I.

2108

Mémoire sur les
Conditions de résolubilité des équations par radicaux.
(Œuvres, p. 33)
(Texte autographe du Mémoire présenté à l'Académie)

Le renvoi aux "Œuvres" de Galois a été ajouté par l'Éditeur du "Nouveau manuscrit" de Evariste Galois publié par la Société Mathématique Gauthier-Villars 1907.
Le renvoi aprés (M.) a été ajouté par l'auteur du "Manuscrit de Evariste Galois" Gauthier-Villars 1908.
J. L.

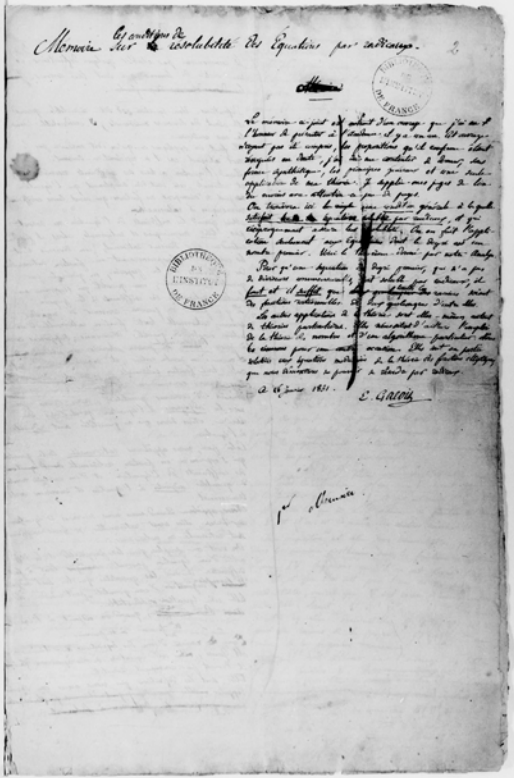
II.

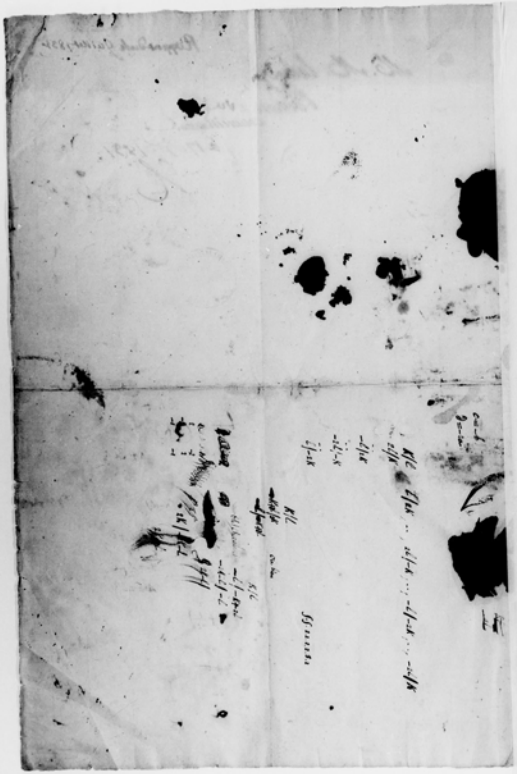
Rapport du 6 juillet 1832.

1

M. M. Lacroix
Poisson vu
communiqué
le 17. juin 1831.

Mémoire sur l'établissement des Equations par différences. 2.





Mémoire sur les conditions de résolubilité des Equations par radicaux. 2

~~Théorie~~

Le mémoire ci-joint est extrait d'un ouvrage que j'ai eu l'honneur de présenter à l'Académie, il y a un an. Cet ouvrage n'ayant pas été compris, les propositions qu'il renferme étant énoncées en texte, j'ai cru devoir donner des formes synthétiques, les principes généraux et une seule application de ma théorie. Je supplie mes juges de lire mes vues avec attention en peu de pages.

On trouvera ici les conditions générales à laquelle satisfait ~~les~~ les équations solubles par radicaux, et qui n'appartiennent aux seules solubles. On en fait l'application seulement aux équations dont le degré est un nombre premier. Mais la théorie donnée par notre Analyse

Pour qu'une équation de degré premier, qui n'a pas de diviseurs commensurables, soit soluble par radicaux, il faut et il suffit que toutes les racines soient des fonctions rationnelles de deux quelconques d'entre elles.

Les autres applications de la théorie sont des mêmes subst de théories particulières. Elles résultent d'ailleurs l'emploi de la théorie des nombres et d'une algorithme particulier dont les éléments pour une autre occasion. Elles ont en particulier les équations solubles de la classe des fonctions elliptiques qui nous donnerons le moyen de traiter par calcul.

A 16 juin 1831.

E. GALOIS

pour Mémoire.

1

Principes.

Je commencerai par établir quelques définitions et une suite de lemmes qui sont tous connus. ~~[illegible]~~

Définitions. Une équation est dite réductible quand elle admet des diviseurs rationnels; irréductible dans le cas contraire.

Il faut ici expliquer ce qu'on doit entendre par le mot rationnel: car il se reproduira 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 de l'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.

Il y a plus: on pourra convenir de regarder comme rationnelle toute fonction rationnelle d'un certain nombre de quantités déterminées, supposées connues à 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 fonction rationnelle des coefficients de l'équation et d'un certain nombre de quantités adjointes à l'équation et convenues arbitrairement.

Quand nous nous servirons d'équations auxiliaires, elles seront rationnelles, si leurs coefficients sont rationnels en notre sens.

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.

Ainsi, quand on adjoint à l'équation

$$\frac{x^n-1}{x-1}=0 \quad n \text{ premier}$$

une racine d'une des équations auxiliaires de M. Gauss, cette équation se décompose en facteurs, et devient par conséquent réductible.

Telles sont les définitions que nous avons cru devoir rappeler ~~[illegible]~~.

M. Lacroix

La démonstration de ce lemme n'est pas suffisante; mais il est vrai d'après le n°. 100 du mémoire de Lagrange, Berlin, 1771.

* Nous avons transcrit textuellement la démonstration que nous avons donnée de ce lemme dans un mémoire présenté en 1830. Nous y joignons comme document historique la note suivante qu'a cru devoir y apposer M. Poisson.

On jugera.

Note de l'auteur

** Il est remarquable que de cette proposition on peut conclure que toute équation dépend d'une équation auxiliaire telle que toutes les racines de cette nouvelle équation soient des fonctions rationnelles les unes des autres. Car l'équation auxiliaire en V est dans ce cas.

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

~~[illegible]~~ En effet en multipliant entre elles toutes les fonctions de la forme $V-\varphi(a,b,c,\ldots)$ [illegible]

2

Lemme I. 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 et l'autre équation sera encore rationnel; donc, etc.

Lemme II. Étant donnée une équation quelconque, qui n'a pas de racines égales, dont les racines sont $a, b, c, \ldots$ 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

$$V = Aa + Bb + Cc + \ldots$$

$A, B, C, \ldots$ étant des nombres entiers convenablement choisis.

Lemme III. 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 proposée s'exprimeront rationnellement en fonction de V.

En effet, soit $V=\varphi(a,b,c,d,\ldots)$ ou bien

$$V-\varphi(a,b,c,d,\ldots)=0$$

Multiplions entre elles toutes les équations semblables que l'on obtient en permutant dans celle-ci toutes les lettres, la première seulement restant fixe; [illegible] $(V-\varphi(a,b,c,d,\ldots))(V-\varphi(a,c,b,d,\ldots))\ldots$ [illegible] symétrique en $b, c, d, \ldots$ laquelle pourra par conséquent s'écrire en fonction de a. Nous aurons donc une équation de la forme

$$F(V,a)=0$$

Or je dis que de là on peut tirer la valeur de a. Il suffit pour cela de chercher la solution commune à cette équation et à la proposée. Cette solution est la seule commune, car on ne peut avoir, par exemple,

$$F(V,b)=0$$

sans que la fonction $\varphi(a,\ldots)$ soit égale à la fonction $\varphi(b,\ldots)$. Ce qui est contre l'hypothèse.

Il suit de là que a s'exprime en fonction rationnelle de V, et il en est de même des autres racines.

Cette proposition** est citée sans démonstration par Abel dans le mémoire posthume sur les fonctions elliptiques.

Lemme IV. 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 $V, V', V'', \ldots$ les racines de cette équation irréductible. Je dis que si $a=f(V)$ est une des racines de la proposée, $f(V')$ sera de même une racine de la proposée.

En effet V′ doit s'obtenir par l'échange des lettres dans la fonction V. [illegible] $F(V',a)=0$ [illegible]

[illegible] $F(V',a)=0$ [illegible]

[illegible] $F(V',a)=0$ [illegible] $f(V')$

1

Principes.

Je commencerai par établir quelques définitions et une suite de lemmes qui sont tous connus. ~~[illegible]~~

Définitions. Une équation est dite réductible quand elle admet des diviseurs rationnels; irréductible dans le cas contraire.

