DÉMONSTRATION DU THÉORÈME FONDAMENTAL DE GALOIS DANS LA THÉORIE DE LA RÉSOLUTION ALGÉBRIQUE DES ÉQUATIONS

PAR

J. T. SÖDERBERG

À UPSALA.

1. Dans les quelques pages suivantes je me propose de présenter une démonstration nouvelle et très simple de l'important théorème de GALOIS sur l'existence du groupe de substitutions appelé *groupe d'une équation algébrique.* Elle a été publiée en suédois dans ma thèse inaugurale *Deduktion af nödvändiga och tillräckliga vilkoret för möjligheten af algebraiska eqvationers solution med radikaler,* Upsala Universitets Årsskrift, 1886. Je la présente ici avec de légères modifications.

2. Avant d'en commencer l'exposition nous aurons à nous expliquer sur le sens particulier que nous attribuerons à certaines expressions. Nous conviendrons de regarder, avec GALOIS, comme *rationnelle* toute quantité qui peut s'exprimer par une fonction rationnelle aux coefficients commensurables à l'unité de certaines quantités données à priori et que nous regarderons comme *connues.* Pour qu'une *fonction* soit appelée *rationnelle* nous entendrons que tous les coefficients en soient rationnelles.

Si une fonction rationnelle des quantités

$$x_0 , x_1 , \ldots , x_{n-1}$$

reste invariable par les substitutions d'un certain groupe, même en sup-

posant $x_0, x_1, \ldots, x_{n-1}$ des variables indépendantes, nous dirons que la *forme* de la fonction reste invariable par ces substitutions. Et nous distinguerons soigneusement ce cas de l'autre, où,

$$x_0, x_1, \ldots, x_{n-1}$$

étant les racines d'une équation donnée

$$x^n + p_1 x^{n-1} + p_2 x^{n-2} + \ldots + p_{n-1} x + p_n = 0$$

à coefficients rationnels, ce n'est que la *valeur* de la fonction qui reste invariable par certaines substitutions.

3. En partant des propositions établies par LAGRANGE dans son célèbre Mémoire *Réflexions sur la résolution algébrique des équations,* Section IV, il est facile d'établir le théorème suivant:

Si y et V sont deux fonctions rationnelles des racines $x_0, x_1, \ldots, x_{n-1}$ d'une équation algébrique donnée, et que la valeur de y reste invariable par toutes les substitutions qui ne changent pas la valeur de V, la fonction y peut s'exprimer en fonction rationnelle de V.

En effet, LAGRANGE a démontré la proposition suivante:

Si z et V sont deux fonctions rationnelles des racines $x_0, x_1, \ldots, x_{n-1}$ d'une équation algébrique, si $1, s_1, \ldots, s_{k-1}$ sont les substitutions qui ne changent pas la forme de la fonction V, si les mêmes substitutions laissent aussi invariable la forme de la fonction z, si enfin $1, \sigma_1, \ldots, \sigma_{i-1}$ sont des substitutions tellement choisies que le tableau

$$\begin{array}{llll} 1, & s_1, & s_2, & \ldots, s_{k-1}, \\ \sigma_1, & s_1\sigma_1, & s_2\sigma_1, & \ldots, s_{k-1}\sigma_1, \\ \sigma_2, & s_1\sigma_2, & s_2\sigma_2, & \ldots, s_{k-1}\sigma_2, \\ \ldots & \ldots & \ldots & \ldots \\ \sigma_{i-1}, & s_1\sigma_{i-1}, & s_2\sigma_{i-1} & \ldots, s_{k-1}\sigma_{i-1} \end{array}$$

donne toutes les substitutions différentes qui ne changent pas la valeur de V,

la moyenne arithmétique des fonctions qui résultent de z en faisant les substitutions $1, \sigma_1, \ldots, \sigma_{i-1}$, *sera exprimable en fonction rationnelle de V.*

