La théorie de Galois

par : Marquer Yoann et Raoul Martin, tuteur : Vincent Cossart

April 5, 2015

Chapter 1

Ce qu'il faut savoir

1.1 Introduction

Ce que nous appelons maintenant la théorie de Galois est l'étude des extensions des corps commutatifs en utilisant les groupes de transformations associés, qui sont appelés les groupes de Galois. Initialement, Galois a créé cette théorie pour l'étude des équations polynômiales, et notamment résoudre le problème de résolution par radicaux de ces équations. Mais elle apporte d'autres résultats, comme la construction à la règle et au compas des polygones réguliers, et elle se généralise, comme pour la théorie de Galois différentielle, où ce sont des équations différentielles et non polynômiales qui sont étudiées. La théorie de Galois intervient également dans des sujets d'actualité, comme les groupes de Galois cosmiques dans la théorie des champs en physique, qui font partie des projets en œuvre pour réconcilier relativité générale et physique quantique.

Mais la théorie initiale écrite par Galois est bien plus simple, après tout Galois lui-même était un étudiant, aussi brillant soit-il. C'est cette théorie que nous allons présenter, sous forme moderne certes, mais en respectant un maximum les preuves et les résultats de la théorie initiale et si possible uniquement ce dont Galois disposait à l'époque. Nous espérons donc que nle présent article sera accessible à des étudiants ou même des lycéens motivés. Ceux qui ont un niveau d'étude supérieur (master et plus) seront probablement intéressés par la démarche historique ainsi que par la simplicité des démonstrations, qui se résument le plus souvent à trouver un polynôme pratique permettant de déduire des propriétés, ce qui est la démarche adoptée par Galois lui-même.

Le choix d'une démarche historique est un très bon prétexte pour présenter dans ce premier chapitre une histoire des mathématiques, en tout cas pour le domaine qui nous intéresse. Ainsi, nous allons faire un "bref" état de l'art concernant la résolution des équations des degrés inférieurs à 5 avant Galois, avant de faire un "bref" exposé des outils disponibles à l'époque de Galois, notamment sur les permutations et les polynômes. Nous en profiterons pour

introduire les structures modernes (structure de groupe, d'anneau et de corps) afin que le lecteur aient toutes les cartes en main pour comprendre la suite de l'article. Ces éléments seront connus de ceux qui ont déjà certaines connaissances en mathématique, mais comme le dit Galois lui-même :

Telles sont les définitions que nous avons cru devoir rappeler. Elles paraîtront peut-être superflues. Mais nous préférons la diffusion à l'obscurité.

Enfin, nous évoquerons la (brève également) vie d'Évariste Galois, qui est intéressante en elle-même (certains diront même romantique), tout en introduisant son œuvre dans le contexte de l'époque.

Dans le second chapitre nous présentons la théorie de Galois classique, en nous inspirant de celle qu'il a présentée dans son premier mémoire intitulé "Mémoire sur les conditions de résolubilité des équations par radicaux" et daté du 16 janvier 1831. Nous ferons les démonstrations selon notre langage moderne, mais comme au paragraphe précédent nous ferons régulièrement des citations du texte original en italique, dans le but de coller à la structure originale du texte et d'expliciter, voire corriger, certaines démonstrations du texte original. En effet, ce mémoire est avant tout un premier jet, et Galois passe rapidement voire omet certaines démonstrations, et certaines sont fausses, ce qui nous a obligé à nous écarter un peu du texte.

Le troisième chapitre servira d'exemple illustratif à la théorie. Nous nous proposons d'utiliser la théorie pour construire à la règle et au compas des polyèdres réguliers, comme le fit Gauss pour le polyèdre à dix-sept côtés.

1.2 Un "bref" état de l'art

1.2.1 Premiers pas

La notion de nombre est apparue assez tôt dans l'histoire de l'humanité et s'est développée notamment avec le commerce (valeurs et calculs) et l'agriculture (aires et géométrie). Une équation apparaît comme la formalisation d'un problème, comme : "que faut-il ajouter à 6 pour avoir 10 ?" qui se traduit par $x + 6 = 10$, où x représente la valeur inconnue. Il s'agit d'une équation du premier degré, qui se résoud en passant le 6 à droite et en changeant de signe, opération appelée "al-jabr" par les mathématiciens arabes, qui donna le mot algèbre. Les premiers problèmes algébriques naquirent notamment de la géométrie. "J'ai additionné 7 fois le côté de mon carré et 11 fois la surface : 6 15" (6 15 correspond à l'écriture en base 60) lit-on sur une tablette babylonienne, soit $11x^2 + 7x = 6 \times 60 + 15 = 375$. Remarquons que cette équation comprend la somme d'une longueur (x) et d'une aire (x^2). La considération des valeurs elles-mêmes en mettant de côté la nature des objets (ligne, surface, volume...) permis l'introduction progressive de la notion de polynôme.