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

Il y a plus: on pourra convenir de regarder comme rationnelle toute fonction rationnelle d'un certain nombre de quantités déterminées, supposées connues à 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 fonction rationnelle des coefficients de l'équation et d'un certain nombre de quantités adjointes à l'équation et convenues arbitrairement.

~~Nous appelons~~ Quand nous nous servirons d'équations auxiliaires, elles seront rationnelles, si leurs coefficients sont rationnels en notre sens.

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.

~~Ainsi~~ Par exemple, quand on adjoint à l'équation

$$\frac{x^n-1}{x-1}=0 \quad \text{où } n \text{ premier}$$

une racine d'une des équations auxiliaires de M. Gauss, cette équation se décompose en facteurs et devient par conséquent réductible.

Telles sont les définitions que nous avons cru devoir rappeler ~~[illegible]~~

M. Poinsot [illegible]

Lemme I. Une équation irréductible ne peut avoir aucune racine commune avec une ~~autre~~ équation rationnelle sans la diviser.

Car le plus grand commun diviseur entre l'équation irréductible et l'autre équation sera encore rationnel; donc, etc.

Lemme II. Étant donnée une équation quelconque, qui n'a pas de racines égales, dont les racines sont $a, b, c, \ldots$ 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

$$V = Aa + Bb + Cc + \ldots$$

$A, B, C, \ldots$ étant des nombres entiers convenablement choisis.

Lemme III. 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 proposée s'exprimeront rationnellement en fonction de V.

En effet, soit $V = \varphi(a, b, c, d, \ldots)$ ou bien

$$V - \varphi(a, b, c, d, \ldots) = 0$$

Multiplions entre elles toutes les équations semblables que l'on obtient en permutant dans celles-ci toutes les lettres, la première seulement restant fixe; il viendra ~~[illegible]~~ expression symétrique en $b, c, d, \ldots$, laquelle pourra par conséquent s'écrire en fonction de a; on aura donc une équation de la forme

$$F(V, a) = 0$$

Or je dis que de là on peut tirer la valeur de a. Il suffit pour cela de chercher la solution commune à cette équation et à la proposée. Cette solution est la seule commune car on ne peut avoir, par exemple,

$$F(V, b) = 0$$

sans que l'une des fonctions $\varphi(a, \ldots)$ soit égale à l'une des fonctions $\varphi(b, \ldots)$, ce qui est contre l'hypothèse.

Il suit de là que a s'exprime en fonction rationnelle de V, et il en est de même des autres racines.

Cette proposition* est citée sans démonstration, par Abel dans le mémoire posthume sur les fonctions elliptiques.

Lemme IV. 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 $V\ V'\ V'' \ldots$ les racines de cette équation irréductible. Si $a = f(V)$ est une des racines de la proposée, $f(V')$ sera de même une racine de la proposée.

~~[illegible]~~ V' doit être obtenu par l'échange des lettres dans la fonction V. ~~[illegible]~~ $F(V', a) = 0$ ~~[illegible]~~

[illegible] $F(V', a) = 0$ [illegible]

[illegible]

Cette démonstration [illegible] insuffisante [illegible] le n° 100 du mémoire de Lagrange, Berlin, 1771.

* Voici un travail fait spécialement [illegible] que nous avons donnée de ce lemme dans un mémoire présenté en 1830. Nous y joignons comme document historique la note qu'a cru devoir y apposer M. Poisson.

On jugera.

Note de l'auteur.

* N. B. Il est remarquable que de cette proposition on peut conclure que toute équation ~~peut aussi~~ dépend d'une équation auxiliaire telle que toutes les racines de cette nouvelle équation soient des fonctions rationnelles les unes des autres. Car l'équation auxiliaire en V est dans ce cas.

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

En effet en multipliant entre elles toutes les ~~équations~~ facteurs de la forme $V - \varphi(a, b, c, \ldots)$ [illegible]

[illegible]

Proposition I.

Théorème. Soit une équation donnée dont $a, b, c, \ldots$ sont les racines. On pourra toujours assigner un groupe de permutations des lettres $a, b, c, \ldots$ qui jouira de la propriété suivante :

1° Toute fonction des racines invariable par les substitutions de ce groupe sera nécessairement rationnelle.

2° Réciproquement, toute fonction des racines rationnelle et tellement exprimée sera invariable par les permutations de ce groupe.

(Dans le cas des équations abéliennes, ce groupe n'est autre chose que l'ensemble des $1.2.3\ldots n$ permutations possibles sur les n lettres, puisque dans ce cas la fonction symétrique répond seule à la détermination rationnelle.)

(Dans le cas de l'équation $x^n = a$, si l'on suppose $x = r,\ \alpha r,\ \alpha^2 r,\ \ldots\ \alpha^{n-1} r$, α étant une racine primitive, le groupe de permutations sera exprimé tout simplement par

$$\begin{matrix} a & b & c & \ldots & K \\ b & c & d & \ldots & Ka \\ c & d & \ldots & Ka & b \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ K & a & b & \ldots & \cdot \end{matrix}$$

Dans un cas particulier, quelconque la somme de p permutations est égale au degré de l'équation, et la même chose arrivant lors même que l'on ajoute à toutes les racines certaines fonctions rationnelles de toutes les autres.)

Démonstration. Soit V une fonction rationnelle des racines $a, b, c, \ldots$ qui ne change pas par les substitutions du groupe G de la proposition. Désignons par $V', V'', V''', \ldots$ les fonctions semblables formées avec les racines $b, c, d, \ldots$; $V'', V''', \ldots$ les fonctions semblables formées avec les racines $c, d, \ldots$; etc.

Considérons maintenant l'équation qui est l'équation résolvante pour trouver toutes les fonctions rationnelles de V. Cette équation admettra V pour racine, puisque V est une fonction rationnelle des racines. Soient $V, V', V'', \ldots$ les racines de cette équation.

Désignons par $p_1, p_2, p_3, \ldots$ les permutations du groupe G de la proposition.

Considérons les n permutations suivantes des racines

$$\begin{matrix} p_1 V & p_2 V & p_3 V & \ldots & p_{n-1} V \\ p_1 V' & p_2 V' & p_3 V' & \ldots & p_{n-1} V' \\ p_1 V'' & p_2 V'' & p_3 V'' & \ldots & p_{n-1} V'' \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ p_1 V^{(n-1)} & p_2 V^{(n-1)} & p_3 V^{(n-1)} & \ldots & p_{n-1} V^{(n-1)} \end{matrix}$$

Je dis que ces n permutations sont toutes différentes. En effet, si l'équation $p_\alpha V = p_\beta V$ avait lieu, on aurait aussi $p_\alpha V' = p_\beta V'$, $p_\alpha V'' = p_\beta V''$, etc., et l'on aurait $p_\alpha = p_\beta$, ce qui est contre l'hypothèse.

Ces n permutations forment un groupe G' dont G est un diviseur. En effet, si p_α et p_β sont deux permutations du groupe G, $p_\alpha V$ et $p_\beta V$ sont deux des racines de l'équation résolvante, et $p_\alpha p_\beta V$ est aussi une racine de cette équation, puisque $p_\alpha p_\beta$ est une permutation du groupe G. Donc $p_\alpha p_\beta V$ est égal à l'une des racines $V, V', V'', \ldots$; donc $p_\alpha p_\beta$ est une des permutations $p_1, p_2, p_3, \ldots$; donc le groupe G' contient le produit de deux quelconques de ses permutations.

Soient maintenant $p_1, p_2, p_3, \ldots$ les permutations du groupe G qui ne changent pas V, et p_α une autre permutation du même groupe. Les permutations

$$p_\alpha V,\ p_1 p_\alpha V,\ p_2 p_\alpha V,\ p_3 p_\alpha V,\ \ldots$$

sont toutes différentes, car si l'on avait $p_\alpha V = p_\beta V$, on aurait $p_\alpha = p_\beta$, ce qui est contre l'hypothèse. Ces permutations sont donc les mêmes que les permutations

$$V,\ p_1 V,\ p_2 V,\ p_3 V,\ \ldots$$

seulement elles sont disposées dans un autre ordre. Donc

$$V + p_1 V + p_2 V + p_3 V + \ldots = p_\alpha V + p_1 p_\alpha V + p_2 p_\alpha V + p_3 p_\alpha V + \ldots$$

Donc V est une fonction rationnelle des racines, puisque l'équation dont V est racine admet une racine rationnellement connue, à savoir V lui-même. Donc V est une fonction rationnelle des racines invariable par les substitutions du groupe G.

Réciproquement, toute fonction rationnelle des racines, invariable par les substitutions du groupe G, est évidemment une racine de l'équation résolvante. Or, cette équation n'ayant que des racines rationnellement connues, il est clair que toute fonction rationnelle des racines est rationnellement connue.