Or, il est facile de s'assurer que notre proposition est une conséquence immédiate de celle de LAGRANGE. D'abord, la moyenne arithmétique des fonctions qu'on obtient de y par les substitutions $1, s_1, \ldots, s_{k-1}$, est une fonction nouvelle z, dont la forme reste invariable par ces substitutions. De plus, si l'on forme la moyenne arithmétique des fonctions résultant de z par les substitutions $1, \sigma_1, \ldots, \sigma_{i-1}$, on aura le même résultat qu'en prenant la moyenne arithmétique de toutes les fonctions qui s'obtiennent de y en faisant les substitutions du tableau ci-dessus. Mais il suit de notre hypothèse que toutes ces fonctions, et par conséquent leur moyenne arithmétique, sont égales à y. Donc, en appliquant à la fonction z le théorème de LAGRANGE, on voit que y s'exprime en fonction rationnelle de V.

c. q. f. d.

4. Supposons que

$$V_0, V_1, \ldots, V_{i-1}$$

soient toutes les formes différentes dont la valeur est égale à la valeur donnée V_0 qu'on puisse faire acquérir à la fonction V en faisant toutes les substitutions possibles. Considérons toutes les substitutions dont l'effet est de remplacer le système des formes

$$V_0, V_1, \ldots, V_{i-1}$$

par un autre qui ne contient pas de forme nouvelle; il est évident que ces substitutions forment un groupe. Nous dirons que ce groupe appartient à la valeur V_0 de la fonction V. Les substitutions de ce groupe sont, par conséquent, celles qui laissent invariable la valeur de chacune des fonctions

$$V_0, V_1, \ldots, V_{i-1}.$$

Il est facile maintenant de modifier la proposition citée plus haut de la manière suivante:

Si y est une fonction rationnelle des racines $x_0, x_1, \ldots, x_{n-1}$ *dont la valeur n'est pas changée par les substitutions du groupe appartenant à une*

valeur donnée de la fonction V, on peut exprimer y en fonction rationnelle de V.

En effet, on peut choisir les quantités rationnelles

$$k_0, k_1, \ldots, k_{i-1}$$

de manière que la valeur de la fonction

$$Q = k_0 V_0 + k_1 V_1 + \ldots + k_{i-1} V_{i-1}$$

ne reste invariable que par les substitutions qui laissent invariable la valeur de chacune des fonctions $V_0, V_1, \ldots, V_{i-1}$. Donc y est fonction rationnelle de Q et, par conséquent, de V, puisque toutes les fonctions $V_0, V_1, \ldots, V_{i-1}$ ont la même valeur V.

5. Avant d'aborder la démonstration du théorème fondamental de GALOIS, nous établirons encore le point suivant. Admettons que U et V soient les valeurs données de deux fonctions rationnelles des racines $x_0, x_1, \ldots, x_{n-1}$ Il est facile alors de former une autre fonction rationnelle R des mêmes racines, telle que le groupe appartenant à une valeur donnée de R soit formé par les substitutions communes aux deux groupes qui appartiennent aux valeurs données des deux fonctions U et V. En effet, supposons que

$$U_0, U_1, \ldots, U_{i-1}$$

soient les différentes formes de la première fonction dont la valeur est U, et que

$$V_0, V_1, \ldots, V_{j-1}$$

aient une signification analogue pour la fonction V. Considérons une fonction rationnelle de la forme

$$R = h_0 U_0 + h_1 U_1 + \ldots + h_{i-1} U_{i-1} + k_0 V_0 + k_1 V_1 + \ldots + k_{j-1} V_{j-1},$$

où nous supposerons que les coefficients h et k soient des quantités rationnelles. Toutes les formes diverses que peut acquérir la fonction R par les substitutions, seront représentées par la formule

$$h_0 U_{\alpha_0} + h_1 U_{\alpha_1} + \ldots + h_{i-1} U_{\alpha_{i-1}} + k_0 V_{\beta_0} + k_1 V_{\beta_1} + \ldots + k_{j-1} V_{\beta_{j-1}},$$

où $U_{\alpha_0} \dots U_{\alpha_{i-1}}$ et $V_{\beta_0} \dots V_{\beta_{j-1}}$ sont des formes quelconques que peuvent acquérir les fonctions U et V par les substitutions. Il est clair que nous pouvons choisir les coefficients h et k, de manière que la valeur de chacune de ces formes soit différente de la valeur donnée, à moins que toutes les fonctions $U_{\alpha_0} \dots U_{\alpha_{i-1}}$ n'aient la valeur U et les fonctions $V_{\beta_0} \dots V_{\beta_{i-1}}$ la valeur V.

