ANNALES DE LA FACULTÉ DES SCIENCES DE TOULOUSE

T. LALESCO

La théorie générale de Galois

Annales de la faculté des sciences de Toulouse 2^e série, tome 10 (1908), p. 113-123

<http://www.numdam.org/item?id=AFST_1908_2_10__113_0>

LA

THÉORIE GÉNÉRALE DE GALOIS,

PAR M. T. LALESCO.

1. Le présent Travail est un exposé de la théorie générale de Galois pour les équations algébriques, en prenant pour point de départ la propriété fondamentale du groupe de Galois de caractériser le domaine de rationalité d'une équation algébrique. Une démonstration, à ce point de vue, du théorème de Galois a été donnée pour la première fois par J. Sörderberg (1). MM. J. Drach (2) et Vessiot ont approfondi cette manière d'envisager la question, en mettant en évidence le rôle joué par les relations auxiliaires qui existent entre les racines d'une équation. M. Vessiot (3) a introduit ainsi la notion des systèmes automorphes et en a déduit une démonstration du théorème de Galois, qu'il a étendu ensuite aux équations différentielles linéaires.

Ce point de vue est certainement plus logique; la méthode de Galois, qui est une méthode de découverte, donne une importance particulière aux résolvantes appelées aujourd'hui les résolvantes de Galois; or ces résolvantes ne se distinguent des autres résolvantes totales que par une propriété qui les rend plus accessibles mais nullement plus importantes, de sorte que lorsqu'on approfondit la structure d'un corps algébrique, on est obligé de faire un détour pour arriver à l'idée fondamentable du cycle des résolvantes.

Dans la méthode directe que nous suivons, un point important est de trouver une démonstration simple du théorème de Galois; celle qui est donnée dans ce Mémoire découle simplement du théorème fondamental des fonctions symétriques et de celui de Lagrange, le caractère de relativité du groupe de Galois apparaissant clairement de la définition elle-même. L'analyse détaillée de la structure du corps algébrique nous conduit ensuite avec une grande simplicité à tous les résultats de la théorie générale de Galois; on remarquera une démonstration intuitive du théorème de Kronecker sur la possibilité de réduction d'un groupe de Galois.

(1) *Acta mathematica,* 1888, p. 297.

(2) E. BOREL et J. DRACH, *Introduction à la théorie des nombres.*

(3) *Annales de l'École Normale supérieure,* 1904, p. 1-85.

2. Au commencement je vais rappeler quelques propositions élémentaires de la théorie des groupes et plus précisément les théorèmes de Cauchy et Lagrange, simplement pour fixer le langage dans ce qui va suivre.

Étant donnés un groupe P de degré p et un de ses sous-groupes Q de degré $q(p=rq)$, et si l'on désigne par $S_1, S_2, \ldots, S_q$ les permutations du sous-groupe Q, les permutations de P peuvent être rangées dans un Tableau de la forme

$$\begin{array}{cccc} S_1T_1 & S_2T_1 & \ldots & S_qT_1, \\ S_1T_2 & S_2T_2 & \ldots & S_qT_2, \\ \ldots\ldots & \ldots\ldots & \ldots & \ldots\ldots, \\ S_1T_r & S_2T_r & \ldots & S_qT_r, \end{array}$$

$T_1, T_2, \ldots, T_r$ étant des permutations convenables de P qui ne se trouvent pas en Q.

J'appellerai ce Tableau, le Tableau de P relatif à Q.

On peut présenter le théorème de Lagrange de la manière suivante :

Les notations ci-dessus étant conservées, supposons que P contient des permutations de n lettres : $x_1, x_2, \ldots, x_n$, et appelons les fonctions des n lettres qui permettent (1) ce groupe de permutations, les *quantités données*. Supposons à présent qu'il existe une fonction $\varphi(x_1, x_2, \ldots, x_n)$ qui permet les permutations de Q et qui prend la même valeur ou des valeurs différentes pour les permutations du groupe P suivant que ces permutations appartiennent à une même ligne ou à des lignes différentes du Tableau de P relatif à Q; désignons par $\varphi_1, \varphi_2, \ldots, \varphi_r$ les r valeurs différentes ainsi obtenues. On appelle une telle fonction, une *fonction du sous-groupe* Q *relatif à* P *ou appartenant à* Q.

