La théorie de Galois

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

March 21, 2017

Contents

Chapter 1

Ce qui était connu à l'époque de Galois

1.1 Introduction

Ce que nous appelons de nos jours la "théorie de Galois" est l'étude des extensions de corps commutatifs par les groupes de permutation associés, appelés les "groupes de Galois".

Galois a initialement présenté sa théorie pour étudier le problème de résolubilité des équations polynomiales, et cette théorie fut formalisée et enrichie par la suite, notamment pour la théorie de Galois différentielle, et même des problèmes contemporains, comme les groupes de Galois cosmiques dans les travaux d'Alain Connes sur la réunification entre physique quantique et relativité générale.

Nous présentons ici la théorie de Galois selon son "Mémoire sur les conditions de résolubilité des équations par radicaux" publié le 16 janvier 1831. Comme ce mémoire est avant tout une ébauche, nous ferons cette présentation en langage moderne pour nous assurer que les idées énoncées pouvaient bien mener à une construction juste de la théorie.

Nous suivons donc la démarche utilisée par Galois, et nous ferons des citations du texte original lorsqu'un rapprochement sera possible.

Présenter la théorie selon les idées de Galois permet de montrer sa simplicité intrinsèque, par exemple les preuves se résument la plupart du temps à trouver un bon polynôme qui permette de conclure, mais nous obligera à n'utiliser que les outils disponibles à l'époque de Galois.

Notre propos est ici de montrer que ces outils étaient suffisants, et que les idées modernes de groupe ou de corps étaient déjà présentes dans les écrits de Galois, bien que pas encore formalisées.

1.2 Vocabulaire lié aux permutations, groupes et corps

Le vocabulaire utilisé par Galois et ses contemporains diffère du nôtre sur quelques points, révélant une compréhension un peu différente d'objets mathématiques apparemment similaires.

Par exemple, ils auraient appelé substitution ce que nous appelons permutation (précisons que les permutations étaient bien connues à l'époque), et auraient réservé le terme de permutation à des arrangements spécifiques d'éléments, que nous décririons comme des n-uplets.

> Les substitutions sont le passage d'une permutation à l'autre.
>
> La permutation d'où l'on part pour indiquer les substitutions est toute arbitraire, quand il s'agit de fonctions. Car il n'y a aucune raison pour que dans une fonction de plusieurs lettres, une lettre occupe un rang plutôt qu'un autre.
>
> Cependant comme il ne peut gère se former l'idée d'une substitution sans celle d'une permutation, nous ferons dans le langage un emploi fréquent des permutations, et nous ne considérerons les substitutions que comme le passage d'une permutation à une autre.
>
> Quand nous voudrons grouper des substitutions nous les ferons toutes provenir d'une même permutation.
>
> Évariste Galois.

Néanmoins il précise bien que la permutation liée à un réarrangement du n-uplet de départ ne dépend pas du choix de ce n-uplet.

De plus, Galois utilise le mot "groupe" dans un sens moderne, car il l'associe à la stabilité par composition dans le cas des permutations, ce qui permet bien de déduire l'inversion, et l'identité correspond chez lui au n-uplet choisi au départ pour représenter les permutations (notons qu'il s'agit de permutations dans un ensemble à n éléments et pas forcément spécifiquement dans $|[1, n]|$).

> Comme il s'agit de questions où la disposition primitive des lettres n'influe en rien, dans les groupes que nous considérerons, on devra avoir les mêmes substitutions quelle que soit la permutation d'où l'on sera parti. Donc si dans un pareil groupe on a les substitutions S et T, on est sûr d'avoir la substitution ST.
>
> Évariste Galois.

De même que pour les groupes, la notion de corps est déjà présente, bien que le terme de "corps" ne soit pas employé. Galois utilise la notion de "rationnellement connue" pour exprimer qu'une quantité peut-être exprimée comme quotient des coefficients de l'équation à étudier.

> Il faut ici expliquer ce qu'on doit entendre par le mot rationnel : car il représentera souvent.