Corollaire. Si l'équation donnée est irréductible, les racines $V, V', V'', \ldots$ de l'équation résolvante sont toutes différentes. En effet, si $V = V'$, V reste inaltéré par les substitutions du groupe G, et par conséquent est rationnellement connu. Donc V est une fonction rationnelle des racines invariable par les substitutions du groupe G', dont G est un diviseur. Donc l'équation résolvante admet une racine rationnellement connue, ce qui est contre l'hypothèse.

Si $V = V'$, on a aussi $V = V''$, $V = V'''$, etc. Donc V est une fonction rationnelle des racines invariable par les substitutions du groupe G, dont G est un diviseur. Donc l'équation résolvante admet une racine rationnellement connue, ce qui est contre l'hypothèse.

Si $V = V'$, on a aussi $V = V''$, $V = V'''$, etc. Donc V est une fonction rationnelle des racines invariable par les substitutions du groupe G', dont G est un diviseur. Donc l'équation résolvante admet une racine rationnellement connue, ce qui est contre l'hypothèse.

Proposition II.

Théorème. Si l'on adjoint à une équation de degré n d'une équation auxiliaire irréductible dont le degré m est un diviseur de n, les n racines de l'équation ne vont pas changer, on bien il se partagera en p groupes appartenant à l'équation proposée, exactement quand on la suppose réduite au moyen de l'équation auxiliaire, et ces groupes jouiront de la propriété remarquable, que l'on passera de l'un à tous les autres en faisant subir à toutes les permutations de chacun d'eux une même substitution de n lettres.

Si, de sorte l'équation $V = 0$, l'équation en V était elle-même irréductible, il est clair que le groupe de l'équation en x ne pourrait changer. Si au contraire elle a un diviseur, alors l'équation en V se décomposera en facteurs de même degré p. Si la fonction

$$f(V, V') \times f(V, V') \times f(V, V'') \times \ldots$$

$V, V', V'', \ldots$ étant les racines de l'équation en V, est invariable par les substitutions du groupe de l'équation en x, cette équation jouira de la propriété énoncée au n° 2 du groupe donné d'un même nombre de permutations, puisque chaque valeur de V correspond à p permutations. Si, au contraire, cette fonction change de valeur, elle prendra p valeurs différentes, puisque l'équation en V est supposée réduite au moyen de l'équation auxiliaire. Soient $V, V', V'', \ldots$ ces p valeurs différentes. Si l'on désigne par $p_1, p_2, p_3, \ldots$ les permutations du groupe de l'équation en x, on aura

$$\begin{matrix} p_1 V & p_2 V & p_3 V & \ldots & p_{n-1} V \\ p_1 V' & p_2 V' & p_3 V' & \ldots & p_{n-1} V' \\ p_1 V'' & p_2 V'' & p_3 V'' & \ldots & p_{n-1} V'' \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ p_1 V^{(p-1)} & p_2 V^{(p-1)} & p_3 V^{(p-1)} & \ldots & p_{n-1} V^{(p-1)} \end{matrix}$$

Ces n permutations forment un groupe G' dont le groupe G de la proposition est un diviseur. Soient $p_1, p_2, p_3, \ldots$ les permutations du groupe G qui ne changent pas V, et p_α une autre permutation du même groupe. Les permutations

$$p_\alpha V,\ p_1 p_\alpha V,\ p_2 p_\alpha V,\ p_3 p_\alpha V,\ \ldots$$

sont toutes différentes, car si l'on avait $p_\alpha V = p_\beta V$, on aurait $p_\alpha = p_\beta$, ce qui est contre l'hypothèse. Ces permutations sont donc les mêmes que les permutations

$$V,\ p_1 V,\ p_2 V,\ p_3 V,\ \ldots$$

seulement elles sont disposées dans un autre ordre. Donc

$$V + p_1 V + p_2 V + p_3 V + \ldots = p_\alpha V + p_1 p_\alpha V + p_2 p_\alpha V + p_3 p_\alpha V + \ldots$$

Donc V est une fonction rationnelle des racines, puisque l'équation dont V est racine admet une racine rationnellement connue, à savoir V lui-même. Donc V est une fonction rationnelle des racines invariable par les substitutions du groupe G', dont G est un diviseur. Donc l'équation résolvante admet une racine rationnellement connue, ce qui est contre l'hypothèse.

Si $V = V'$, on a aussi $V = V''$, $V = V'''$, etc. Donc V est une fonction rationnelle des racines invariable par les substitutions du groupe G', dont G est un diviseur. Donc l'équation résolvante admet une racine rationnellement connue, ce qui est contre l'hypothèse.

Nous appelons ici invariable non seulement une fonction dont la forme est invariable par les substitutions des racines entre elles, mais encore celle dont la valeur numérique ne varierait pas par ces substitutions. Par exemple, si $Fx = 0$ est une équation, Fx est une fonction des racines qui ne varie par aucune permutation.

Quand nous disons qu'une fonction est rationnellement connue, nous voulons dire que sa valeur numérique est exprimable en fonction rationnelle des coefficients de l'équation et des quantités adjointes.

A ajouter dans les définitions

~~Cette partie ...~~

Les substitutions sont le passage d'une permutation à l'autre.

La permutation dont on part pour indiquer les substitutions est tout 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 on ne peut guère se former l'idée d'une substitution sans ~~se former~~ 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.

Comme il s'agit toujours 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.

PROPOSITION I.

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

1° que toute fonction des racines invariable[*] par les substitutions de ce groupe soit rationnellement connue;

2° réciproquement, que toute fonction des racines déterminable rationnellement soit invariable par les substitutions.

(Dans le cas des équations algébriques, ce groupe n'est autre chose que l'ensemble des $1.2.3\ldots m$ permutations possibles sur les m lettres, puisque, dans ce cas, les fonctions symétriques sont seules déterminables rationnellement.)

(Dans le cas de l'équation $\frac{x^n-1}{x-1}=0$, si l'on suppose $a=r$, $b=r^g$, $c=r^{g^2}$, ..., g étant une racine primitive, le groupe de permutations sera simplement celui-ci

$a\ b\ c\ d \ldots k$

$b\ c\ d \ldots k\ a$

$c\ d \ldots k\ a\ b$

$\ldots$

$k\ a\ b\ c \ldots j$

dans ce cas particulier, le nombre des permutations est égal au degré de l'équation, et la même chose aurait lieu dans les équations dont toutes les racines seraient des fonctions rationnelles les unes des autres.)

Démonstration. Quelle que soit l'équation donnée, on pourra trouver une fonction rationnelle V des racines telle que toutes les racines soient fonctions rationnelles de V. Cela posé, considérons l'équation irréductible dont V est racine (Lemmes III et IV). Soient $V, V', V'', \ldots, V^{(n-1)}$ les racines de cette équation.

Soient $\varphi V,\ \varphi_1 V,\ \varphi_2 V, \ldots, \varphi_{m-1} V$ les racines de la proposée.

Écrivons les n permutations suivantes des racines

$(V)\quad \varphi V,\ \varphi_1 V,\ \varphi_2 V, \ldots, \varphi_{m-1} V$

$(V')\quad \varphi V',\ \varphi_1 V',\ \varphi_2 V', \ldots, \varphi_{m-1} V'$

$(V'')\quad \varphi V'',\ \varphi_1 V'',\ \varphi_2 V'', \ldots, \varphi_{m-1} V''$

$\ldots$

$(V^{(n-1)})\quad \varphi V^{(n-1)},\ \varphi_1 V^{(n-1)},\ \varphi_2 V^{(n-1)}, \ldots, \varphi_{m-1} V^{(n-1)}$

Je dis que ce groupe de permutations jouit de la propriété énoncée.

En effet, 1° toute fonction F des racines invariable par les substitutions de ce groupe pourra être écrite ainsi $F = \psi V$, et l'on aura

$$\psi V = \psi V' = \psi V'' = \ldots = \psi V^{(n-1)}$$

La valeur de F pourra donc se déterminer rationnellement.

2° Réciproquement, si une fonction F est déterminable rationnellement, et que l'on pose $F = \psi V$, on devra avoir

$$\psi V = \psi V' = \psi V'' = \ldots = \psi V^{(n-1)}$$

puisque l'équation en V n'a pas de diviseur commensurable, et que V satisfait à l'équation rationnelle $F = \psi V$, F étant une quantité rationnelle. Donc la fonction F sera nécessairement invariable par les substitutions du groupe écrit ci-dessus.

Ainsi ce groupe jouit de la double propriété dont il s'agit dans le théorème proposé. Le théorème est donc démontré.

Nous appellerons groupe de l'équation le groupe en question.

Scholie. Il est évident que dans le groupe de permutations dont il s'agit ici, la disposition des lettres n'est point à considérer, mais seulement les substitutions de lettres par lesquelles on passe d'une permutation à l'autre.

Ainsi l'on peut se donner arbitrairement une première permutation, pourvu que les autres permutations s'en déduisent toujours par les mêmes substitutions de lettres. Le nouveau groupe ainsi formé jouira évidemment des mêmes propriétés que le premier, puisque dans le théorème précédent, il ne s'agit que des substitutions que l'on peut faire dans les fonctions.