Relativement à ces fonctions on a les deux propositions suivantes :

1° (Théorème de Lagrange.) *Une fonction qui permet les permutations du sous-groupe* Q (mais qui peut en permettre encore d'autres) *est une fonction donnée d'une fonction quelconque appartenant à ce sous-groupe;*

2° *Deux fonctions d'un sous-groupe* Q *relatives à* P *sont des fonctions données l'une de l'autre.*

Ces deux théorèmes peuvent être lus, une fois pour toutes, sur la formule

$$\Phi(y)\left[\frac{\psi_1}{y-\varphi_1}+\frac{\psi_2}{y-\varphi_2}+\ldots+\frac{\psi_r}{y-\varphi_r}\right]=F(y),$$

où

$$\Phi(y)=(y-\varphi_1)(y-\varphi_2)\ldots(y-\varphi_r),$$

(1) Cela veut dire qu'elles ne changent pas de *valeur* si on leur applique ces permutations. Dans ce qui suit, il s'agira, pour fixer les idées, de la *valeur arithmétique* des expressions, c'est-à-dire les lettres $x_1, x_2, \ldots, x_n$ représentent des nombres bien déterminés; mais tous les raisonnements s'appliquent aussi au cas général d'un nombre quelconque de paramètres.

et $\psi_1, \psi_2, \ldots, \psi_r$ désignent les valeurs toutes différentes ou non d'une fonction qui permet aussi les permutations de Q. Il suffit de remarquer que $F(y)$ permet les permutations de P en se rappelant qu'elles forment un groupe et que $\Phi'(\varphi_i) \not\equiv 0$ d'après la définition de φ.

LE GROUPE DE L'ÉQUATION.

3. Partons d'une équation

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n = 0,$$

qui soit irréductible ou non dans le domaine

$$D(a_0, a_1, a_2, \ldots, a_n),$$

et dont les racines soient $x_1, x_2, \ldots, x_n$.

Le domaine $D(a_0, a_1, a_2, \ldots, a_n)$ est l'ensemble de toutes les fonctions rationnelles des coefficients de l'équation, c'est-à-dire de toutes les fonctions qui dérivent des coefficients à l'aide des quatre opérations fondamentales. On l'appelle le *domaine de rationalité* de l'équation.

Considérons à présent l'ensemble de toutes les fonctions rationnelles des racines $x_1, x_2, \ldots, x_n$ de l'équation. Cet ensemble contiendra aussi toutes les fonctions symétriques fondamentales, par conséquent aussi le domaine de rationalité de l'équation; j'appellerai cet ensemble *le corps de l'équation*.

Cela posé, considérons toutes les grandeurs du corps qui font partie du domaine de rationalité de l'équation. J'appellerai ces grandeurs *les quantités connues* du corps. Nous savons qu'on en trouve toujours, par exemple les fonctions symétriques fondamentales. Mais, par suite de la nature particulière de l'équation considérée, il peut se faire qu'on en puisse trouver encore d'autres. Supposons par exemple qu'entre les racines de notre équation, il existe la relation $5x_1x_2 = 3x_n + x_3$.

Il est évident que, dans ce cas, la fonction

$$\frac{3x_n + x_3}{x_1 x_2} = 5$$

sera aussi une quantité connue, et ainsi de suite.

Cela posé, prenons l'ensemble de *toutes* les permutations qui laissent invariables les valeurs de *toutes* ces quantités connues.

Il coïncidera avec le groupe symétrique, que nous désignons dorénavant par P, si entre les racines de l'équation il n'existe aucune relation à coefficients appartenant à D; il peut aussi se réduire à la substitution identique.

Cet ensemble forme un groupe. En effet appliquons une quelconque de ses

permutations. Une quantité connue se transforme dans une autre quantité connue puisque sa valeur n'a pas changé; donc en appliquant une permutation de l'ensemble, les quantités ne font que s'échanger entre elles. Il suit de là que le produit des deux permutations laissera aussi invariables les valeurs des quantités connues; il appartiendra donc aussi à l'ensemble, ce qui démontre la proposition.