> Quand l'équation a tous ses coefficients numériques et rationnels, cela veut dire simplement que l'équation peut se décomposer en facteurs qui aient leurs coefficients numériques et rationnels.
>
> Mais quand les coefficients d'une équation ne seront pas TOUS numériques et rationnels, alors il faudra entendre par diviseur rationnel, un diviseur dont les coefficients s'exprimeraient en fonction rationnelle des coefficients de la proposée, en général par quantité rationnelle, une quantité qui s'exprime en fonction rationnelle des coefficients de la proposée.
>
> Évariste Galois.

De plus, Galois introduit avec son vocabulaire la notion d'extension de corps, c'est à dire un corps où l'on a adjoint une certaine racine du polynôme à étudier.

> 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.
>
> 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. Nous dirons que ces quantités sont ADJOINTES à l'équation.
>
> Cela posé, nous appellerons RATIONNELLE toute quantité qui s'exprimera en fonctions rationnelle des coefficients de l'équation et d'un certain nombre de quantités ADJOINTES de l'équation et convenues arbitrairement.
>
> Évariste Galois.

1.3 Résultats connus sur les polynômes

Galois et ses contemporains avaient déjà certains résultats concernant les polynômes.

Par exemple, Galois remarque que travailler sur une extension de corps peut rendre réductible un polynôme irréductible sur le corps de base :

> On voit au surplus que les propriétés et les difficultés d'une équation peuvent être tout à fait différentes suivant les quantités qui lui sont adjointes. Par exemple, l'adjonction d'une quantité peut rendre réductible une équation irréductible.
>
> Évariste Galois.

Par la suite nous utiliserons beaucoup les deux résultats suivants :

> Une équation irréductible ne peut avoir aucune racine commune avec une équation rationnelle sans la diviser.
>
> Car le plus grand commun diviseur entre l'équation irréductible proposée et l'autre équation sera encore rationnel ; donc, etc.
>
> Évariste Galois.

L'autre résultat n'est même pas annoncé dans le mémoire de Galois car considéré évident à l'époque :

Soit un polynôme à coefficients rationnels ayant comme racines $x_1, ...x_n$ et S un polynôme symétrique en ces racines, alors $S(x_1, ...x_n)$ est rationnel.

Où l'expression "S est symétrique en $x_1, ...x_n$" signifie que pour toute permutation $\sigma \in S_n$, $S(x_{\sigma(1)}, ...x_{\sigma(n)}) = S(x_1, ...x_n)$.

Chapter 2

La théorie de Galois... selon 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 (en effet, pour n = 0 ou 1 l'extension de corps est le corps initial).

Par la suite nous noterons E l'ensemble formé par les racines de P.

2.2 Résolvante de Galois

> Étant 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.
>
> Évariste Galois.

Par la suite, Galois note φ cette fonction, que nous appelons la "résolvante", et V la valeur de φ 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.

Lemme 2.2.1. *Il existe 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, $\varphi(y_1, ...y_n) \neq \varphi(z_1, ...z_n)$.*

Preuve. Prouvons ce lemme avec $A = N, B = N^2, C = N^3, \ldots$ où N est un entier suffisamment grand.

Prenons $N > \alpha/\beta$, où $\alpha = \sum_{i,j=1}^{n} |x_i - x_j|$ et $\beta = \min_{i,j\in|[1,n]|,i\neq j}|x_i - x_j|$.

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. □

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

Par la suite nous utiliserons le polynôme Q, défini comme le polynôme minimal de V.

2.3 Théorème de l'élément primitif

Pour montrer le théorème de l'élément primitif, nous aurons besoin d'un résultat préliminaire :

Lemme 2.3.1. *K[V] = K(V) est un corps.*

Preuve. Comme K[V]⊆ K(V), il ne reste qu'à montrer que K(V)⊆ K[V].

Soit F(V) ∈ K(V), $F(V) = \frac{a(V)}{b(V)}$ où A(V), B(V) ∈ K[V] et B(V) ≠ 0.

Comme B(V) ≠ 0, nous avons que B et Q sont premiers entre eux.

En effet soit W une racine de Q. Si W est racine de B, comme Q irréductible, nous avons que $Q|B$, et donc V est racine de B, ce qui contredit B(V) ≠ 0.

Donc B et Q n'ont aucune racine en commun, et ils sont premiers entre eux.