Mais alors R est une fonction comme celle dont nous avons annoncé l'existence. Les fonctions $U_{\alpha_0} \dots U_{\alpha_{i-1}}$ ayant toutes la valeur U, et les fonctions $V_{\beta_0} \dots V_{\beta_{i-1}}$ la valeur V, on a

$$R = (h_0 + \dots + h_{i-1})\,U + (k_0 + \dots + k_{j-1})\,V.$$

6. Il est facile à présent d'établir le théorème de Galois, dont voici l'énoncé:

Si une équation algébrique n'a pas de racines égales, il y a toujours un groupe de substitutions — et il n'y en a qu'un — qui jouit de la double propriété suivante:

1° *toute fonction rationnelle des racines dont la valeur est rationnelle, reste invariable par les substitutions du groupe;*

2° *réciproquement, toute fonction rationnelle des racines dont la valeur n'est pas changée par les substitutions du groupe, s'exprime rationnellement par les quantités connues.*

Ce groupe a été appelé par Galois *le groupe de l'équation*.

Considérons l'ensemble des groupes qui appartiennent à des valeurs données des fonctions rationnelles de $x_0, x_1, \dots, x_{n-1}$ exprimables rationnellement par les quantités connues. Parmi ces groupes, il y en aura un dont l'ordre est moindre ou égal à celui de tout autre groupe. Soit G ce groupe; je dis qu'il jouit de la double propriété dont il s'agit.

En effet, soient Γ un quelconque des groupes considérés, I le groupe des substitutions communes à G et à Γ, ω et Ω les fonctions rationnelles des racines auxquelles correspondent les groupes G et Γ; il y aura (n° 5) une fonction rationnelle des racines, dont le groupe appartenant à une valeur donnée sera précisément I. De plus, cette fonction s'exprimant en fonction rationnelle et linéaire de ω et Ω, il faut que sa valeur soit rationnelle. L'ordre de I ne peut donc être inférieur à celui de G,

d'où il suit que ces deux groupes sont identiques, et que, par conséquent, les substitutions de G font toutes partie du groupe Γ.

La première partie du théorème de GALOIS se trouve donc établie.

La démonstration de la seconde partie est immédiate. En effet (n° 4) toute fonction rationnelle des racines dont la valeur reste invariable par les substitutions de G, s'exprime rationnellement par ω et, en conséquence, par les quantités connues.

Il ne nous reste plus qu'à démontrer que le groupe d'une équation est unique. S'il n'en était pas ainsi, soit H un autre groupe jouissant comme G des propriétés du groupe de l'équation. Comme au n° 4, nous pouvons former une fonction rationnelle ω_1 dont la valeur reste invariable par les substitutions de G, mais est changée par toute autre substitution. Cette fonction s'exprimant rationnellement par les quantités connues, sa valeur reste invariable par les substitutions du groupe H, qui par conséquent est contenu dans G.

Mais d'un autre côté, les racines étant inégales, nous pouvons aussi, par un procédé bien connu (voir p. ex. JORDAN, *Traité des substitutions*, pag. 255), trouver une fonction rationnelle ω_2 dont non seulement la valeur, mais la forme même reste invariable par les substitutions de H et dont la valeur est changée par toute autre substitution. Par suite de notre hypothèse cette fonction est une quantité rationnelle et par conséquent il faut que sa valeur soit invariable par les substitutions de G. Ces substitutions appartiennent donc aussi au groupe H, et par conséquent les groupes G et H sont identiques, ce qui achève la démonstration du théorème de GALOIS.