Appelons Q ce groupe; il contient toutes les permutations qui n'altèrent pas les valeurs des quantités connues.

Toute autre permutation de P altère la valeur d'une, au moins, des quantités connues.

On appelle ce groupe le *groupe de Galois* de l'équation donnée.

Nous allons démontrer à présent que ce groupe est encore plus intimement lié aux quantités connues dans ce sens que non seulement les valeurs des quantités connues restent inaltérées aux permutations du groupe de Galois, mais qu'en outre ce sont les seules; autrement dit, si l'on trouve qu'une grandeur du corps permet les permutations du groupe Q, on peut affirmer que c'est une quantité connue.

Nous allons démontrer cette proposition fondamentale connue sous le nom de *théorème de Galois,* en remarquant simplement que l'on peut déterminer une quantité connue du corps qui soit une fonction du groupe Q relatif au groupe symétrique P.

En effet, parmi les quantités connues du corps, il y en a au moins une qui change de valeur si on lui applique la permutation T_2 de la seconde ligne du Tableau de P relatif à Q; autrement, cette permutation laisserait aussi inaltérées les valeurs de toutes les quantités connues, ce qui est contre l'hypothèse que Q contient toutes les permutations de cette catégorie. Appliquons à cette quantité les permutations de Q; nous obtiendrons ainsi q expressions différentes ou non, mais dont la valeur est la même, puisque nous avons à faire avec une quantité connue. Or la valeur de ces expressions ne reste pas la même si on leur applique la permutation T_2, puisque, par exemple, la quantité primitive prend sûrement une autre valeur; donc on peut trouver une fonction symétrique A de ces expressions, qui elle-même change de valeur si on lui applique la permutation T_2 (1). Cette quantité, par suite de sa symétrie, prendra donc la même valeur pour les permutations d'une même ligne du Tableau, et changera sûrement de valeur pour les permutations de la seconde ligne.

Le même raisonnement s'applique pour chaque ligne; on peut donc trouver des

(1) En effet, si *toutes* les fonctions symétriques fondamentales de ces expressions restaient inaltérées par la substitution T_2, ces expressions ne pourraient que s'échanger entre elles, et par conséquent garder la même valeur; or nous savons qu'il y en a une au moins, la première choisie, qui change sûrement de *valeur*.

quantités *connues* du corps $A_1, A_2, \ldots, A_r$ telles que si l'on applique les permutations d'une ligne du Tableau, l'une au moins de ces grandeurs change de valeur, chacune d'elles prenant la même valeur pour toutes les permutations d'une même ligne. L'expression $u = u_1 A_1 + u_2 A_2 + \ldots + u_r A_r$, dans laquelle $u_1, u_2, \ldots, u_r$ désignent des paramètres, ne prend donc des valeurs identiquement égales pour deux permutations appartenant à des lignes différentes. Dès lors, on peut déterminer d'une infinité de manières les paramètres $u_1, u_2, \ldots, u_r$ dans le domaine D, de manière que les *valeurs mêmes* soient différentes; ce qui montre simplement que la fonction u est, d'après la définition, une fonction du groupe Q relatif à P.

Le théorème de Lagrange répond à présent immmédiatement à la question. Observons d'abord que, d'après le théorème fondamental des fonctions symétriques, toutes les fonctions données du groupe symétrique P sont les fonctions rationnelles de $a_0, a_1, \ldots, a_n$. Prenons maintenant une fonction qui admette les permutations de Q; d'après le théorème de Lagrange elle sera une fonction donnée (avec des coefficients rationnels en $a_0, a_1, \ldots, a_n$) d'une fonction quelconque appartenant à Q. Mais nous venons de trouver parmi les quantités connues une telle fonction. Donc notre fonction sera une fonction rationnelle d'une quantité connue, c'est-à-dire aussi une quantité connue. C. Q. F. D.