L'équation de cette tablette est une équation de degré 2 (quadratique), et la

solution (exprimée sous forme géométrique) à ce genre d'équation était connue en Mésopotamie dès 1700 av JC. L'équation quadratique est assez simple et nous servira de modèle pour les degrés 3 et 4. Mais dans ce chapitre nous ne présenterons pas les résultats comme les mathématiciens de l'époque l'auraient fait. Par exemple, les nombres devant représenter des quantités géométriques, et donc positives, la notion de nombre négatif en tant que vrai nombre ne fut admise que tardivement, surtout en Occident. Ainsi, pour conserver des coefficients positifs dans les équations la résolution était scindée en de multiples sous-cas. Pour le degré 2, il y avait par exemple les cas : $ax^2 + bx + c = 0$, $ax^2 + c = bx$, $ax^2 + bx = c$ ou $ax^2 = bx + c$ qui étaient à l'époque considérés comme bien distincts, contrairement à nos jours, et nous n'étudierons donc ici que l'équation $ax^2 + bx + c = 0$ en acceptant que les coefficients a, b et c soient éventuellement négatifs.

Le but est de se ramener à une forme canonique plus simple $x^2 + \alpha = 0$, puis de résoudre. Soit $P(X) = aX^2 + bX + c$ un polynôme de degré 2 ($a \neq 0$). Cherchons les racines de P, c'est à dire les x tels que le polynôme P s'annule en x :

$ax^2 + bx + c = 0$

$\Leftrightarrow x^2 + (b/a)x + c/a = 0$

$\Leftrightarrow (x + b/2a)^2 - b^2/4a^2 + c/a = 0$

$\Leftrightarrow (x + b/2a)^2 = (b^2 - 4ac)/(2a)^2$.

Notons que si $b^2 - 4ac < 0$, alors sa racine est un nombre imaginaire, et que si $b^2 - 4ac = 0$ alors la solution est double.

$\Leftrightarrow x + b/2a = \pm\sqrt{b^2 - 4ac}/2a$, soit $x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$.

1.2.2 Résolution algébrique

La notion abstraite d'inconnue fut appliquée par trois civilisations, qui ébauchèrent l'étude théorique des équations : la Grèce, l'Arabie et l'Inde. Au IIIème siècle av JC, Euclide rédige les Éléments qui introduisent le traitement axiomatique de la géométrie, puis Diophante au IIIème siècle ap JC introduit la notion d'inconnue et une écriture algébrique. Indépendamment, dans le monde arabe du VIIIème siècle Al-Khawarizmi fait de même, et de même dans l'Inde au XIIème siècle avec Bhaskara II. C'est à ce siècle également que les mathématiciens arabes, comme Al-Khayyam, utilisent sans problème les irrationnels et développent des techniques de résolution géométrique. Les Indiens eux utilisent les nombres négatifs sans problème, contrairement à l'Europe. Il fallut attendre l'Italie du XVIème siècle, où les mathématiciens se livrèrent à une âpre compétition, pour que l'équation cubique soit résoluble en toute généralité, puis peu après ce fut également le cas pour l'équation quartique en suivant la même méthode. C'est à cette époque qu'apparaissent les nombre imaginaires qui dans un premier temps ne servent que d'intermédiaires pour trouver des solutions réelles (de même que les nombres négatifs), avant d'être acceptés comme nombre en tant que tels.

Comme la méthode est à peu près la même pour les équations de degré 3 ou

4, nous détaillerons l'équation cubique et résumerons la résolution de l'équation quartique. De même que pour l'équation quadratique, nous pouvons ramener l'équation initiale $ax^3 + bx^2 + cx + d = 0$ à une équation sous forme canonique $x^3 + \alpha x + \beta = 0$, puis un changement de variable nous permettra de résoudre l'équation :

$ax^3 + bx^2 + cx + d = 0 \Rightarrow x^3 + (b/a)x^2 + (c/a)x + d/a = 0$
$\Leftrightarrow (x + b/3a)^3 - (b^2/3a^2)x - b^3/27a^3 + (c/a)x + d/a = 0$
$\Leftrightarrow (x + b/3a)^3 - ((b^2 + 3ac)/3a^2)x - (b^3 + 27a^2d)/27a^3 = 0$
$\Leftrightarrow (x + b/3a)^3 - ((b^2 + 3ac)/3a^2)(x + b/3a - b/3a) - (b^3 + 27a^2d)/27a^3 = 0$
$\Leftrightarrow (x + b/3a)^3 - ((b^2 + 3ac)/3a^2)(x + b/3a) - (b^3 + 27a^2d)/27a^3 - b/3a((b^2 + 3ac)/3a^2) = 0$
$\Leftrightarrow (x + b/3a)^3 - ((b^2 + 3ac)/3a^2)(x + b/3a) - (27a^2d + 9abc - 2b^3)/27a^3 = 0$
En faisant le changement de variable y = x + b/3a nous avons l'équation :
$y^3 - ((b^2 + 3ac)/3a^2)y - (27a^2d + 9abc - 2b^3)/27a^3 = 0$
Cette équation est bien de la forme $x^3 + \alpha x + \beta = 0$, avec $\alpha = (b^2 + 3ac)/3a^2$ et $\beta = (27a^2d + 9abc - 2b^3)/27a^3$.
Résolvons à présent la forme simplifiée $x^3 + \alpha x + \beta = 0$:

Si $\alpha = 0$, alors l"équation devient $x^3 = -\beta$, ce qui revient juste à extraire une racine troisième. Etudions maintenant le cas $\alpha \neq 0$:

Faisons le changement de variable x = y - z, en posant $3yz = \alpha$, nous obtenons :
$x^3 + \alpha x + \beta = 0$
$\Leftrightarrow (y - z)^3 + \alpha(y - z) + \beta = 0$
$\Leftrightarrow y^3 - 3y^2z + 3yz^2 - z^3 + \alpha(y - z) + \beta = 0$
$\Leftrightarrow y^3 - z^3 + (y - z)(-3yz + \alpha) + \beta = 0$
$\Leftrightarrow y^3 - z^3 + \beta = 0$
$\Leftrightarrow 3^3y^3(y^3 - z^3 + \beta) = 0$
$\Leftrightarrow 27y^6 - (3xy)^3 + 27y^3\beta = 0$
$\Leftrightarrow 27y^6 - \alpha^3 + 27y^3\beta = 0$
$\Leftrightarrow 27(y^3)^2 + 27\beta y^3 - \alpha^3 = 0$
Il s'agit d'une équation de degré 2 en y^3, que nous pouvons donc résoudre pour obtenir y^3 et donc y en extrayant la racine troisième.
Puis, de $3yz = \alpha$ nous déduisons $z = \alpha/3y$ ($y \neq 0$ car $\alpha \neq 0$).
Enfin, avec y et z nous déduisons x = y - z.

Passons à la quartique :
Nous ramenons l'équation $ax^4 + bx^3 + cx^2 + dx + e = 0$ à la forme canonique $x^4 + \alpha x^2 + \beta x + \gamma = 0$, d'où :
$x^4 = -\alpha x^2 - \beta x - \gamma$
Nous introduisons une nouvelle variable y vérifiant une équation arbitraire appelée (E) que nous choisirons par la suite, d'où :
$(x^2 + y)^2 = x^4 + 2x^2y + y^2 = -\alpha x^2 - \beta x - \gamma + 2x^2y + y^2$
$\Leftrightarrow (x^2 + y)^2 = (-\alpha + 2y)x^2 - \beta x + (-\gamma + y^2)$

Le membre de droite est un polynôme de degré 2, et pour qu'il ait une racine double il faut et il suffit que $\beta^2 - 4(-\alpha + 2y)(-\gamma + y^2) = 0$, qui est précisément l'équation (E) que nous choisissons. Il s'agit d'une équation de degré 3 en y, donc que nous pouvons résoudre pour trouver le nombre y. Donc $(-\alpha+2y)x^2-\beta x+(-\gamma+y^2) = A(x+B)^2$ où A = $(-\alpha+2y)$ et B = $-\beta/2(-\alpha+2y)$, d'où :

$(x^2 + y)^2 = (-\alpha + 2y)(x - \beta/2(-\alpha + 2y))^2$

$\Leftrightarrow x^2 + y = \sqrt{-\alpha + 2y}(x - \frac{\beta}{2(-\alpha+2y)})$

Il s'agit d'une équation de degré 2 en x, que nous pouvons donc résoudre pour trouver x.

Comme l'introduction des nombres négatifs et des nombres imaginaires permet de trouver, moyennant quelques contorsions, les solutions aux équations polynômiales de degré inférieur à 5, la question à présent est de savoir s'il est possible d'utiliser le même genre de méthode pour résoudre les équations de degré supérieur ou égal à 5.

Comme l'équation quadrique a été résolue en suivant cette méthode dans la foulée de la résolution de la cubique, il semblait à l'époque qu'il suffirait juste de chercher quelques temps quels étaient les calculs adaptés pour résoudre le degré suivant, et continuer dans la foulée, voire trouver par récurrence une manière générale de résoudre toutes les équations polynômiales.

Néanmoins, les mathématiciens réalisèrent que ce n'était pas aussi facile qu'il était possible de le croire à la fin de la Renaissance.

1.2.3 Théorie des équations

Á la fin du XVIème siècle, le mathématicien français Viète introduit la notion moderne de polynôme et la notation associée, c'est dire comme une somme de puissances de l'inconnue, avec des coefficients. Puis Descartes introduit la notion de repères et d'équations, ce qui permet d'étudier les objets géométriques par le simple calcul, et plus par le traitement purement axiomatique issu des Éléments.