Ce qui caractérise un groupe. On peut partir d'une des permutations quelconques du groupe. Les substitutions sont indépendantes même du nombre des racines.

~~$S, T = U$~~

S_T

Il y a quelque chose à compléter dans cette démonstration. Je n'ai pas le temps. (Note de l'A.)

~~Car si l'on élimine r entre $f(V, r) = 0$ et $F(r) = 0$ ... il ne peut arriver que de deux choses l'une: ou le résultat de l'élimination sera du même degré en V que $f(V, r)$, ou il sera d'un degré plus grand.~~

PROPOSITION II.

Théorème. Si l'on adjoint à une équation donnée la racine r d'une équation auxiliaire irréductible, 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'équation auxiliaire; 2° ces groupes jouiront de la propriété remarquable, que l'on passera de l'un à l'autre en opérant dans toutes les permutations du premier une même substitution de lettres.

1° Si, après l'adjonction de r, l'équation en V dont il est question plus haut reste irréductible, il est clair que le groupe de l'équation ne sera pas changé. Si au contraire elle se réduit, alors l'équation en V se décomposera en p facteurs tous de même degré et de la forme

$$f(V, r) \times f(V, r') \times f(V, r'') \times \ldots$$

$r', r'', \ldots$ étant d'autres valeurs de r. Ainsi le groupe de l'équation proposée se décomposera aussi en ~~...~~ groupes chacun d'un même nombre de permutations, puisqu'à chaque valeur de V correspond une permutation. Ces groupes seront respectivement ceux de l'équation proposée, quand on lui adjoindra successivement $r, r', r'', \ldots$

PROPOSITION III.

PROPOSITION IV.

PROPOSITION V.

2° Nous avons vu plus haut que toutes les valeurs de V étaient des fonctions rationnelles les unes des autres. D'après cela, supposons que V étant une racine de $f(V, r) = 0$, $F(V)$ en soit une autre. Il est clair que de même si V' est une racine de $f(V, r') = 0$, $F(V')$ en sera une autre.*

Cela posé, je dis que l'on obtient le groupe relatif à r' en opérant partout dans le groupe relatif à r une même substitution de lettres.

En effet si l'on a par exemple $\varphi_\mu F(V) = \varphi_\nu V$ on aura encore, (Lemme I), $\varphi_\mu F(V') = \varphi_\nu V'$. Donc pour passer de la ~~...~~ permutation $(F(V))$ à la permutation $(F(V'))$, il faut faire la même substitution que pour passer de la ~~substitution~~ permutation (V) à la permutation (V').

Le théorème est donc démontré.

PROPOSITION III.

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

~~En effet, dans ce cas, il revient au même d'adjoindre à l'équation telle ou telle valeur de r. Par conséquent ses propriétés doivent être les mêmes après l'adjonction de telle ou telle valeur. Ainsi son groupe doit être le même quant aux substitutions. (Prop. I, scholie) Donc, &c.~~

PROPOSITION IV.

Théorème. Si l'on adjoint à une équation la valeur numérique d'une certaine fonction de ses racines, le groupe de l'équation s'abaissera de manière à n'avoir plus d'autres permutations que celles par lesquelles cette fonction est invariable.

En effet, d'après la proposition I, ~~...~~ toute fonction connue doit être invariable par les permutations du groupe de l'équation.

PROPOSITION V.

Problème. Dans quel cas une équation est-elle soluble par de simples radicaux ?

J'observerai d'abord que pour résoudre une équation, il faut successivement abaisser son groupe jusqu'à ne contenir plus qu'une seule permutation. Car, quand une équation est résolue, une fonction quelconque de ses racines est connue, même quand elle n'est invariable par aucune permutation.

Cela posé, cherchons à quelle condition doit satisfaire le groupe d'une équation, pour qu'il puisse s'abaisser ainsi par l'adjonction ~~...~~ de quantités radicales. 5

Suivons la marche des opérations possibles dans cette solution en considérant comme ~~...~~ opérations distinctes, l'extraction de chaque racine de degré premier.

Adjoignons à l'équation le premier radical extrait dans la solution ; il pourra arriver deux cas : ou bien par l'adjonction de ce radical, le groupe des permutations de l'équation sera diminué ; ou bien, cette extraction de racine n'étant qu'une simple préparation, le groupe restera le même.

Toujours sera-t-il qu'après un certain nombre fini d'extractions de racines, le groupe devra se trouver diminué, sans quoi l'équation ne serait pas soluble.

Si arrivé à ce point, il y avait plusieurs manières de diminuer le groupe de l'équation proposée par une simple extraction de racine, il faudrait, pour ce que nous allons dire, considérer seulement un radical du degré le moins haut possible parmi tous les simples radicaux qui sont tels que la connaissance de chacun d'eux diminue le groupe de l'équation.

Soit donc p le nombre premier qui représente ce degré minimum, en sorte que par une extraction de racine de degré p, on diminue le groupe de l'équation.

Nous pouvons toujours supposer, du moins pour ce qui est relatif au groupe de l'équation, que parmi les quantités adjointes précédemment à l'équation se trouve une racine $p$ième de l'unité α. Car comme cette expression s'obtient par des extractions de racines de degré inférieur à p, sa connaissance n'altérera en rien le groupe de l'équation.

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

Je dis réciproquement que si le groupe de l'équation peut se partager en p groupes qui jouissent de cette double propriété, on pourra, par une simple extraction de racine $p$ième et par l'adjonction de cette racine $p$ième, ~~...~~ réduire le groupe de l'équation à l'un de ces groupes partiels.

Prenons en effet une fonction des racines qui soit invariable pour toutes les substitutions de l'un des groupes partiels, et varie pour aucune autre substitution.*

Soit θ cette fonction ~~...~~ des racines.

Opérons sur la fonction θ l'une des substitutions du groupe total qui ne lui sont pas communes avec les groupes partiels. Soit θ_1 le résultat. Opérons sur la fonction θ_1 la même substitution, et soit θ_2 le résultat, et ainsi de suite.

Comme p est un nombre premier, cette suite ne pourra s'arrêter qu'au ~~terme~~ θ_{p-1}, en sorte que l'on aura, $\theta_p = \theta$, $\theta_{p+1} = \theta_1$, et ainsi de suite.

Cela posé, il est clair que la fonction

$$(\theta + \alpha\theta_1 + \alpha^2\theta_2 + \cdots + \alpha^{p-1}\theta_{p-1})^p$$

* Car l'on aura $f(F(V), r)$ = une fonction divisible par $f(V, r)$. Donc (Lemme I) $f(F(V'), r')$ = une fonction divisible par $f(V', r')$.

1832 Proposition III. Théorème. Si l'on adjoint à une équation toutes les racines ~~...~~ d'une équation auxiliaire, les groupes dont il est question dans le théorème II jouiront de plus de cette propriété que les substitutions ~~...~~ sont les mêmes dans chaque groupe.

On trouvera la démonstration

* N. Il suffit pour cela de choisir une fonction symétrique des diverses valeurs que prend par les permutations de l'un de ces groupes partiels, une fonction qui ~~...~~ n'est invariable par aucune substitution.

soit invariable par toutes les permutations du groupe total, et parcourent un [illegible] commun.

Si l'on extrait la racine $p$ième de cette fonction et qu'on l'adjoigne à l'équation, alors par la proposition IV, le groupe de l'équation ne contiendra plus d'autres substitutions que celles des groupes partiels.

Ainsi, pour que le groupe d'une équation puisse s'abaisser par une simple extraction de racine, la condition ci-dessus est nécessaire et suffisante.

Adjoignons à l'équation le radical en question, nous pourrons raisonner maintenant sur le nouveau groupe comme sur le précédent, et il faudra qu'il se décompose lui-même de la manière indiquée et ainsi de suite jusqu'à un certain groupe qui ne contiendra plus qu'une seule permutation.

Scolie. Il est aisé d'observer cette marche dans la résolution connue des équations générales du 4e degré. En effet, ces équations se résolvent au moyen d'une équation du 3e degré, qui exige elle même l'extraction d'une racine carrée. Dans la suite naturelle des idées, c'est donc par cette racine carrée qu'il faut commencer. Or en adjoignant à l'équation du 4e degré cette racine carrée, le groupe de l'équation qui contenait en tout 24 substitutions, se décompose en deux qui n'en contiennent que douze. En désignant par abcd les racines, voici l'un de ces groupes.

abcd	acdb	adbc
badc	cabd	dacb
cdab	dbac	bcad
dcba	bdca	cbda

Maintenant ce groupe se partage lui même en trois groupes comme il est indiqué aux théorèmes II et III. Ainsi par l'extraction d'un seul radical du 3e degré il reste simplement le groupe

abcd
badc
cdab
dcba

Ce groupe se partage de nouveau en deux groupes

abcd	cdab
badc	dcba

Ainsi, après une simple extraction de racine carrée, il restera

abcd
badc

ce qui se résoudra enfin par une simple extraction de racine carrée.