4. La notion du groupe de Galois est essentiellement relative; sa définition et le théorème de Galois montrent qu'elle naît de la considération du domaine des quantités connues $D(a_0, a_1, \ldots, a_n)$ qu'elle caractérise. Si l'on élargit le domaine des quantités connues, si nous avons le moyen de connaître d'autres fonctions des racines, d'autres grandeurs du corps qui n'appartiennent nécessairement à D, et si l'on considère comme connu, outre l'ensemble D, l'ensemble plus élargi qui contient aussi ces quantités, il est clair que le groupe des permutations qui laisseront inaltérées les valeurs de toutes ces grandeurs, sera un sous-groupe de Q, car elles doivent d'abord appartenir à Q, puisque dans notre nouveau domaine se trouve aussi le domaine D, et d'autre part toutes les permutations de Q ne peuvent pas appartenir au nouveau groupe, car il y en aura certainement qui changeront les nouvelles grandeurs introduites comme connues.

On peut remarquer que la définition et la démonstration du théorème de Galois s'appliquent mot à mot, quel que soit le domaine des quantités connues, pourvu qu'il dérive d'un nombre quelconque de grandeurs du corps, à l'aide des quatre opérations fondamentales et avec des coefficients appartenant à D.

Par rapport à ce domaine, le nouveau sous-groupe jouira donc des mêmes propriétés que le groupe de Galois par rapport au domaine de rationalité, et c'est dans ce sens que l'on doit comprendre la locution si souvent employée : « Le groupe de Galois se réduit à un de ses sous-groupes »; cela veut dire simplement

que par rapport au nouveau domaine connu, le rôle et les propriétés du groupe de Galois appartiennent maintenant à son sous-groupe.

L'ÉTUDE DU CORPS.

5. Prenons une grandeur du corps qui ne soit pas connue. Cette grandeur peut ne permettre aucune permutation du groupe Q; on a un tel exemple dans l'expression linéaire $u_1x_1+u_2x_2+\ldots+u_nx_n$ pour des valeurs convenablement choisies des u. On peut dire que cette grandeur appartient à la substitution identique (relatif à Q, ce que l'on sous-entendra dorénavant), et on l'appelle un *élément primitif* du corps.

Mais il peut se faire que la fonction $\varphi(x_1, x_2, \ldots, x_n)$ considérée permette quelques permutations de Q. *Ces permutations forment un groupe* Q_1 (1). Si nous nous imaginons le Tableau de Q relatif à Q_1, la fonction φ change de valeur si nous lui appliquons des permutations qui ne se trouvent pas dans la première ligne : elle prend la même valeur pour les permutations d'une même ligne et des valeurs différentes pour des permutations de lignes différentes (1). C'est donc *une fonction du sous-groupe* Q_1. Soient $\varphi_1, \varphi_2, \ldots, \varphi_r$ les r valeurs différentes ainsi obtenues qui s'appellent des *éléments conjugués*.

L'équation

$$\Phi(y)=(y-\varphi_1)(y-\varphi_2)\ldots(y-\varphi_r)=0$$

est une équation dont les coefficients appartiennent à $D(a_0, a_1, \ldots, a_n)$ parce qu'elle admet les permutations de Q quel que soit y; elle y est de plus irréductible puisqu'un produit d'un nombre moindre de facteurs ne reste pas identiquement égal à lui-même pour toutes les permutations de Q, c'est-à-dire n'est pas une quantité connue.

Les fonctions $\varphi_2, \ldots, \varphi_r$ appartiennent aussi à des sous-groupes de Q; pour les trouver observons, par exemple, pour la fonction φ_2, qu'on a

$$\varphi_2=\varphi_1(S_1T_2)=\varphi_1(S_2T_2)=\ldots=\varphi_1(S_qT_2).$$

Si donc U désigne une permutation qui transforme une permutation de la forme S_kT_2 en une autre de la forme S_iT_2, nous aurons

$$S_iT_2=S_kT_2U,$$

d'où l'on tire

$$U=T_2^{-1}S_k^{-1}S_iT_2=T_2^{-1}S_cT_2.$$

---

(1) Cela résulte, comme c'est bien connu, très simplement des propriétés du groupe de Galois.

Toutes les permutations de la forme $T_2^{-1} S_e T_2$ ($e = 1, 2, \ldots, r$) laissent évidemment invariable la fonction φ_2 et, d'après ce que nous venons de voir, elle seulement. Elles forment donc un groupe et c'est à ce groupe qu'appartient donc la fonction φ_2. En répétant le même raisonnement pour toutes les fonctions φ, nous obtenons r sous-groupes de Q de même degré, qui peuvent être représentés symboliquement sous la forme $T_1^{-1} S T_1$, $T_2^{-1} S T_2$, ..., $T_n^{-1} S T_n$ et qui s'appellent des *sous-groupes conjugués*.

