|_L = g$. Comme x et y sont racines de P_i irréductible sur M il existe $\tau \in \mathrm{Gal}(LM/M)$ tel que $\tau(x) = y$. Comme $\mathrm{Gal}(LM/M)$ est distingué dans $\mathrm{Gal}(LM/K)$, $\sigma := \widehat{g}\tau\widehat{g}^{-1}$ est dans ce sous-groupe. On a $\sigma(g(x)) = g(y)$ de sorte que ces éléments sont conjugués sur M, donc que $g(y)$ est racine de P_j.

9.7 *Remarques.* 1) On notera qu'ici, le stabilisateur de X_i est (l'image de) $\mathrm{Gal}(LM/M)$ et qu'il est distingué dans G.

2) D'une certaine manière il est plus difficile de dire quand une extension est primitive ! Intuitivement, cela signifie qu'on ne peut casser P sans le réduire en miettes, i.e. en morceaux de degré 1.

9.8 *Exemples.* 1) On considère le polynôme $P(X) = X^6 - 2$, irréductible sur $\mathbf{Q}$, et aussi sur $\mathbf{Q}(j)$ (par le critère d'Eisenstein appliqué à l'élément 2 de $\mathbf{Z}[j]$). Il a 6 racines dans $\mathbf{C}$: $\alpha = \sqrt[6]{2}$ (la racine réelle positive), $-\alpha$, $\pm j\alpha$ et $\pm j^2\alpha$. Soit $L = \mathbf{Q}(j, \alpha)$ son corps de décomposition. Le groupe de Galois $G := \mathrm{Gal}(L/\mathbf{Q}(j))$ est $\mathbf{Z}/6\mathbf{Z}$, engendré par $\tau(\alpha) = -j\alpha$. L'opération de G sur $X = \{\pm\alpha, \pm j\alpha, \pm j^2\alpha\}$ est doublement imprimitive, au sens où elle admet deux partitions stables. Si l'on numérote les racines α, $-\alpha$, $j\alpha$, $-j\alpha$, $j^2\alpha$ et $-j^2\alpha$ de 1 à 6, on a $\tau = (145236)$ et les deux partitions sont $\{135\}$, $\{246\}$ et $\{12\}$, $\{34\}$, $\{56\}$. Cela correspond au fait que le stabilisateur d'une racine dans l'opération est réduit à l'identité et que ce sous-groupe n'est pas maximal, majoré qu'il est par les sous-groupes (distingués) cycliques d'ordres 2 et 3 de $\mathbf{Z}/6\mathbf{Z}$.

Les extensions intermédiaires correspondant à ces sous-groupes distingués sont respectivement $\mathbf{Q}(\sqrt{2})$ et $\mathbf{Q}(\sqrt[3]{2})$ et les décompositions de P correspondantes sont $X^6 - 2 = (X^3 - \sqrt{2})(X^3 + \sqrt{2})$ et $X^6 - 2 = (X^2 - \sqrt[3]{2})(X^2 - j\sqrt[3]{2})(X^2 - j^2\sqrt[3]{2})$.

2) Si P est de degré 4 et de groupe $\mathfrak{S}_4$, on a le sous-groupe $H = \mathbf{V}_4$ et son corps fixe M, de degré 6 sur K. Comme $\mathbf{V}_4$ est transitif sur les x_i, P reste irréductible sur M. Voilà un exemple où l'opération est primitive bien que G ne soit pas simple.

9.3.2 Un contre-exemple

La question est de savoir si l'hypothèse de normalité de M est indispensable, autrement dit, si, pour être dans le cas évoqué par Galois, il faut que le groupe H de 9.2.2 soit distingué. L'exemple suivant montre que, sans cette hypothèse, les facteurs P_i ne sont pas nécessairement de même degré.

9.9 *Exemple.* On utilise ici les notations et les résultats de [10] p. 22-27.