Au XVIIème siècle est introduit le calcul infinitésimal où le polynôme devient la fonction polynômiale, c'est à dire que ce n'est plus le polynôme en tant qu'objet formel qui est utilisé, mais la fonction associée qui à une variable associe le polynôme en cette variable. La fonction polynômiale est alors étudiée et munie de propriétés, comme la continuïté ou la dérivabilité. Le lien avec l'algèbre se perd un peu et les travaux deviennent alors plus du ressort du l'analyse.

Au XVIIIème siècle, Vandermonde étudie les polynômes cyclotomiques, c'est à dire les polynômes irréductibles divisant les polynômes de la forme $X^n = 1$, dont les racines sont appelées les racines n-ièmes de l'unité. Le terme "cyclotomique" vient du grec et signifie "qui partage le cercle". En effet, les racines de l'unités peuvent être vues comme les points du cercles obtenus en divisant le cercle en n morceaux.

Pendant ce temps, alors que ses contemporains cherchaient à reprendre les méthodes utilisées pour les degrés inférieurs à cinq en cherchant des astuces de

calcul qui auraient échappé à leurs prédecesseurs, Lagrange publie un article mettant fin à ces tâtonnements en publiant un article démontrant qu'il n'est pas possible de transposer ce genre de méthode pour résoudre les équations de degré supérieur ou égal à 5.

La question n'est donc plus de savoir comment résoudre une équation quintique ou de degré supérieur, mais déjà de savoir si elle est résoluble ou non.

Au début du XIXème siècle, Gauss étudie l'équation cyclotomique en utilisant la notion de polynôme formel, ce qui peut être vu comme un retour à la notion de polynôme selon Viète. Comme Vandermonde et Lagrange, il s'aperçoit que le problème est lié à un certain choix de "bonnes" fonctions rationnelles, qui seraient invariables par substitutions des racines, et que ces fonctions sont liées à la structure de groupe des racines. Il arrive ainsi à mettre le doigt sur le noeud du problème, et parvient même à appliquer ses résultats pour construire à la règle et au compas le polyèdre régulier à 17 côtés.

C'est Abel, dont les travaux étaient globalement inconnus de Galois, qui démontre qu'en supposant l'équation quintique résoluble par radicaux s'ensuit une absurdité liée aux permutations des variables qu'avaient étudiées Gauss. Mais comme Galois, il mourût jeune et ses travaux ne furent pas reconnus de son vivant. Abel apportait donc une réponse négative à la question de résolubilité en général de la quintique. Galois, de son côté, réussit à montrer dans quel cas elle est résoluble et apporte une réponse généralisable à d'autres degrés que 5.

Nous allons à présent présenter sous forme moderne des résultats connus à l'époque de Galois, et qui nous sont nécessaires dans notre exposé de sa théorie.

1.3 Quelques prérequis (à retravailler)

Nous allons ici introduire les notions de groupe, de sous-groupe et de sous-groupe simple.

Nous présentons l'exemple des permutations et énoncerons que si $n \geq 5$ le sous-groupe alterné A_5 est simple.

Nous allons maintenant introduire les notions d'anneau et de corps.

Nous présentons l'exemple des polynômes, en faisant des précisions sur la notion de polynômes symétriquers et de divisibilité, et énoncerons deux résultats que nous utiliserons souvent par la suite.

Le premier :

Soient S un polynome symétrique en n variables et P un polynôme de degré n admettant pour racine $x_1, ...x_n$, alors les nombres $S(x_1, ...x_n)$ appartiennent à l'anneau engendré par les coefficients de P.

Le second :

Une équation irréductible ne peut avoir aucune racine commune avec équation rationnelle sans la diviser.

Il y a quelque chose à compléter dans cette démonstration. Je n'ai pas le temps. ;-)

Brouillon :

Le résultat suivant était qualifié d'évident à l'époque de Galois, et nous servira beaucoup :

Soient S un polynome symétrique en n variables et P un polynôme de degré n admettant pour racine $x_1, ...x_n$, alors les nombres $S(x_1, ...x_n)$ appartiennent à l'anneau engendré par les coefficients de P.

Les polynômes de cette section sont à coefficients dans un anneau A commutatif unitaire.

Un polynôme P de $A[X_1, ...X_n]$ est dit symétrique si pour tout $\sigma \in S_n, P(X_{\sigma(1)}, ...X_{\sigma(n)}) = P(X_1, ...X_n)$.

Nous définissons le polynôme symétrique élémentaire de degré k de $A[X_1, ...X_n]$ comme $s_k = \sum_{H \subseteq \{1,...n\}, cardH=k} \prod_{i \in H} X_i$. Pour $k < n, s_k = 0$.

(vérifier la preuve du livre)

Le second résultat :

Une équation irréductible ne peut avoir aucune racine commune avec équation rationnelle sans la diviser.