6. Cela posé, on peut faire la remarque suivante :

Chaque grandeur du corps permet la permutation identique; donc, d'après le théorème de Lagrange, *chaque grandeur du corps s'exprime rationnellement à l'aide d'un élément primitif.*

Mais, d'autre part, toutes les valeurs conjuguées d'un élément primitif sont évidemment des grandeurs du corps et aussi primitifs; donc, l'équation irréductible que satisfait l'élément primitif jouit de la propriété que toutes ses racines s'expriment rationnellement en fonction de l'une quelconque d'entre elles. C'est donc une équation *normale*. On appelle ces équations *les résolvantes de Galois de l'équation,* ou *de son corps;* la dernière désignation est préférable comme on verra par la suite. Leur degré N est égal au degré du groupe de Galois; on appelle, pour cette raison, l'élément important N *le degré du corps et du groupe.*

7. Considérons maintenant la fonction quelconque du corps $\varphi(x_1, x_2, \ldots, x_n)$; nous avons vu qu'elle satisfait à une équation irréductible $\Phi(y) = 0$ dont les autres racines $\varphi_2, \ldots, \varphi_r$ sont ses éléments conjugués, et que ces fonctions sont les fonctions de r sous-groupes conjugués de degré q : Q_1, Q_2, ..., Q_r. Il peut arriver deux cas :

α. Tous ces différents groupes peuvent n'avoir aucune permutation commune. Si nous considérons donc l'expression $u = u_1\varphi_1 + u_2\varphi_2 + \ldots + u_r\varphi_r$, cette expression ne restera identiquement égale à elle-même pour aucune permutation de Q, car une telle permutation se trouvant en un Q_i, ne peut pas se trouver à la fois dans tous les Q, d'après l'hypothèse. On en conclut que c'est un élément primitif du corps. On a donc ce résultat remarquable :

L'équation $\Phi(y) = 0$ *a le même corps que l'équation* $F(x) = 0$.

Les racines de l'une sont fonctions rationnelles de l'autre et inversement. Nous appellerons de telles équations comme $F(x) = 0$, $\Phi(y) = 0$, par rapport au corps, *ses résolvantes totales*. En particulier, les résolvantes de Galois sont aussi des résolvantes totales, mais avec une propriété de plus, elles sont aussi normales.

β. Les sous-groupes Q_1, Q_2, ..., Q_r peuvent avoir un certain nombre de per-

mutations communes; cet ensemble forme un groupe I commun et on l'appelle ordinairement *le plus grand commun diviseur* des Q_i. Dans ce cas, l'expression $u = u_1\varphi_1 + u_2\varphi_2 + \ldots + u_i\varphi_i$ permettra les permutations de I et, pour des valeurs convenablement choisies des paramètres, seulement celles-là; c'est donc une fonction de I et, d'après le théorème de Lagrange, c'est un élément primitif du corps $D(\varphi_1, \varphi_2, \ldots, \varphi_r)$. L'équation irréductible à laquelle satisfait u sera de degré i, i étant l'indice de I et sera naturellement une résolvante de Galois du corps $D(\varphi_1, \varphi_2, \ldots, \varphi_r)$. Nous trouvons donc ce résultat :

Si les sous-groupes $Q_1, Q_2, \ldots, Q_r$ *ont un sous-groupe commun* I, *le corps* $D(\varphi_1, \varphi_2, \ldots, \varphi_r)$ *est une partie seulement du corps* $D(x_1, x_2, \ldots, x_n)$ *et son degré est égal à l'indice i de* I.

Nous désignerons cette circonstance en disant que le corps a un sous-corps et nous appellerons les équations $\Phi(y) = 0$ dans ce cas, des *résolvantes partielles* du corps. La connaissance des racines d'une résolvante partielle ne fait donc connaître qu'un sous-corps du corps.