L'on obtient ainsi soit la solution de Descartes soit celle d'Euler. Car bien que après la résolution de l'équation auxiliaire du 3e degré, ce dernier extraie trois racines carrées, on sait qu'il suffit de deux puisque la troisième s'en déduit rationnellement.

Nous allons maintenant appliquer cette théorie aux équations irréductibles dont le degré est premier.

PROPOSITION VI.

Une équation irréductible de degré premier ne peut devenir réductible par l'adjonction d'un radical.

Car si r, r', r'', ... sont les diverses valeurs du radical, et $Fx = 0$ l'équation proposée, il faudrait que Fx se partageât en facteurs

$f(x, r) \times f(x, r') \times \ldots$

tous de même degré, ce qui ne se peut à moins que $f(x, r)$ ne soit du premier degré en x.

Ainsi une équation irréductible de degré premier ne peut devenir réductible, à moins que son groupe ne se réduise à une seule permutation.

PROPOSITION VIII.

Quel est le groupe d'une équation irréductible de degré premier n, soluble par radicaux?

D'après la proposition précédente, le plus petit groupe possible avant celui qui n'a qu'une seule permutation, contiendra n permutations. Or un groupe de permutations d'un nombre premier n de lettres ne peut se réduire à n permutations, à moins que l'une de ces permutations ne se déduise de l'autre par une substitution circulaire de l'ordre n. (Voir le mémoire de M. Cauchy, Journal de l'École, 17.) Ainsi l'avant dernier groupe sera de la forme

$$\left.\begin{array}{llllll} x_0 & x_1 & x_2 & x_3 & \ldots & x_{n-1} \\ x_1 & x_2 & x_3 & x_4 & \ldots & x_{n-1}\ x_0 \\ x_2 & x_3 & \ldots & & & x_{n-1}\ x_0\ x_1 \\ \ldots & & & & & \\ x_{n-1} & x_0 & x_1 & \ldots & & x_{n-2} \end{array}\right\} \quad (G)$$

x_0, x_1, x_2, ... x_{n-1} étant les racines.

Maintenant le groupe qui précédera immédiatement celui-ci dans l'ordre des décompositions devra se composer d'un certain nombre de groupes ayant tous les mêmes substitutions que celui-ci. Or j'observe que ces substitutions peuvent s'exprimer ainsi. (Faisons en général $x_n = x_0$, $x_{n+1} = x_1$, ... Il est clair que chacune des substitutions du groupe (G) s'obtient en mettant partout à la place de x_k, x_{k+c}, c étant une constante.)

Considérons l'un quelconque des groupes semblables au groupe (G). D'après le théorème II, il devra s'obtenir en opérant dans ce groupe une même substitution, par exemple en mettant partout dans le groupe (G) à la place de x_k, $x_{f(k)}$, f étant une certaine fonction.

Les substitutions de ce nouveau groupe diffèrent de celles de la même façon que celles du groupe G, ce dont on s'assure ainsi

$f(kx+c) = f(x) + C$

C étant indépendant de k.

Une fonction admettra

$f(kx+c) = f(x) + nC$

$f(k^2x+nc) = f(x) + nC$

si $C = 0$, ou bien

$f(x) = ax+b$ ou bien

$fx = akx+b$

a et b étant des constantes.

Donc le groupe qui possède immédiatement le groupe G de même ordre que les substitutions telles que

$x, \quad \frac{kx+b}{ckx+b}$

et ne contenant que, par conséquent toutes substitutions semblables qui aient le groupe G.

Le raisonnement sur un groupe donné est le général, et il s'ensuit que le groupe dans l'ordre de théorie, c'est à dire le groupe adjoint de l'équation ne peut contenir que les substitutions de la forme

$x, \quad \frac{kx+b}{ckx+b}$

Donc, si une équation irréductible de degré premier est résoluble par radicaux, le groupe de cette équation ne contient que des substitutions de la forme

$x, \quad \frac{kx+b}{ckx+b}$

a et b étant des constantes.

Réciproquement : une condition qui lie à elle que l'équation soit résoluble par radicaux. Cherchons en effet les fonctions

$(x, kx+b, k^2x+b, \ldots k^{n-1}x+b)^n = X_1$

$(x_1+kx_2+k^2x_3+\ldots+k^{n-1}x_n)^n = X_2$

$(x_1+kx_2+k^2x_3+\ldots+k^{n-1}x_1)^n = X_3$

. . . . . .

. . . . . .

il est au moins de $n!$ fonctions, et non moins, puisque si on permute $x_1, x_2, x_3 \ldots$ de toutes les manières possibles les fonctions $X_1, X_2, X_3 \ldots$ ne peuvent prendre que $n!$ valeurs. Donc une substitution de $n!$ lettres pour la fonction X_1, &c.

Ainsi, pour qu'une équation irréductible de degré premier soit résoluble par radicaux, il faut et il suffit qu'une fonction irrationnelle des racines admette

$x, \quad \frac{kx+b}{ckx+b}$

dont absolument comme

Ainsi la fonction

$(X_1 - X)(X_2 - X)(X_3 - X) \ldots$

Dans laquelle est X une racine.

Il faut bien et il suffit que l'équation qui donne cette fonction rationnelle, quelque soit X, ait toutes ses racines.

Si l'équation proposée a tous ses coefficients rationnels l'équation qui donne cette fonction le aura tous aussi, et il suffira de reconnaître si cette équation auxiliaire de degré $1.2.3 \ldots (n-1)$ a ou non une racine rationnelle ou que l'on sait faire.

Si C était $= 0$ lorsque x^n est fonction employée dans la question, alors nous allons présenter le théorème sous une autre forme.

PROPOSITION VIII.

Théorème. Pour qu'une équation irréductible de degré premier soit résoluble par radicaux, il faut et il suffit que tous quelconques de ses racines étant connus, les autres s'en déduisent rationnellement.

Pareillement, il a fallu : que les substitutions

$x, \quad \frac{kx+b}{ckx+b}$

ne laissent jamais plus d'une lettre à la même place, et ce n'est qu'en s'appuyant sur cette remarque, que la proposition IV, son groupe donne la valeur à une seule permutation.

Si nous eussions admis, ainsi faisant, que deux ou plus substitutions du groupe ne laissaient plus d'une lettre aux mêmes places. Pareillement le groupe entier doit se composer de $n(n-1)$ permutations. Donc il en résulterait que toutes substitutions semblables (sans que $n!$ soient au moins de $n!$ permutations). Donc tous substitutions du groupe $x, \frac{kx+b}{ckx+b}$, donne substitution de la condition

$x, \quad f(kx+c) = fx + C$

Donc, &c.

Ce théorème est d'une démonstration

Groupe du théorème VII.

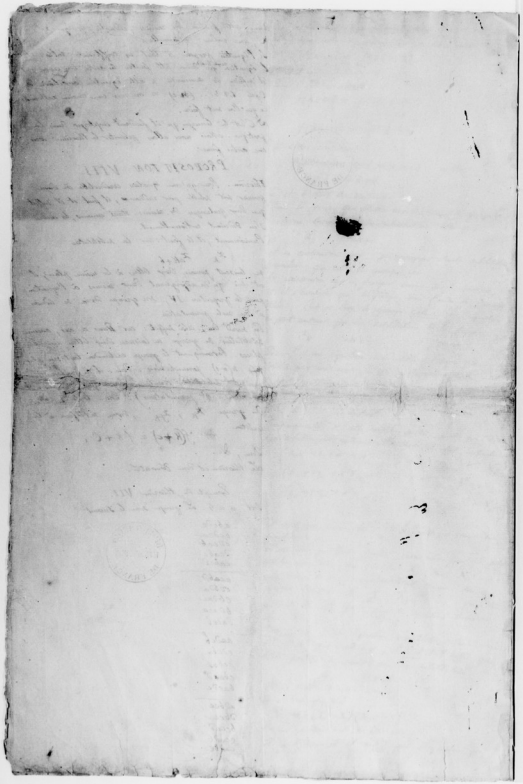
Soit $n = 6$. Le groupe sera le suivant

abcdef
bcdeaf
cdeabf
deabcf
eabcdf

aeabcf
ecbadf
cbdaef
bdcaef
daecbf

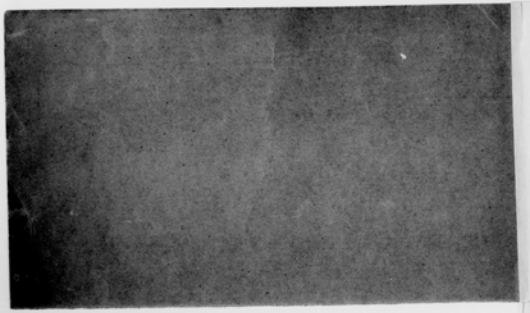
aedbcf
cbdaef
bdaecf
cbaedf
baedcf

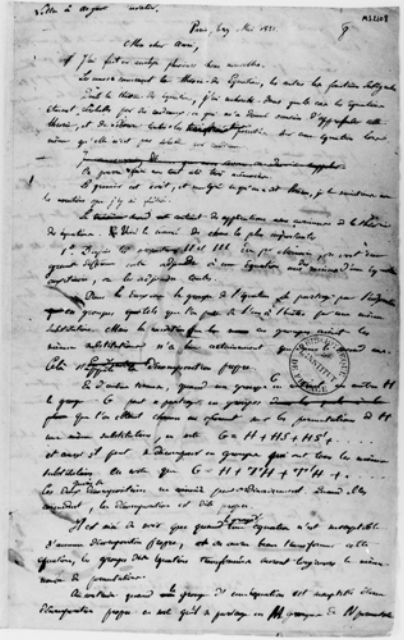
adbecf
dbeacf
becadf
ecadbf
cadbef



Lettre à Auguste Chevalier
du 19 mai 1832

(Œuvres, p. 25)





Paris, 29 Mai 1881.