Faisons le bézout dans K[X] : il existe α, β dans K[X] tels que α(X)B(X) + β(X)Q(X) = 1, et comme Q(V) = 0, nous avons α(V)B(V) = 1, soit $\frac{1}{B(V)} = \alpha(V) \in$ K[V].

D'où F(V) = $\frac{A(V)}{B(V)}$ = A(V)$\alpha(V) \in$ K[V]. □

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.

Évariste Galois.

Proposition 2.3.2. $K[x_1, ...x_n] = K[V]$

Preuve. Comme $V = \varphi(x_1, ...x_n) \in K[x_1, ...x_n]$ nous avons $K[V] \subseteq K[x_1, ...x_n]$.

Pour avoir l'inclusion inverse il suffit de montrer que les racines $x_1, ...x_n$ s'expriment rationnellement en fonction de V.

En effet, dans ce cas nous avons $x_1 \in K(V)$, ... $x_n \in K(V)$, d'où $K[x_1, ...x_n] \subseteq K(V) = K[V]$, donc $K[x_1, ...x_n] = K[V]$, c'est à dire que V, la valeur de la résolvante en les racines de P, est l'élément primitif.

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 $\varphi_i(y_1, ...y_n) = \varphi(y_{\tau(1)}, ...y_{\tau(n)})$ est une résolvante.

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

D'où x_i est racine du polynôme $F_i(X) = \prod_{(y_2,...y_n)\in E^{n-1}}(V-\varphi_i(X, y_2, ...y_n))$, 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 : $\prod_{(y_2,...y_n)\in E^{n-1}}(V - \varphi_i(x_j, y_2, ...y_n)) = 0$

Comme $K[x_1, ...x_n]$ est intègre, il existe un (n-1)-uplet $(y_2, ...y_n)$ tel que $V - \varphi_i(x_j, y_2, ...y_n) = 0$, d'où $\varphi_i(x_j, y_2, ...y_n) = V = \varphi_i(x_i, ...x_{\tau(n)})$ 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 :
$\alpha(X)P(X) + \beta(X)F_i(X) = X - x_i$ dans K(V)[X].

En faisant X=0, nous avons $x_i = -\alpha(0)P(0) - \beta(0)F_i(0) \in K(V)$. □

Notons pour la suite $x_i = f_i(V) \in$ K(V) = K[V].

2.4 Construction des permutations des racines

Rappelons que Q est le polynôme minimal de V.

Notons $V_1, ...V_m$ ses racines, avec $V_1 = V$.

Nous utiliserons par la suite le résultat suivant :

Lemme 2.4.1. *Pour tout* V_k, $V_k = \varphi(f_1(V_k), ...f_n(V_k))$.

Preuve. Rappelons que $V_1 = \varphi(x_1, ...x_n) = \varphi(f_1(V_1), ...f_n(V_1))$, donc V_1 est racine de $X - \varphi(f_1(X), ...f_n(X)) \in$ k[X], d'où Q $|X - \varphi(f_1(X), ...f_n(X))$, d'où pour tout V_k, $V_k = \varphi(f_1(V_k), ...f_n(V_k))$. □

Ainsi, par les f_i chaque V_k est associé à un n-uplet $(f_1(V_k), ...f_n(V_k))$, et réciproquement par φ.

Nous pouvons donc construire le tableau suivant, où chaque ligne est caractérisée par un V_k et formée par le n-uplet $(f_1(V_k), ...f_n(V_k))$:

$$\begin{array}{c|cccc} V_1 & f_1(V_1) & f_2(V_1) & \dots & f_n(V_1) \\ V_2 & f_1(V_2) & f_2(V_2) & \dots & f_n(V_2) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ V_m & f_1(V_m) & f_2(V_m) & \dots & f_n(V_m) \end{array}$$

Nous alllons montrer par la suite que ce tableau donne le groupe de Galois associé à l'extension où l'on a ajouté les racines de P.

Les trois lemmes suivants vont nous permettre de déduire que chaque V_k définit une unique permutation des racines de P, puis à la section suivante nous montrerons que l'ensemble des permutations de S_n associé est bien un groupe, qui ne dépend que de P et de la résolvante φ.