8. Une propriété remarquable des résolvantes concerne la relation qui existe entre leurs groupes et peut être établie de la manière suivante :

Chaque élément d'un corps d'une équation, comme tout nombre algébrique, satisfait à une seule équation irréductible. Par conséquent, les autres racines de l'équation irréductible à laquelle satisfait un élément du corps sont ses éléments conjugués. Si l'élément est primitif et si l'on connaît les autres racines de son équation irréductible, les permutations à l'aide desquelles on passera à celles-ci seront donc les permutations du groupe de Galois de l'équation dont les racines ont engendré le corps en question. On a ainsi un moyen pratique de trouver ces permutations.

Ainsi, par exemple, si l'on considère une résolvante totale du corps, nous avons trouvé comme élément primitif de son corps l'expression $u = u_1\varphi_1 + u_2\varphi_2 + \ldots + u_r\varphi_r$, et l'on obtient ses valeurs conjuguées en appliquant aux x_i les permutations du groupe de Galois de l'équation $F(x) = 0$. A chaque permutation des x_i correspond une permutation des φ_i et ce sont ces permutations qui constitueront, d'après ce que nous venons de voir, le groupe de la résolvante totale considérée.

Donc *les résolvantes totales d'un corps ont leurs groupes de Galois isomorphes* et tous ces groupes découlent simplement de l'un quelconque d'entre eux.

En particulier, le groupe d'une résolvante de Galois, dont les racines sont θ_1, $\theta_2, \ldots, \theta_N$, se composera des substitutions $(\theta_1\theta_1)$, $(\theta_1\theta_2)$, $(\theta_1\theta_3)$, $\ldots$, $(\theta_1\theta_N)$, et c'est en prenant pour point de départ ce groupe particulier que, Galois le premier, et après lui tous les auteurs ont présenté cette théorie.

Pour le cas d'une résolvante partielle, le même raisonnement nous permet d'énoncer que son groupe est de degré i et est formé par les permutations que subissent ses racines si l'on applique dans leurs expressions toutes les N permutations du groupe de la résolvante totale qui a engendré le corps.

On peut donc résumer les résultats trouvés en analysant la structure d'un corps dans l'énoncé suivant :

Toutes les grandeurs du corps de degré N *d'une équation satisfont à des résolvantes totales ou partielles dont le degré est* N *ou un diviseur de* N. *Les résolvantes de degré* N *sont totales et normales.*

L'équation algébrique considérée n'est qu'un anneau d'une chaîne d'équations qui sont les résolvantes de son corps et entre lesquelles se trouve établi le plus intime lien, traduit dans la liaison de leurs groupes : si l'on connaît les racines d'une résolvante totale, les racines de toutes les autres s'en déduisent rationnellement et les groupes de Galois des autres équations sont formés par les permutations subies par leurs racines, si l'on applique dans leurs expressions rationnelles les permutations du groupe de Galois de l'équation connue. Les groupes des résolvantes totales sont, en particulier, isomorphes.

9. La connaissance des racines d'une résolvante partielle ne résout pas complètement le problème de la résolution de l'équation primitive, parce qu'elle fait connaître seulement un sous-corps au lieu du corps tout entier. Mais, dans ce cas, on a du moins une simplification du problème. En effet, l'ensemble des quantités connues sera, à présent, le sous-corps $D(\varphi_1, \varphi_2, \ldots, \varphi_r)$, et le groupe de l'équation se réduit au sous-groupe I, puisque ses permutations, et elles seulement laissent invariables les quantités connues; le groupe I sera donc le groupe de Galois par rapport au nouveau domaine connu $D(\varphi_1, \varphi_2, \ldots, \varphi_r)$; si ν désigne le nombre des permutations que contient I, le nouveau corps sera donc seulement de degré ν et ses résolvantes de Galois, en particulier, des équations normales de degré $\nu < N$.

10. La présence d'une résolvante partielle dans le cycle des résolvantes d'un corps réduit son étude à celle de deux corps de degré moindre i et ν ($N = i\nu$). Il est donc utile de savoir quand cette circonstance se présente. Observons pour cela (nous conservons toujours les notations du n° 7) que les sous-groupes conjugués de I sont tous identiques à I, puisque les autres valeurs conjuguées de la fonction u du groupe I sont des fonctions rationnelles de u, u étant un élément primitif du sous-corps.