Mon cher Ami,

Je viens enfin de mettre la dernière main à mon travail sur les équations modulaires. Il est bien long, et je crains que tu ne trouves que j'ai abusé de ta patience. Mais j'ai tant réfléchi à ce sujet, que je ne pouvais me résoudre à le laisser inachevé. Je te prie donc de vouloir bien le lire, et de me dire ton opinion. Si tu le trouves trop long, je le diviserai en deux parties, dont la première pourra paraître dans le prochain cahier du Journal de Crelle.

Je crois avoir démontré, dans ce travail, que la théorie des équations modulaires dépend de la résolution d'une équation auxiliaire, dont le degré est le nombre des substitutions linéaires entières, de déterminant donné, qui ne changent pas la forme fondamentale. Ce nombre est $= (n+1)\prod\left(1-\frac{1}{p^2}\right)$, p étant un nombre premier quelconque, et le produit s'étendant à tous les nombres premiers impairs qui divisent n. Ainsi, pour $n=5$, on a $6\left(1-\frac{1}{9}\right)\left(1-\frac{1}{25}\right)=\frac{48}{5}$, pour $n=7$, on a $8\left(1-\frac{1}{9}\right)\left(1-\frac{1}{49}\right)=\frac{64}{7}$, pour $n=11$, on a $12\left(1-\frac{1}{9}\right)\left(1-\frac{1}{25}\right)\left(1-\frac{1}{121}\right)=\frac{1440}{121}$, etc.

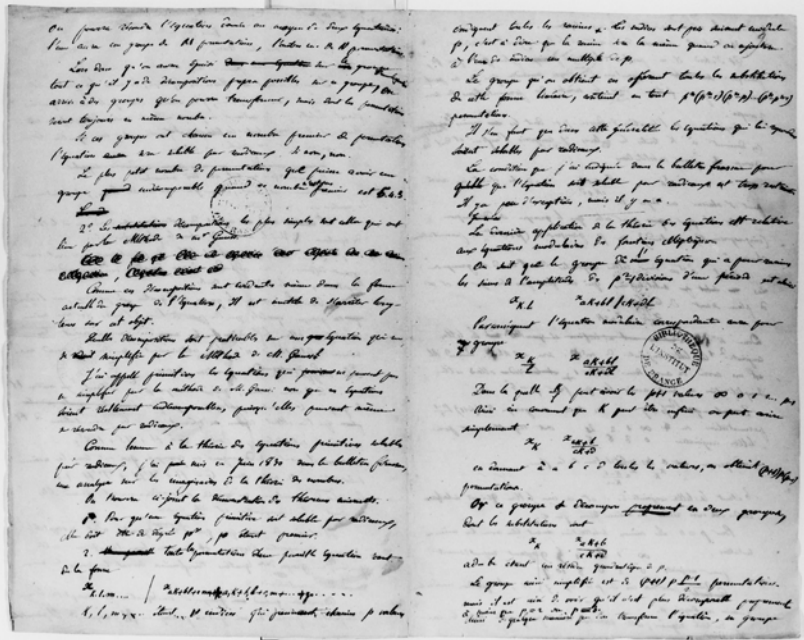
Dans le travail du groupe de l'équation qui partage une fonction quelconque en n parties, on peut se borner à considérer les substitutions linéaires entières, de déterminant n, qui ne changent pas la forme fondamentale $x^2+y^2+z^2$. Le nombre de ces substitutions est $(n+1)\prod\left(1-\frac{1}{p^2}\right)$, comme on vient de le dire.

Si l'on connaît, pour un groupe G de ces substitutions, un autre H dont G soit composé de m groupes semblables à H, on peut abaisser la résolution de l'équation dont dépend G à la résolution d'une équation auxiliaire de degré m, dont les coefficients dépendent de la résolution de l'équation dont dépend H. Si $G=H+HS_1+HS_2+\dots$, et que S_1 soit le plus petit exposant pour lequel HS_1 soit différent de H, S_2 le plus petit exposant pour lequel HS_2 soit différent de H et de HS_1, etc., on a $m=\frac{G}{H}$. Si $G=H+TH+T^2H+\dots$, et que T soit la plus petite puissance de T pour laquelle $T^\alpha H=H$, on a $m=\alpha$.

Si G contient deux groupes H et K, dont le premier soit contenu dans le second, et que $K=H+HT_1+HT_2+\dots$, T_1 étant la plus petite substitution de K qui ne soit pas dans H, T_2 la plus petite substitution de K qui ne soit ni dans H ni dans HT_1, etc., on a $\frac{K}{H}=\frac{G}{K}$.

Il est aisé de voir que quand une équation n'est susceptible d'aucune décomposition propre, et que l'on a trouvé une fonction de ses racines qui ne reste pas la même par toutes les substitutions du groupe de l'équation, on peut toujours trouver une fonction semblable qui ne reste pas la même par toutes les substitutions d'un groupe donné quelconque.

Quand un groupe de substitutions est susceptible d'une décomposition propre, on peut toujours le partager en M groupes de N semblables



toujours le même nombre de permutations.

Abel a été amené à considérer ce problème.

Et Galois a posé le problème plus généralement que P, puisque dans celui-ci l'équation n'est jamais plus que P, avec p pour facteur dans le nombre des permutations du groupe.

Voyons donc si l'équation d'ordre p est résoluble par radicaux ou donnant à R toutes les valeurs d'un groupe d'ordre p des substitutions

$$S,\quad S^{\alpha+\beta}=S^{\alpha}S^{\beta}$$

pour $\alpha=0$ à $\alpha=p-1$ inclusivement.

Il faut d'abord que p soit premier.

Car il faut que le groupe de Galois (supposé résoluble) ait p pour facteur d'ordre premier.

Soient α' et β' deux lettres conjuguées dans Ω et Ω_1 des groupes tels que substituées l'une à l'autre elles donnent le même résultat.

Dans Ω α' et β' sont conjuguées et α' a α lettres conjuguées. Dans Ω_1 α' a α_1 lettres conjuguées. Or α et α_1 ne sont pas différents. Car si α était α_1 on aurait $S^{\alpha}=1$, S étant une substitution telle que S^{α} substituée à α' donne α' et substituée à β' donne β'.

Considérons par exemple $p=7$ et prenons un groupe de $(p+1)!=8!$ permutations où les lettres conjuguées sont respectivement pour

$$\infty \quad 0 \quad 1 \quad 2 \quad 4$$
$$0 \quad 3 \quad 6 \quad 5$$

Le groupe est de la substitution de la forme

$$S_k \quad S_{k+1} \quad S_{k+2}$$

k étant la lettre conjuguée à ∞ et α une lettre qui est substituée elle-même à même rang que ∞.

Pour $p=11$ les mêmes substitutions auront lieu avec les mêmes lettres ;

$$\infty \quad 1 \quad 3 \quad 4 \quad 5 \quad 9$$

pour conjuguées

$$0 \quad 2 \quad 6 \quad 8 \quad 10 \quad 7$$

Pour $p=13$ on a $p=6\frac{1}{2}+11$, l'équation n'est résoluble par radicaux que si p est premier.

En tout cas, cette condition n'est pas suffisante dans le cas [illegible]

la théorie nouvelle exigera la différentielle.

Ce but qu'on donne de plus grand intérêt d'une même fonction algébrique à avoir toujours [illegible] même genre, plus de grandeur algébrique, même genre.

Remarque. Il n'y a pas d'autre fonction pour laquelle cette propriété ait lieu.

Cette propriété absolument caractéristique y appartient dans toute [illegible] plus les intégrales de fonctions algébriques.

On trouve à la fois toutes les fonctions intégrales dont la différentielle est une fonction de la première espèce et d'une même fonction irrationnelle de la variable, qui elle-même n'est pas une rationnelle, qu'elle n'appartient pas à l'équation par des radicaux.