Enfin, à la dernière section, nous montrerons que ce groupe ne dépend en fait que de P.

> 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. Soit V, V', V"... les racines de cette équation irréductible. Si a = f(V) est une des racines de la proposée, f(V') de même sera une racine de la proposée.
>
> Évariste Galois.

Lemme 2.4.2. *Pour tout j, $k \in |[1, n]|$, $f_j(V_k)$ est une racine de P.*

C'est à dire que les éléments du tableau sont des racines de P.

Preuve. Soit x_j une racine quelconque de P, et $F_j(X) = \prod_{i=1}^{n}(x_i - f_j(X))$ symétrique en les x_i donc dans K[X].

Comme $x_j = f_j(V_1)$, V_1 est racine de $F_j(X)$, d'où Q(X) divise $F_j(X)$, et $V_1, ...V_m$ sont racines de F_j.

Donc pour chaque V_k il existe i tel que $x_i - f_j(V_k) = 0$, donc les $f_j(V_k)$ sont des racines de P. □

Lemme 2.4.3. *Pour un k fixé, les $f_j(V_k)$ sont distincts.*

C'est à dire que chaque ligne du tableau est une permutation des racines de P.

Preuve. 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 $x_i \neq x_j$. □

Lemme 2.4.4. *Deux racines distinctes de Q définissent deux permutations distinctes des racines de P.*

C'est à dire que chaque ligne du tableau est distincte des autres.

Preuve. Montrons le lemme par contraposée.

Soient deux permutations définies par deux racines de Q V_j et V_k, si ces permutations sont égales,

alors $(f_1(V_j), \ldots\ f_n(V_j)) = (f_1(V_k), \ldots\ f_n(V_k))$,

d'où $V_j = \varphi(f_1(V_j), \ldots f_n(V_j)) = \varphi(f_1(V_k), \ldots f_n(V_k)) = V_k$. □

Proposition 2.4.5. *Chaque V_k définit une unique permutation des racines de P.*

Preuve. En effet, comme il y a n applications f_i et que par le lemme 2.4.2 les $f_j(V_k)$ sont des racines de P, pour un V_k fixé les $f_j(V_k)$ donnent au plus n racines de P.

De plus, comme elles sont distinctes (lemme 2.4.3), il y en a exactement n. Donc en fixant un V_k nous obtenons un unique n-uplet $(f_1(V_k), \ldots\ f_n(V_k))$, qui est une permutation des racines de P, et le lemme 2.4.4 nous assure que ces permutations sont distinctes. □

2.5 Définition du groupe de Galois

Comme, à k fixé, $(f_1(V_k), \ldots\ f_n(V_k))$ est une permutation des racines de P, il existe $\sigma_k \in S_n$ telle que :

$(f_1(V_k), \ldots\ f_n(V_k)) = (x_{\sigma_k(1)}, \ldots\ x_{\sigma_k(n)}) = (f_{\sigma_k(1)}(V_1), \ldots\ f_{\sigma_k(n)}(V_1))$

D'où $V_k = \varphi(f_1(V_k), \ldots f_n(V_k)) = \varphi(f_{\sigma_k(1)}(V_1), \ldots f_{\sigma_k(n)}(V_1)) =: F_{\sigma_k}(V_1)$.

Définition 2.5.1. *Gal* $:= \{\sigma \in S_n,\ F_\sigma(V_1)$ *racine de* $Q\}$

Notons que Gal ne dépend que de P et de la résolvante φ.

Comme $V_1 = \varphi(x_1, ...x_n)$ nous avions que Q(Y) divise $\prod_{\sigma \in S_n}(Y - \varphi(x_{\sigma(1)}, ...x_{\sigma(n)}))$, donc Q(Y) est un produit de $(Y - \varphi(x_{\sigma(1)}, ...x_{\sigma(n)}))$. En fait, les σ sont les éléments de Gal :

Lemme 2.5.2. $Q(Y) = \prod_{\sigma \in Gal}(Y - \varphi(x_{\sigma(1)}, ...x_{\sigma(n)}))$

Preuve. Pour tout $\sigma \in$ Gal, $\varphi(x_{\sigma(1)}, ...x_{\sigma(n)}) = \varphi(f_{\sigma(1)}(V_1), ...f_{\sigma(n)}(V_1)) = F_\sigma(V_1)$ est racine de Q.