1.4 Evariste Galois

Galois est né en 1811 à Bourg-la-Reine. Il intègre le collège Luis-le-Grand en 1823 et obtient des prix en latin et en grec. Il redouble sa seconde et, suite à une réforme pédagogique, suit des cours de mathéamtiques qui le passionnent. Il se met à lire Legendre, Lagrange et Gauss, et en 1826 il obtient un prix de mathématiques. L'année suivante, l'un de ses professeurs déclare : "C'est la fureur des mathématiques qui le domine ; aussi je pense qu'il vaudrait mieux pour lui que ses parents consentent à ce qu'il ne s'occupe que de cette étude ".

En 1828 il se présente au concours d'entrée de l'École polytechnique, mais échoue. En 1829 il publie son premier article dans les "Annales de mathématiques pures et appliquées" de Gergonne où il traite du développement en fractions continues des racines d'un polynôme. La même année il présente ses premiers mémoires sur la théorie des équations à l'Académie des sciences. Il se présente encore une fois à l'École polytechnique, et le suicide de son père précède de peu son second échec.

Il est néanmoins admis à l'École préparatoire et soumets d'autres articles sur la théorie des équations et un article sur la théorie des nombres. Cauchy aurait refusé de présenter ses mémoires sur la résolubilité des équations algébriques afin qu'il puisse les soumettre, sous une version révisée, au Grand Prix des sciences mathématiques de 1830. Mais le prix est accordé à Abel (à titre posthume) et à Jacobi. Le mémoire de Galois avait été envoyé à Fourier, qui meure en mai et le mémoire est annoncé perdu. Pourtant, en juin 1831, Cauchy aurait fait part de son intérêt pour les travaux de Galois dans un journal.

La révolution de juillet 1830 marque le début de l'engagement politique de Galois du côté républicain. Les tensions avec la direction de l'École provoquèrent

l'expulsion de Galois, qui venait d'obtenir sa licence, pendant qu'il s'engageait dans la Société des Amis du Peuple. Galois publie un autre mémoire l'année suivante, et ses activités le font arrêter : il passe un mois en prison avant d'être jugé et acquitté. Puis il est de nouveau arrêté pour port illégal d'uniforme et condamné à six mois de prison. Le mémoire de 1831 aurait été soumis à Poisson, mais il le refusa pour le moment car il semblait difficile à évaluer et Galois avait promis dans son mémoire une théorie plus vaste. En prison, Galois travaille ses mémoires sur les équations et entame des recherches sur les fonctions elliptiques.

En 1832 il est transféré dans une clinique privée à cause d'une épidémie de choléra, où il y rencontre une jeune femme dont il s'éprend. Elle lui demande de rompre, puis il est blessé à l'estomac lors d'un duel au pistolet. Il est transporté à l'hôpital et y meurt à l'âge de 20 ans et 7 mois, probablement d'une péritonite, après avoir refusé les offices d'un prêtre. Le Précurseur de Lyon publie un compte rendu détaillé de la mort d'Evariste, apportant ces précisions : "Le pistolet étant l'arme choisie par les deux adversaires, ils ont trouvé trop dur pour leur ancienne amitié d'avoir à viser l'un sur l'autre et ils s'en sont remis à l'aveugle décision du sort. À bout portant, chacun d'eux a été armé d'un pistolet et a fait feu. Une seule de ces armes était chargée."

La veille du duel il a rédigé plusieurs lettres, notamment une à Auguste Chevalier qui est considérée comme son testament mathématique : Galois enjoint à son ami de " prier publiquement Jacobi ou Gauss de donner leur avis, non sur la vérité, mais sur l'importance des théorèmes " qu'il a trouvés et dont il dresse le bilan, et de faire imprimer la lettre dans la Revue encyclopédique, ce que Chevalier fit en septembre 1832. Galois fut enterré le 2 juin 1832 au cimetière du Montparnasse à Paris en présence de deux à trois mille républicains.

Les papiers d'Évariste Galois, rassemblés par Chevalier et son jeune frère Alfred furent soumis à Liouville qui recommanda à l'Académie des sciences son principal résultat de la théorie des équations algébriques obtenu en septembre 1843. Liouville fit ensuite publier les travaux de Galois en 1846 dans son journal, le Journal de mathématiques pures et appliquées, ce qui leur conféra aussitôt un rayonnement international.

Chapter 2

La théorie de Galois... par Galois

2.1 Présentation du problème

Le problème est d'étudier les racines d'un polynome P à coefficients dans un corps K (Galois travaillait sur des rationnels, mais le corps K peut être quelconque de caractéristique 0), et de déterminer (éventuellement) l'expression des racines en fonction des coefficients de P. S'il est possible d'écrire une telle expression, nous dirons que l'équation P(X) = 0 est soluble par radicaux. Nous pouvons supposer que P admet n racines distinctes $x_1, ...x_n$, où n est au moins égal à 2.

Nous nous servirons de cette étude pour démontrer qu'une équation de degré 5 ou plus peut ne pas être résoluble par radicaux.