Ainsi les trouve que le nombre des périodes distinctes de chacune de l'intégrale la plus générale obtenue de cette manière est toujours un nombre pair.

Ainsi par ce moyen, on aura la théorie suivante,

Par beaucoup de théorèmes on obtient ici à l'exemple des fonctions algébriques et logarithmiques.

La fonction de première espèce [illegible] pour la partie algébrique et logarithmique est nulle.

Il y en a [illegible] distincts.

La fonction de seconde espèce [illegible] pour la partie algébrique est purement algébrique.

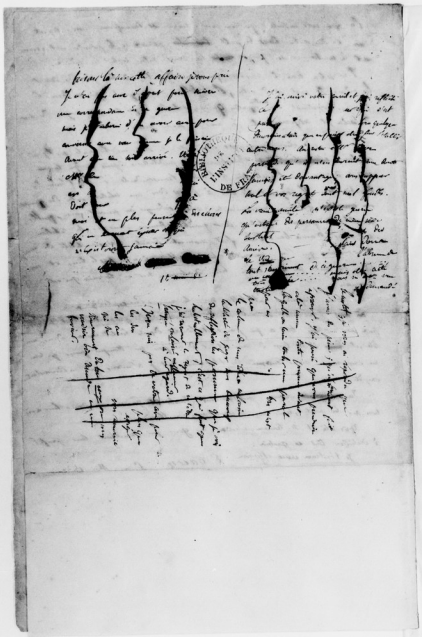
Il y en a [illegible] distincts.

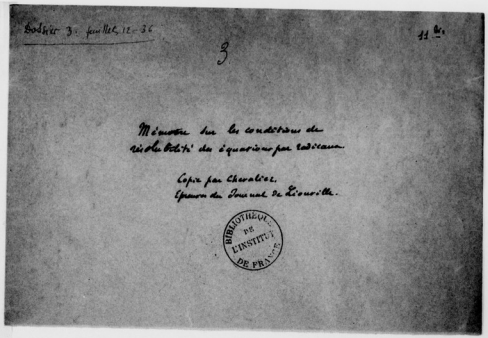
Les fonctions [illegible] ne peuvent exprimer [illegible] de même [illegible] ainsi jamais infinies qu'une fois, et de plus que leur partie logarithmique [illegible] les unes [illegible] les autres, par des [illegible] algébriques. La différence [illegible] $\Pi(a,a)$ est finie, on aura la théorie

$$\Pi(a,a)-\Pi(a,a)=\sum \varphi a\,\varphi a$$

ou φa est [illegible] de première espèce. On en doit [illegible] fonction en appelant $\Pi(a)$, [illegible] fonction de $\Pi(a,a)$ [illegible] par relations à une même fonction $\Pi(a)$,

$$\Pi(a)=\sum \varphi a\,\varphi a.$$





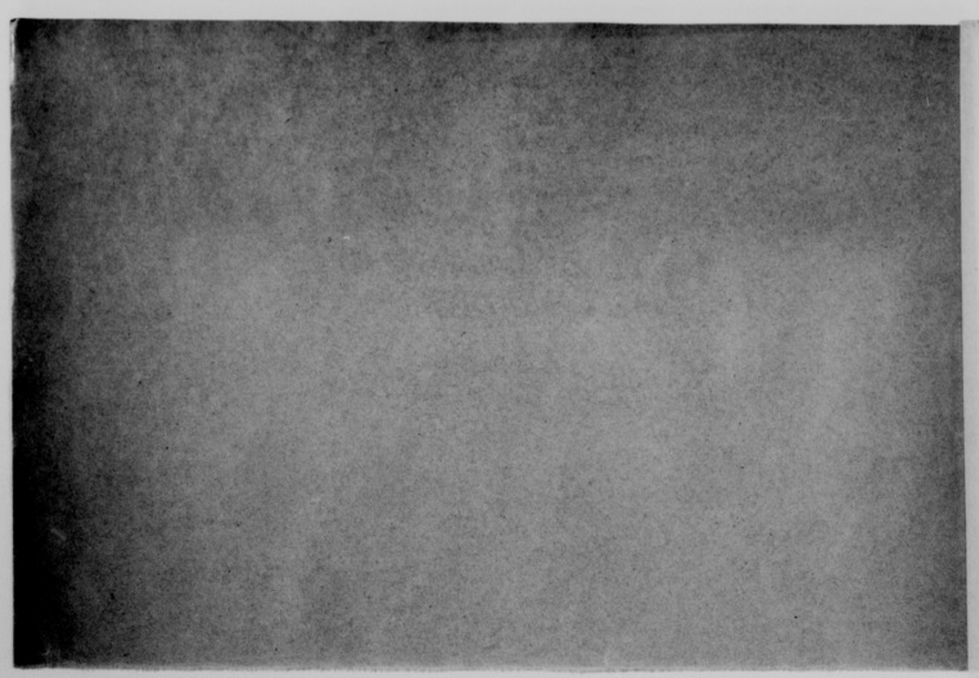
3

11 pp.

Mémoire sur les conditions de stabilité de l'équateur par rotation.

Copie par Chevalier.

Epreuve du Journal de Liouville.



Mémoire sur les conditions de résolubilité des Equations par radicaux.

[1] Le mémoire ci-joint est extrait d'un ouvrage que j'ai eu l'honneur de présenter à l'académie il y a un an. Cet ouvrage n'ayant pas été compris, les propositions qu'il renferme étant révoquées en doute, j'ai cru me contenter de donner sans somme synthétique, les principes généraux, et une seule application de ma théorie. je supplie mes juges de lire du moins avec attention ce peu de pages.

On trouvera ici une condition générale à la quelle satisfait toute équation soluble par radicaux, et qui réciproquement assure leur résolubilité. on en fait l'application seulement aux équations dont le degré est un nombre premier. voici le théorème donné par notre analyse :

Pour qu'une équation de degré premier, qui n'a pas de diviseurs commensurables, soit soluble par radicaux, il faut et il suffit que toutes les racines soient des fonctions rationelles de deux quelconques d'entr'elles.

Les autres applications de la théorie, sont elles-mêmes autant de théories particulières. Elles nécessitent d'ailleurs l'emploi de la théorie des nombres, et d'un algorithme particulier : nous les réservons pour une autre occasion. Elles sont en partie relatives aux équations modulaires de la théorie des fonctions elliptiques, que nous démontrons ne pouvoir se résoudre par radicaux.

Ce 16 janvier 1831. E. Galois.

(1) j'ai jugé convenable de placer en tête de ce mémoire la préface qu'on va lire, bien que je l'aie trouvée biffée dans le manuscrit. ce manuscrit est précisément celui qui fut présenté à l'académie. A.Ch.

Je commencerai par établir quelques définitions et une suite de Lemmes qui leur seront communs.

Définitions. Une équation est dite réductible quand elle admet des diviseurs rationnels; irréductible dans le cas contraire.

Il faut expliquer ce qu'on doit entendre par le mot rationnel dont il se reproduira souvent.

Quand l'équation a tous ses coefficients numériques et rationnels, alors il faudra entendre par diviseurs rationnels, des diviseurs dont les coefficients s'exprimeront en fonctions rationnelles des coefficients de la proposée, en général par quantités rationnelles, des quantités qui s'expriment en fonctions rationnelles des coefficients de la proposée.

Il y a plus: on pourra convenir de regarder comme rationnelle toute fonction rationnelle d'un certain nombre de quantités déterminées, supposées connues à priori: par ex: on pourra choisir une certaine racine d'une équation et on pourra regarder comme rationnelle toute fonction rationnelle de cette racine.

Lorsque nous conviendrons de regarder ainsi comme connues de certaines quantités, alors nous dirons que nous les disposons à l'équation qu'il s'agit de résoudre. Nous dirons que ces quantités sont dépendantes de l'équation.

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

Quand nous nous occuperons d'équations numériques, elles seront rationnelles, de leurs coefficients sont rationnels en notre sens.

On voit déjà en général que la propriété et la difficulté d'une équation peuvent être tout à fait différentes suivant les quantités qui lui sont dépendantes par la disposition d'une quantité peut rendre réductible une équation irréductible.

Ainsi, quand on dispose de l'équation

$$\frac{x^n-1}{x-1} = 0$$ où n est premier

une racine d'une des équations auxiliaires de Mr Gauss, telle équation se décompose en facteurs, et devient par conséquent réductible.

Les substitutions sont le passage d'une permutation à l'autre.

[La permutation] Dieu bien peut pour indiquer les substitutions en 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 on ne peut guère se former l'idée D'une substitution sans se former 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.

[Comme il s'agit toujours De fonctions où la disposition primitive Des lettres, n'influe en rien Dans le grouper que nous considérerons, on Devra avoir Les mêmes substitutions quelle que soit la permutation D'où l'on les fera partir. Dans le Cas D'un pareil groupe on a Les substitutions S et T, on est sûr D'avoir la substitution ST.

[Celles toutes les Définitions que nous avons cru Devoir rappeler.