Donc les racines de $\prod_{\sigma \in Gal}(Y - \varphi(x_{\sigma(1)}, ...x_{\sigma(n)}))$ sont des racines de Q, d'où $\prod_{\sigma \in Gal}(Y - \varphi(x_{\sigma(1)}, ...x_{\sigma(n)}))$ divise Q.

Or, comme chaque V_k définit une unique permutation σ_k des racines, il y a autant de V_k que de σ_k, et donc $\prod_{\sigma \in Gal}(Y - \varphi(x_{\sigma(1)}, ...x_{\sigma(n)}))$ et Q sont de même degré.

D'où il existe $\lambda \in$ K tel que $\prod_{\sigma \in Gal}(Y - \varphi(x_{\sigma(1)}, ...x_{\sigma(n)})) = \lambda Q$, et comme $\prod_{\sigma \in Gal}(Y - \varphi(x_{\sigma(1)}, ...x_{\sigma(n)}))$ et Q sont unitaires, nous avons l'égalité. □

Pour montrer que Gal est un groupe, nous aurons besoin d'un lemme préliminaire, que nous réutiliserons par la suite :

Lemme 2.5.3. $\forall \sigma \in Gal, \exists k \in |[1, m]|, \forall j \in |[1, n]|, f_{\sigma(j)}(V_1) = f_j(V_k)$

Preuve. Comme $\sigma \in$ Gal, il existe k tel que $V_k = F_\sigma(V_1) = \varphi(f_{\sigma(1)}(V_1), ...f_{\sigma(n)}(V_1))$, et comme $V_k = \varphi(f_1(V_k), ...f_n(V_k))$, par la propriété de la résolvante nous avons que pour tout j $\in |[1, n]|$, $f_{\sigma(j)}(V_1) = f_j(V_k)$. □

Proposition 2.5.4. *Gal est un groupe pour la composition.*

Preuve. Gal est un sous ensemble de S_n, qui est un groupe.

Donc pour montrer que Gal est un groupe, il suffit de montrer qu'il est un sous-groupe de S_n, c'est à dire qu'il contient l'identité et qu'il est stable par composition et inversion.

$$\begin{aligned} \text{Comme } F_{id}(V_1) &= \varphi(f_{id(1)}(V_1), ...f_{id(n)}(V_1)) \\ &= \varphi(f_1(V_1), ...f_n(V_1)) \\ &= \varphi(x_1, ...x_n) \\ &= V_1 \end{aligned}$$

$F_{id}(V_1)$ est bien une racine de Q, donc id $\in$ Gal.

Comme S_n est un groupe fini, il suffit de montrer que Gal est stable par composition pour avoir la stabilité par inversion (Lagrange).

Il ne reste donc plus qu'à montrer qu'il est stable par composition.

Soient τ, $\sigma \in$ Gal.

Comme $\tau \in$ Gal, il existe k tel que pour tout j $\in |[1, n]|$, $f_{\tau(j)}(V_1) = f_j(V_k)$.

$$\begin{array}{rcl} \text{D'où } F_{\tau\circ\sigma}(V_1) & = & \varphi(f_{\tau(\sigma(1))}(V_1), ...f_{\tau(\sigma(n))}(V_1)) \\ & = & \varphi(f_{\sigma(1)}(V_k), ...f_{\sigma(n)}(V_k)) \\ & = & F_\sigma(V_k) \end{array}$$

Comme $\sigma \in$ Gal, $F_\sigma(V_1)$ est une racine de Q, d'où $Q(F_\sigma(V_1)) = 0$, d'où V_1 est racine de $Q(F_\sigma(X))$, d'où Q $|Q(F_\sigma(X))$, d'où V_k est racine de $Q(F_\sigma(X))$, d'où $Q(F_\sigma(V_k)) = 0$, d'où $F_\sigma(V_k)$ est racine de Q.

Donc $F_{\tau\circ\sigma}(V_1) = F_\sigma(V_k)$ est racine de Q, d'où $\tau \circ \sigma \in$ Gal.