2.2 La résolvante de Galois

2.2.1 Définition de la résolvante

Etant donnée une équation quelconque, qui n'a pas de racines égales, dont les racines sont a, b, c ..., on peut toujours former une fonction V des racines, telle qu'aucune des valeurs que l'on obtient en permutant dans cette fonction les racines de toutes manières ne soient égales. Par exemple, on peut prendre V = Aa + Bb + Cc + ... où A, B, C... sont des entiers convenablement choisis.

Par la suite, Galois note la fonction (appelée la résolvante) φ et V la valeur de la fonction en $(x_1, ...x_n)$, aussi nous suivrons cette notation. Une fonction vérifiant les hypothèses de Galois existe, mais ne suffit pas (à notre connaissance) à démontrer les résultats escontés. Aussi nous prendrons une résolvante plus exigeante.

Notons E l'ensemble formé par les racines $x_1, ...x_n$. Nous cherchons à démontrer l'existence d'une application φ de E^n dans $K[x_1, ...x_n]$ telle que pour tous $(y_1, ...y_n)$ et $(z_1, ...z_n)$ n-uplets distincts dans E^n, $\varphi(y_1, ...y_n) \neq \varphi(z_1, ...z_n)$.

Prouvons ce lemme avec $A = N, B = N^2, C = N^3, \ldots$ où N est un entier suffisamment grand. Il suffit de prendre $N > \alpha/\beta$, où α est la somme des $|x_i - x_j|$, et où β est le plus petit $|x_i - x_j|$ possible avec x_i et x_j distinctes.

Supposons par l'absurde qu'il existe $(y_1, ...y_n)$ et $(z_1, ...z_n)$ n-uplets distincts dans E^n (rappelons qu'il y a au moins 2 racines distinctes, donc il est possible d'avoir deux tels n-uplets distincts) tels que $\varphi(y_1, ...y_n) = \varphi(z_1, ...z_n)$. D'où :

$\sum_{i=1}^{n} N^i y_i = \sum_{i=1}^{n} N^i z_i$

Notons r la plus grande valeur des i telle que $y_i \neq z_i$ (qui existe car $(y_1, ...y_n)$ et $(z_1, ...z_n)$ sont distincts). Nous avons donc :

$N^r(y_r - z_r) = -\sum_{i=1}^{r-1} N^i(y_i - z_i)$, d'où :

$N^r\beta \leq N^r|y_r - z_r| \leq \sum_{i=1}^{r-1} N^i|y_i - z_i| \leq N^{r-1}\sum_{i=1}^{r-1}|y_i - z_i| \leq N^{r-1}\alpha$

Donc $N \leq \alpha/\beta$, ce qui contredit l'hypothèse.

Nous continuerons d'utiliser la forme "théorique" de la résolvante (c'est à dire comme fonction φ et non d'après la forme dont nous nous sommes servis pour démontrer son existence. Retenons donc que φ prend des valeurs distinctes en les n-uplets formés sur l'ensemble des racines (propriété de la résolvante), et qu'il s'agit d'une fonction polynomiale.

Notons également que la propriété de la résolvante permet d'établir par φ une bijection entre les n-uplets formés par les racines de P (ou même les permutations des racines) et les valeurs de φ associées.

2.2.2 Théorème de l'élément primitif

La fonction V étant choisie comme il est indiqué dans l'article précédent, elle jouira de cette propriété que toutes les racines de l'équation proposées s'exprimeront rationnellement en fonction de V.

En langage moderne, comme $V = \varphi(x_1, ...x_n) = x_1N + x_2N^2 + ... + x_nN^n \in K[x_1, ...x_n]$, $K[V] \subseteq K[x_1, ...x_n]$. Si les racines $x_1, ...x_n$ s'expriment rationnellement en fonction de V, alors $x_1 \in K[V]$, ... $x_n \in K[V]$, d'où $K[x_1, ...x_n] \subseteq K[V]$, et $K[x_1, ...x_n] = K[V]$, donc V (la valeur de la résolvante en $(x_1, ...x_n)$, les racines de P) est l'élément primitif.

Passons à la preuve :

Soit x_i une racine de P, et soit τ la transposition échangeant 1 et i (si i=1, τ est l'identité). Comme la résolvante ne dépendait pas de l'ordre dans lequel sont écrites les racines de P, la fonction $\psi(y_1, ...y_n) = \varphi(y_{\tau(1)}, ...y_{\tau(n)})$ est une résolvante.

$V = \psi(x_i, ...x_{\tau(n)})$, d'où : $\prod_{(y_2,...y_n)\in E^{n-1}}(V - \psi(x_i, y_2, ...y_n) = 0$.

D'où x_i est racine du polynôme $F_i(X) = \prod_{(y_2,...y_n)\in E^{n-1}}(V - \varphi(X, y_2, ...y_n)$, symétrique en $y_2, ...y_n$, donc à coefficients dans K[V].