On considère une extension de $\mathbf{Q}$ de groupe $\mathfrak{S}_4$, définie par une équation $P(X) = X^4+pX+q$, par exemple X^4+X+1. Appelons $x_1, \ldots, x_4$ les racines de P et $L = \mathbf{Q}(x_1, \ldots, x_4)$ le corps de décomposition. La résolvante de P est le polynôme $R(X) = X^3 - 4qX - p^2$ dont les racines sont $u_1 = x_1x_2 + x_3x_4$, $u_2 = x_2x_3 + x_1x_4$ et $u_3 = x_1x_3 + x_2x_4$. Le groupe de Galois de L sur $\mathbf{Q}(u_3)$ est le groupe diédral :

$$\mathbf{D}_4 = \{\mathrm{Id}, (1234), (13)(24), (1432), (13), (24), (12)(34), (14)(32)\}.$$

On a les formules $u_3 = (x_1 + x_3)^2 = (x_2 + x_4)^2$. Le groupe de Galois de L sur le corps $\mathbf{Q}(\sqrt{u_3}) = \mathbf{Q}(x_1 + x_3) = \mathbf{Q}(x_2 + x_4)$ est le groupe de Klein $S := \mathbf{V}_4 = \{\mathrm{Id}, (13), (24), (13)(24)\}$.

Dans ce cas, on peut préciser l'ensemble $X = G/S$, c'est l'ensemble des 6 conjugués de $x_1 + x_3$, à savoir les $x_i + x_j$, $i \neq j$. Le corps L est aussi le corps de décomposition de $R(X^2)$, de degré 6, dont les racines sont les x_i+x_j (il est clair que les x_i+x_j sont dans L et inversement, si on a les x_i+x_j on a x_1+x_2 et $x_1 + x_3$, donc $x_2 - x_3$ et comme on a aussi $x_2 + x_3$ on a bien x_2 et x_3). Le groupe de Galois est $G = \mathfrak{S}_4$, mais son opération sur les $x_i + x_j$ n'est pas primitive car on a une partition stable : $x_1 + x_3$ va avec $x_2 + x_4$ (car c'est son opposé [83]) et de même $x_1 + x_2$ avec $x_3 + x_4$ et $x_1 + x_4$ avec $x_2 + x_3$. On notera que le polynôme $R(X^2)$ est irréductible sur $\mathbf{Q}$ (car le groupe de Galois est transitif sur ses racines), mais qu'il devient réductible sur l'extension (non galoisienne) $\mathbf{Q}(u_3)$ et que sur ce corps il est produit de deux polynômes irréductibles de degrés 2 et 4 : $X^2 - u_3$ et $U(X) = X^4 - (u_1 + u_2)X^2 + u_1u_2$. Ce dernier polynôme est bien à coefficients dans $\mathbf{Q}(u_3)$ car on a $u_1+u_2 = -u_3$ et $u_1u_2 = p^2/u_3$. Il est irréductible car $\mathrm{Gal}(L/\mathbf{Q}(u_3))$ qui est le groupe $\mathbf{D}_4$ opère transitivement sur les quatre racines de U : $x_1 + x_2$, $x_3 + x_4$, $x_1 + x_4$ et $x_2 + x_3$.

9.4 Le théorème de Galois dit de manière moderne

9.10 Théorème. *On reprend les notations de 5.33 et on suppose que l'équation $P(x) = 0$ est résoluble et que l'action de G sur les x_i est primitive. Alors, n*

83. Si le coefficient $x_1 + \cdots + x_4$ n'est pas nul, les deux éléments sont tout de même liés par leur somme qui est dans $\mathbf{Q}$.

est une puissance de nombre premier.

C'est, *via* les résultats de [10], une conséquence directe de la proposition algébrique suivante :

9.11 Proposition. *Soit G un groupe fini résoluble opérant sur X de manière primitive. Alors le cardinal de X est une puissance de nombre premier.*

Vu 9.2.2, cette proposition est équivalente à la suivante :

9.12 Proposition. *Soit G un groupe fini résoluble et S un sous-groupe maximal de G. Alors, l'indice de S est une puissance de nombre premier.*

Démonstration. On raisonne par récurrence sur le cardinal n de G. Si n est premier le résultat est clair. Sinon, G admet un sous-groupe distingué non trivial N. Plus précisément, G admet un sous-groupe distingué N, qui est un p-groupe abélien. En effet, on a un sous-groupe abélien G_1 distingué en vertu de [10] 2.6.2 et si on en prend un p-Sylow N, il est distingué dans G_1 (car G_1 est abélien), donc caractéristique (car c'est un Sylow), donc distingué dans G.