Réciproquement, supposons que le groupe Q ait un sous-groupe invariant d'indice i; une fonction u appartenant à ce sous-groupe satisfait à une équation irré-

ductible de degré i, dont les racines appartiennent au même groupe, puisque I coïncide avec les groupes conjugués. Donc, d'après le théorème de Lagrange elles peuvent toutes s'exprimer rationnellement en fonction de l'une d'entre elles, ce qui nous prouve que l'équation est normale et que, par conséquent, le corps a un sous-corps de degré i.

Donc, *la condition nécessaire et suffisante qu'un corps ait un sous-corps, c'est que son groupe admette un sous-groupe invariant.*

Il est clair que dans ce cas toutes les résolvantes de ce sous-corps seront naturellement des résolvantes partielles du corps.

LE THÉORÈME DE KRONECKER.

11. La résolution d'une équation et la réduction de son groupe de Galois à la substitution identique sont deux problèmes équivalents. En effet, si les racines de l'équation sont connues, son groupe de Galois se compose de la substitution identique qui, elle seule, laisse inaltérées les valeurs de toutes les racines; réciproquement, si le groupe de Galois d'une équation se compose de la seule substitution identique, toutes les grandeurs du corps et, en particulier, les racines de l'équation satisfont à des équations du premier degré par rapport au domaine connu et sont dès lors aussi connues.

On a été ainsi conduit à chercher quels sont les moyens généraux de réduction du groupe de Galois d'une équation, c'est-à-dire quelle est l'équation la plus générale dont la connaissance des racines nous donne une réduction du groupe d'une équation donnée. Le théorème de Kronecker répond complètement à cette question et nous apprend que ce sont *seulement les équations dont les corps ont avec le corps de l'équation considérée un sous-corps commun.*

La démonstration de ce théorème est immédiate. Soient, comme toujours, $F(x) = 0$ l'équation donnée et $\psi(y) = 0$ l'équation dont les racines soient considérées comme connues; nous supposons donc connu le corps de cette dernière équation. Cela posé, il peut arriver deux cas : les corps des équations $F(x) = 0$ et $\psi(y) = 0$ peuvent n'avoir aucun élément commun ou bien il existe des éléments communs. Dans le premier cas, le groupe de l'équation $F(x) = 0$ reste le même. En effet, supposons qu'il ait été réduit à l'un de ses sous-groupes. Une fonction de ce sous-groupe, admettant les permutations du nouveau groupe de Galois, serait une fonction connue, dès lors un élément du corps de $\psi(y)$, ce qui est contre l'hypothèse. Si donc le groupe a été réduit, les deux corps doivent avoir des éléments communs. Mais dans ce cas, considérons un de ces éléments communs; ses valeurs conjuguées, obtenues en considérant l'élément commun, comme faisant

partie séparément des deux corps, sont aussi des éléments communs parce qu'elles sont uniques; cela prouve simplement que l'ensemble des éléments communs forme un sous-corps dans chacun des deux corps considérés. C. Q. F. D.

L'ensemble des éléments communs peut coïncider avec le corps de l'équation $F(x) = 0$ lui-même; dans ce cas l'équation est complètement résolue, la réduction du groupe est complète : si, par exemple, le corps de $F(x) = 0$ est *simple,* c'est-à-dire n'a pas de sous-corps, toute réduction n'est possible que de cette manière. Mais si l'ensemble des éléments communs forme réellement un sous-corps, il est clair que le groupe de Galois de l'équation $F(x) = 0$ se réduit au sous-groupe permis par les éléments de ce sous-corps.

Nous avons ainsi prouvé, et c'est une remarque importante, qu'il n'existe pas d'autre manière de réduction d'un groupe que celle obtenue par la connaissance des racines d'une résolvante; cela tient à ce que la connaissance d'un sous-corps ou celle des racines d'une résolvante sont deux données évidemment identiques.

Remarquons enfin qu'on peut énoncer le théorème de Kronecker sous la forme suivante :

La connaissance des racines d'une équation ne réduit le groupe de Galois d'une autre que si les cycles dont elles font partie ont des éléments communs; dans ce cas, elle équivaut à la connaissance de ces éléments communs.