Une autre racine x_j avec $j \neq i$ de P ne peut être racine de $F_i(X)$. En effet, supposons par l'absurde que x_j soit racine de $F_i(X)$, c'est à dire :

$\prod_{(y_2,...y_n)\in E^{n-1}}(V - \psi(x_j, y_2, ...y_n) = 0$

Donc il existe un (n-1)-uplet $(y_2, ...y_n)$ tel que $V - \psi(x_j, y_2, ...y_n) = 0$, d'où $\psi(x_i, ...x_{\tau(n)}) = V = \psi(x_j, y_2, ...y_n)$ avec $j \neq i$, ce qui contredit la propriété de la résolvante.

Ainsi, comme la seule racine commune à P(X) et $F_i(X)$ est x_i, X-x_i est le pgcd de P(X) et $F_i(X)$ et nous avons l'identité de Bezout : $A_i(X)P(X) + B_i(X)F_i(X) = X - x_i$ dans K[V][X]. En faisant X=0, nous avons $x_1 = -A_i(0)P(0) - B_i(0)F_i(0) \in K[V]$.

Notons pour la suite $x_i = f_i(V)$.

2.3 Groupe de Galois d'une extension

2.3.1 Construction du Groupe de Galois

Supposons que l'on ait formé l'équation en V, et que l'on ait pris l'un de ses facteurs irréductibles, en sorte que v soit racine d'une équation irréductible. Soient V, V', V",... les racines de cette équation irréductible. Si a = f(V) est une des racine de la proposée, f(V') sera une racine de la proposée.

Soit Q(X) le polynôme minimal de V (il est donc irréductible), et soient $V_1, ...V_m$ ses racines, en notant $V_1 = V$.

Soit x_j une racine quelconque de P, et $F(X) = \prod_{i=1}^{n}(x_i - f_j(X))$ symétrique en les x_i donc dans K(X). Comme $x_j = f_j(V)$, V_1 est racine de F(X), d'où Q(X) divise F(X), et $V_1, ...V_m$ sont racines de F. Donc pour chaque V_k il existe une racine a_i telle que $a_i - f_j(V_k) = 0$, donc les $f_j(V_k)$ sont des racines de P.

Rappelons que les $f_j(V_1) = x_j$ sont distinctes, montrons qu'il en est de même pour tout V_k.

Soit V_k une racine quelconque de Q, supposons par l'absurde qu'il existe f_i et f_j distinctes telle que $f_i(V_k) = f_j(V_k)$. Alors V_k est racine de $f_i(X) - f_j(X)$, polynôme dans K[X]. D'où Q(X) divise $f_i(X) - f_j(X)$, et V_1 est racine de $f_i(X) - f_j(X)$, d'où $f_i(V_1) = f_j(V_1)$, ce qui contredit l'hypothèse.

Ainsi, pour un k donné les $f_i(V_k)$ sont des racines distinctes du polynôme P. Comme il y a n fonctions $f_i(X)$ et n racines distinctes pour P, pour un k donné les $f_i(V_k)$ forment toutes les racines de P, sans répétition.

Donc, à un V_k donné, il est possible d'associer le n-uplet $(f_1(V_k)), ...f_n(V_k)) = (x_{a_1}, ...x_{a_n})$ à une permutation $\sigma \in S_n$ telle que $\sigma(i) = a_i$. L'ensemble de ces permutations est appelé le groupe de Galois associé à l'extension.

2.3.2 Propriétés du Groupe de Galois (à retravailler)

Ces permutations définies chacune par un V_k sont bien distinctes. Pour cela nous allons d'abord démontrer que $V_k = \varphi(f_1(V_k), ...f_n(V_k))$:

$V_1 = \varphi(x_1, ...x_n) = \varphi(f_1(V_1), ...f_n(V_1))$, d'où V_1 est racine de $F(X) = X - \varphi(f_1(X), ...f_n(X)) \in K[X]$, d'où Q divise F et pour tout V_k racine de Q, V_k est racine de F, donc $V_k = \varphi(f_1(V_k), ...f_n(V_k))$.

Montrons maintenant que si $V_j \neq V_k$, alors les permutations associées sont distinctes, c'est à dire qu'il existe i tel que $f_i(V_j) \neq f_i(V_k)$. Pour cela, montrons la contraposée :

En effet, si pour tout i, $f_i(V_j) = f_i(V_k)$, alors $V_j = \varphi(f_1(V_j), ...f_n(V_j)) = \varphi(f_1(V_k), ...f_n(V_k)) = V_k$.

Il nous reste à montrer que ces permutations forment un groupe. (à démontrer)

Piste :

Notons Gal le "groupe" de Galois.

$V = \varphi(x_1, ...x_n)$, notons $\sigma V = \varphi(x_{\sigma(1)}, ...x_{\sigma(1)})$. Nous avons que Gal $= \{\sigma \in S_n; \exists k, \sigma V = V_k\}$. L'inclusion dans le sens direct est immédiate par définition.