Donc Gal est stable par composition, et donc Gal est un groupe. □

2.6 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.
>
> Évariste Galois.

En fait nous nous intéresssons à la propriété (2) pour un certain σ, que nous reformulons ainsi : $\forall F \in K[X_1, ...X_n], F(x_1, ...x_n) = 0 \Rightarrow F(x_{\sigma(1)}, ...x_{\sigma(n)}) = 0$.

Proposition 2.6.1. *Gal vérifie (2).*

Preuve. Soit $\sigma \in$ Gal, d'où (d'après le lemme 2.5.3) il existe k tel que pour tout j $\in |[1, n]|$, $x_{\sigma(j)} = f_{\sigma(j)}(V_1) = f_j(V_k)$, et $F(x_{\sigma(1)}, ...x_{\sigma(n)}) = F(f_1(V_k), ...f_n(V_k)) = \psi(V_k)$, où $\psi \in$ K[X].

Nous supposons $F(x_1, ...x_n) = 0$, et nous voulons montrer que $F(x_{\sigma(1)}, ...x_{\sigma(n)}) = \psi(V_k) = 0$.

$0 = F(x_1, ...x_n) = F(f_1(V_1), ...f_n(V_1)) = \psi(V_1)$, d'où V_1 est racine de ψ, d'où $Q|\psi$, d'où V_k est racine de ψ, et $F(x_{\sigma(1)}, ...x_{\sigma(n)}) = \psi(V_k) = 0$. □

Proposition 2.6.2. *Gal est le plus grand groupe vérifiant (2).*

Preuve. Soit $\sigma \in S_n$ vérifiant (2), montrons qu'elle est dans Gal :

Rappelons que $Q(Y) = \prod_{\tau\in Gal}(Y - \varphi(x_{\tau(1)}, ...x_{\tau(n)}))$, et notons :

$Q_\sigma(Y) = \prod_{\tau\in Gal}(Y - \varphi(x_{\tau\circ\sigma(1)}, ...x_{\tau\circ\sigma(n)}))$

Il suffit de montrer que Q $= Q_\sigma$.

En effet, comme $V_1 = \varphi(x_1, ...x_n)$ est racine de Q(Y), nous avons :

$$\begin{array}{rcl} 0 & = & Q(V_1) \\ & = & Q_\sigma(V_1) \\ & = & \prod_{\tau\in Gal}(V_1 - \varphi(x_{\tau\circ\sigma(1)}, ...x_{\tau\circ\sigma(n)})) \\ & = & \prod_{\tau\in Gal}(\varphi(x_1, ...x_n) - \varphi(x_{\tau\circ\sigma(1)}, ...x_{\tau\circ\sigma(n)})) \end{array}$$

Donc il existe $\tau \in$ Gal tel que $\varphi(x_1, ...x_n) = \varphi(x_{\tau\circ\sigma(1)}, ...x_{\tau\circ\sigma(n)})$.

D'où (par la propriété de la résolvante), pour tout i $\in |[1, n]|$, $x_{\tau\circ\sigma(i)} = x_i$.

Comme les racines sont dictinctes nous avons que pour tout i $\in |[1, n]|$, $\tau \circ \sigma(i) = i$.

D'où $\tau \circ \sigma =$ id, d'où $\sigma = \tau^{-1} \in$ Gal (car Gal est un groupe).

Donc n'importe quel sous groupe de S_n dont les éléments vérifient (2) est inclu dans Gal.

Il ne reste qu'à montrer que Q $= Q_\sigma$:

Chaque $\tau \in$ Gal est associée à un unique V_k, donc nous pouvons noter Gal $= \{\tau_1, ...\tau_m\}$,

d'où : $Q(Y) = \prod_{k=1}^{m}(Y - V_k)$, où $V_k = \varphi(x_{\tau_k(1)}, ...x_{\tau_k(n)})$,

et : $Q(Y) = \sum_{k=1}^{m}(-1)^k s_k(V_1, ...V_m)Y^{m-k}$, où s_k est le polynôme symétrique élémentaire de degré k dans $K[X_1, ...X_m]$.