On considère alors la projection $\pi : G \to \overline{G} = G/N$ et l'image $\overline{S}$ de S. Il y a deux cas.

1) Si $\overline{S} = \overline{G}$, on a $G = NS$ et la restriction à N de la projection $\varphi : G \to G/S$ est surjective. On en déduit une bijection de $N/(N \cap S)$ sur G/S et on voit que G/S a pour cardinal une puissance de p.

2) Si $\overline{S}$ est un sous-groupe strict de $\overline{G}$, c'est un sous-groupe maximal (sinon par image réciproque S ne serait pas maximal dans G) et il y a encore deux cas.

a) Si N est inclus dans S, on a une bijection de G/S sur $\overline{G}/\overline{S}$ et par l'hypothèse de récurrence, le cardinal de $\overline{G}/\overline{S}$ est une puissance de nombre premier.

b) Sinon, on considère l'ensemble NS. Comme N est distingué, NS est un sous-groupe. Il contient S, il n'est pas égal à S (sinon on serait dans le cas a) et il est distinct de G (sinon on serait dans le cas 1). C'est une contradiction avec l'hypothèse que S est maximal.

9.13 *Remarque.* En vérité, il y a beaucoup d'autres choses dans ce mémoire, que je n'ai pas complètement élucidées. Vu l'apparition, dans le cas d'une équation de degré p^2, de cardinaux du type $p^2(p^2-1)(p^2-p)$, je subodore qu'il montre que le groupe d'une telle équation se plonge dans le groupe affine de $\mathbf{F}_p^2$, mais, ...

Références

[1] Abel Niels, *Démonstration de l'impossibilité de la résolution algébrique des équations générales qui passent le quatrième degré.* Journal für die reine und angewandte Mathematik, Band 1, Berlin, 1826.
`https://gallica.bnf.fr/ark:/12148/bpt6k9800489w/f1.item`

[2] Bourbaki Nicolas, *Éléments d'histoire des mathématiques*, Hermann, 1969.

[3] Dahan-Dalmedico A., Peiffer J. *Une histoire des mathématiques*, Le Seuil, coll. Points, 1986.

[4] Galois Evariste, *Œuvres*,
`https://www.irphe.fr/~clanet/otherpaperfile/articles/Galois/N0029062_PDF_1_84.pdf`

[5] Hadlock C.-R., *Field theory and its classical problems*, The Carus Mathematical Monographs, 19, 1978.

[6] Jordan Camille, *Sur la résolution algébrique des équations primitives de degré p^2 (p étant premier impair)*, Journal de mathématiques pures et appliquées 2^e série, tome 13 (1868), p. 111-135.

[7] Lagrange Joseph-Louis, *Réflexions sur la résolution algébrique des équations*
`https://gallica.bnf.fr/ark:/12148/bpt6k229222d/f206`

[8] Lang Serge, *Algebra*, Addison-Wesley, 1965.

[9] Perrin Daniel, *Cours d'algèbre*, Ellipses, 1996.

[10] Perrin Daniel, *Résolution par radicaux*, `https://www.math.u-psud.fr/~perrin/TER/radicaux.pdf`

[11] Stewart Ian, *Galois theory*, Chapmann-Hall, 1973.

[12] Vandermonde Alexandre-Théophile, *Mémoire sur la résolution des équations*, Académie royale des sciences (1771) p. 365-416.
`https://gallica.bnf.fr/ark:/12148/bpt6k35697/f537.item`

[13] Wantzel Pierre-Laurent, *Démonstration de l'impossibilité de résoudre toutes les équations algébriques avec des radicaux*, Nouvelles annales de mathématiques 1ère série, tome 4 (1845), p. 57-65.