Montrons la réciproque, soit $\sigma \in S_n$ telle que $\exists k, \sigma V = V_k$, et montrons qu'elle est dans Gal. Supposons le contraire, alors il existe une permutation des racines σ qui n'est pas dans Gal telle que $\sigma V = V_k$. Or, V_k définit une permutation des racines par $V_k = \varphi(f_1(V_k), ...f_n(V_k))$. D'où $\varphi(x_{\sigma(1)}, ...x_{\sigma(1)}) = V_k = \varphi(f_1(V_k), ...f_n(V_k))$ avec $(x_{\sigma(1)}, ...x_{\sigma(1)}) \neq (f_1(V_k), ...f_n(V_k))$, ce qui est contraire à la propriété de la rsolvante.

Pour montrer que Gal $= \{\sigma \in S_n; \exists k, \sigma V_1 = V_k\}$ est bien un groupe, il suffit de montrer que pour tout i Gal $= \{\sigma \in S_n; \exists k, \sigma V_i = V_k\}$. En effet, si c'est bien le cas nous montrons la stabilité par composition :

Soient σ et τ deux permutations de Gal. Nous avons que $\sigma \circ \tau V_1 = \sigma V_k = V_k$, d'où $\sigma \circ \tau$ est une permutation de Gal.

Comme id V = V, l'identité est bien dans Gal, et l'inverse s'obtient par Lagrange car Gal comme sous ensemble de S_n, groupe fini, est fini.

Il nous reste donc à montrer que pour tout i Gal $= \{\sigma \in S_n; \exists k, \sigma V_i = V_k\}$, c'est à dire que σ V est racine de Q si et seulement si σV_j est racine de Q.

La question peut se ramener à déterminer si F(X) $= \prod_{i=1} m(X - \sigma V_i)$ est dans K[X]. En effet, si oui alors σV_i racine de Q $\Rightarrow$ Q divise F $\Rightarrow$ (même degré, unitaires) Q = F $\Rightarrow$ σV_j racine de Q, ce qui montre l'équivalence.

2.3.3 Caractérisation du Groupe de Galois

Soit une équation donnée, dont a, b, ... sont les m racines. Il y aura toujours un groupe de permutations des lettres a, b, c ... qui jouira de la propriété suivante :

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

2) réciproquement, que toute fonction des racines, déterminables rationnellement, soit invariable par ces substitutions.

Galois prouve ce théorème (existentiel) en construisant ce que nous avons appelé le groupe de Galois associé à l'extension, qui dépendait de la résolvante

φ construite plus haut. Cette caractérisation donne une condition nécessaire et suffisante ne dépendant pas de φ , donc le groupe de Galois construit en réalité ne dépend pas de φ .

Question : en fait il ne s'agit que d'une implication, en quoi est-ce une caractérisation ? Notion de maximalité ?

Passons à la preuve :

Soit F une fonction des racines invariantes par les substitutions de ce groupe, montrons qu'elle est à valeur dans K. Comme la résolvante induit une bijection entre les n-uplets des racines et les valeurs associées, nous pouvons écrire que $F(x_1, ...x_n) = \psi(V_1)$, soit $F(f_1(V_1), ...f_n(V_1)) = \psi(V_1)$, et plus généralement, pour tout k : $F(f_1(V_k), ...f_n(V_k)) = \psi(V_k)$. Comme F est invariantes par les substitutions de ce groupes, pour tout j et k nous avons $F(f_1(V_j), ...f_n(V_j)) = F(f_1(V_k), ...f_n(V_k))$, soit $\psi(V_j) = \psi(V_k)$. D'où ψ est symétrique en les V_k, donc les $F(f_1(V_k), ...f_n(V_k)) = \psi(V_k)$ sont dans K.

Réciproquement, soit F une fonction des racines à valeur dans K, montrons qu'elle est invariable par les subsitutions de ce groupe. De même que précédemment, nous pouvons poser $F(f_1(V_k), ...f_n(V_k)) = \psi(V_k)$. D'où V_1 est racine de $F(f_1(V_1), ...f_n(V_1)) - \psi(X)$, et comme $F(f_1(V_1), ...f_n(V_1))$ est dans K, il s'agit d'un polynôme dans K[X]. D'où Q(X) le divise, et les $V_1, ...V_m$ sont racines de $F(f_1(V_1), ...f_n(V_1)) - \psi(X)$, c'est à dire pour tout k, $\psi(V_k) = F(f_1(V_1), ...f_n(V_1)) = V$. Donc les $\psi(V_k)$, et donc les $F(f_1(V_k), ...f_n(V_k))$, sont égaux. D'où F est invariante par les permutations de ce groupe.

2.3.4 Décomposition du Groupe de Galois

Si l'on adjoint à une équation donnée la racine r d'une équation auxiliaire irréductible et de degré p premier,

1) 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 appartenant chacun à l'équation proposée respectivement quand on lui adjoint chacune des racines de l'équations auxiliaire ;

2) ces groupes jouiront de la propriéét remarquable, que l'on passera de l'un à l'autre en opérant dans toutes les permutations du premier une même substitution de lettres.