$s_k(V_1, ...V_m) = s_k(\varphi(x_{\tau_1(1)}, ...x_{\tau_1(n)}), ...\varphi(x_{\tau_m(1)}, ...x_{\tau_m(n)})) =: S_k(x_1, ...x_n)$, où $S_k \in K[X_1, ...X_n]$.

Comme Q est à coefficients dans K, $S_k(x_1, ...x_n) = s_k(V_1, ...V_m) \in$ K pour tout k.

De même pour Q_σ :

$$\begin{array}{rcl} Q_\sigma(Y) & = & \prod_{\tau\in Gal}(Y - \varphi(x_{\tau\circ\sigma(1)}, ...x_{\tau\circ\sigma(n)})) \\ & = & \prod_{k=1}^{m}(Y - \varphi(x_{\tau_k\circ\sigma(1)}, ...x_{\tau_k\circ\sigma(n)})) \\ & = & \prod_{k=1}^{m}(Y - V_k^\sigma) \text{ où } V_k^\sigma \\ & = & \varphi(x_{\tau_k\circ\sigma(1)}, ...x_{\tau_k\circ\sigma(n)}) \end{array}$$

D'où $Q_\sigma(Y) = \sum_{k=1}^{m}(-1)^k s_k(V_1^\sigma, ...V_m^\sigma)Y^{m-k}$,

$$\begin{array}{rcl} \text{et } s_k(V_1^\sigma, ...V_m^\sigma) & = & s_k(\varphi(x_{\tau_1\circ\sigma(1)}, ...x_{\tau_1\circ\sigma(n)}), ...\varphi(x_{\tau_m\circ\sigma(1)}, ...x_{\tau_m\circ\sigma(n)})) \\ & = & S_k(x_{\sigma(1)}, ...x_{\sigma(n)}) \end{array}$$

Soit $F_k(X_1, ...X_n) := S_k(X_1, ...X_n) - S_k(x_1, ...x_n) \in K[X_1, ...X_n]$.

Comme $F_k(x_1, ...x_n) = 0$ et que σ vérifie la propriété (2), nous avons $F_k(x_{\sigma(1)}, ...x_{\sigma(n)}) = 0$, d'où $S_k(x_{\sigma(1)}, ...x_{\sigma(n)}) = S_k(x_1, ...x_n)$, pour tout k.

$$\begin{array}{rcl} \text{D'où : } Q_\sigma(Y) & = & \sum_{k=1}^{m}(-1)^k s_k(V_1^\sigma, ...V_m^\sigma)Y^{m-k} \\ & = & \sum_{k=1}^{m}(-1)^k S_k(x_{\sigma(1)}, ...x_{\sigma(n)})Y^{m-k} \\ & = & \sum_{k=1}^{m}(-1)^k S_k(x_1, ...x_n)Y^{m-k} \\ & = & \sum_{k=1}^{m}(-1)^k s_k(V_1, ...V_m)Y^{m-k} \\ & = & Q(Y) \end{array}$$

□

En fait, l'ensemble des permutations de S_n vérifiant (2) est un groupe, qui n'est autre que Gal, résultat que nous allons démontrer pour affirmer que :

Théorème 2.6.3. *Gal ne dépend que de P.*

Preuve. Rappelons que Gal ne dépendait que de P et de la résolvante φ que nous avons utilisé pour le construire.

Gal vérifie (2) d'où :

Gal $\subseteq \{\sigma \in S_n, \forall F \in K[X_1, ...X_n], F(x_1, ...x_n) = 0 \Rightarrow F(x_{\sigma(1)}, ...x_{\sigma(n)}) = 0\}$,

or tout $\sigma \in S_n$ vérifiant (2) est dans Gal, nous avons l'inclusion inverse, donc Gal $= \{\sigma \in S_n, \forall F \in K[X_1, ...X_n], F(x_1, ...x_n) = 0 \Rightarrow F(x_{\sigma(1)}, ...x_{\sigma(n)}) = 0\}$, qui ne dépend que des racines de P. □

Donc le groupe Gal ne dépend que de P, nous l'appelons le groupe de Galois associé à l'extension où l'on a ajouté les racines de P.