Lemme I. Une équation irréductible ne peut avoir aucune racine commune avec une équation rationnelle sans Diviseurs. Car le plus grand commun Diviseur entre l'équation irréductible proposée et l'autre équation sera nécessairement rationnel; Donc

Lemme II. étant Donnée une équation algébrique qui n'a pas De racines égales, dont les racines sont a, b, c, ... on peut toujours former une fonction V De racines, telle que toutes les valeurs que cette fonction prend Dans les substitutions Des racines De l'équation proposée soient toutes inégales.

[Car on ne peut prendre

$$V = A.a + B.b + C.c + \dots$$

A, B, C, étant Des nombres entiers convenablement choisis.

Lemme III. Si 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 proposée s'expriment rationnellement en fonction De V.

(1) J'ai trouvé en marge Dans le manuscrit De Galois la note suivante tracée au crayon par M. Liouville.

« Cette Démonstration De ce Lemme n'est pas suffisante; mais il est vrai, d'après le principe Du mémoire De Lagrange : Berlin 1771. »

« Immédiatement après Galois a écrit :

« Nous nous réservons particulièrement la Démonstration que nous venons D'indiquer De ce Lemme dans le mémoire présenté en 1830, mais j'ai jugé inutile De donner la même Démonstration pour un Théorème déjà connu. M. Liouville a supposé

J. Ch.

En effet, soit $V = \varphi(a, b, c, \ldots)$ on aura

$$V - \varphi(a, b, c, \ldots) = 0$$

Multipliez entr'elles toutes les équations semblables que l'on obtient en permutant dans celle-ci toutes les lettres, la première seulement restant fixe; il viendra une équation suivante

$$\{V - \varphi(a, b, c, \ldots)\}\{V - \varphi(a, c, b, \ldots)\}\{V - \varphi(a, b, c, \ldots)\}\ldots$$

équivaut en $b, c, \ldots$ laquelle pourra par conséquent devenir en fonction de a. Donc aurez donc une équation de la forme

$$F(V, a) = 0$$

Or je dis que de là on peut tirer la valeur de a: il suffit pour cela de chercher la solution commune à cette équation et à la proposée. Cette solution est la seule commune, car on ne peut avoir, par exemple:

$$F(V, b) = 0$$

Cette équation ayant un facteur commun avec l'équation semblable dont b est une des fonctions $f(a, \ldots)$ devra être égale à zéro dans tous les cas, donc une fonction $f(a, \ldots)$ sera égale à une fonction $\varphi(b, \ldots)$ ce qui est contre l'hypothèse.

Il suit de là, que a s'exprime en fonction rationnelle de V, et il en est de même de chacune des autres racines.

Cette proposition (1) est utile pour démontrer rigoureusement par Abel dans le mémoire posthume sur les fonctions elliptiques.

Lemme IV Supposons que l'on ait formé l'équation en V; et que l'on ait pris l'une de ses facteurs irréductibles V; et que V soit racine d'une équation irréductible. — On sait que V étant racine de cette équation, toutes les autres $V, V', V'', \ldots$ en seront racines de la proposée, irréductible. Si $a = f(V)$ est une des racines de la proposée, $f(V')$ en sera une autre racine de la proposée.

En effet, en multipliant entr'elles toutes les facteurs de la forme $V - \varphi(a, b, c, \ldots)$ on aura opéré sur les lettres toutes les permutations possibles, on

(1) Il est remarquable que de cette proposition on peut conclure que toute équation dépend d'une équation auxiliaire telle que toutes les racines de cette nouvelle équation, soient des fonctions rationnelles les unes des autres. Car l'équation aux racines en V est dans ce cas.

En toute cette remarque est peut-être inexacte: en effet, une équation qui a cette propriété n'est pas en général plus facile à résoudre qu'une autre.

(note de traducteur)

aura une équation rationnelle en V, laquelle ne pourra être identiquement résoluble par l'équation en question. Donc V' sera fourni par **Lagrange** en lettres dans la fonction V. Soit $F(V,a)=0$ l'équation qui en résulte en permutant. Dans V toutes les lettres sont la première : on aura donc $F'(V',b)=0$ équation pouvant être égal à a, mais n'étant certainement jamais V. Donc racine de l'équation proposée par conséquent donne racine de la proposée et $F(V,a)=0$ conséquent la même que celle qui résultera de la proposée et résultât $a=f(V)$. De même si résultera $b=f(V)$. De $F(V,b)=0$ combinée la dernière

Proposition I.

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

1° que toute fonction des racines invariable par les substitutions de ce groupe sera rationnellement connue.

2° réciproquement, que toute fonction des racines déterminable rationnellement, sera invariable par les substitutions. (Dans le cas d'une équation algébrique, ce groupe n'est autre chose que l'ensemble des $1.2.3 \ldots m$ permutations possibles sur les m lettres, puisque dans ce cas, les fonctions symétriques sont toutes déterminables rationnellement (Dans le cas de l'équation $\frac{x^n-1}{x-1}=0$, si l'équation a pour racines $a=x$ $b=x^2$ $c=x^3 \ldots$ et étant une racine primitive, le groupe de permutations sera simplement celui-ci :

$$\begin{array}{ccccccc} a & b & c & d & \ldots & \ldots & k \\ b & c & d & e & \ldots & k & a \\ c & d & e & \ldots & \ldots & k & a \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ k & a & b & c & \ldots & \ldots & i \end{array}$$

Dans ce cas particulier, le nombre des permutations est égal au degré de l'équation, et la même chose aurait lieu

(1) nous appellerons désormais invariable non seulement une fonction dont la forme est invariable par les substitutions des racines entr'elles, mais encore celle dont la valeur numérique ne varie pas par ces substitutions. Par exemple, si $x=0$ est une équation, x^2 sera une fonction des racines qui ne variera pas comme permutations.

Quand une démonstration une fonction est rationnellement connue, nous voulons dire que la valeur numérique est appréciable en fonction rationnelle des coefficients de l'équation et d'une quantité égale. (note de l'auteur).

Dans les équations dont toutes les racines soient des fonctions rationnelles les unes des autres.)

Démonstration. Quelle que soit l'équation donnée, on pourra trouver une fonction rationnelle V des racines telle que ses puissances aient toutes des fonctions rationnelles de V, celle-ci, par exemple, qui est la première équation irréductible dont V est racine. — (Lemmes III et IV.) Soient $V, V', V'', \ldots V^{(n-1)}$ les racines de cette équation.

L'objet $\psi V, \psi_1 V, \psi_2 V, \ldots, \psi_{n-1} V$ les racines de la proposée.

Prenons les n permutations suivantes des racines

$$\begin{array}{llll} \psi V, & \psi_1 V & \psi_2 V & \ldots \ldots \psi_{n-1} V \\ \psi V', & \psi_1 V' & \psi_2 V' & \ldots \ldots \psi_{n-1} V' \\ \psi V'', & \psi_1 V'' & \psi_2 V'' & \ldots \ldots \psi_{n-1} V'' \\ \ldots & \ldots & \ldots & \ldots \\ \psi V^{(n-1)}, & \psi_1 V^{(n-1)} & \psi_2 V^{(n-1)} & \ldots \ldots \psi_{n-1} V^{(n-1)} \end{array}$$

je dis que ce groupe de permutations jouit de la propriété énoncée.

En effet, 1° toute fonction E des racines, invariable par les substitutions de ce groupe, pourra être égalée à $F\psi V$, et l'on aura

$$\psi V = \psi V' = \psi V'' = \ldots \ldots = \psi V^{(n-1)}$$

La valeur de F pourra donc se déterminer rationnellement.

2° *Réciproquement.* Si une fonction E est déterminable rationnellement, et que l'on ait $E = \psi V$, on aura aussi

$$\psi V = \psi V' = \psi V'' = \ldots \ldots = \psi V^{(n-1)}$$

puisque l'équation en V n'a par hypothèse commensurable et que V satisfait à l'équation $E = \psi V$, E étant une quantité rationnelle. Donc la fonction E des racines est nécessairement invariable par les substitutions du groupe écrit ci-dessus.

Voilà un groupe jouissant de la double propriété dont il s'agit dans le théorème proposé. Le théorème est donc démontré.

Nous appellerons groupe de l'équation le groupe en question. Il est clair que dans le groupe de permutations dont il s'agit ici, la disposition des lettres n'est point

à considérer, mais seulement les substitutions de lettres par lesquelles on passe d'une permutation à l'autre.

Ainsi l'on peut se donner arbitrairement une première permutation, pourvu que les autres permutations s'en déduisent toujours par les mêmes substitutions de lettres. Le nouveau groupe ainsi formé jouira évidemment des mêmes propriétés que le premier, puisque dans le théorème précédent, il ne s'agit que des substitutions que l'on peut faire dans les fonctions.

Scholie 2. Les substitutions sont indépendantes même du nombre des racines.

PROPOSITION II.

Théorème (1). Si l'on adjoint à une équation donnée la racine r d'une équation auxiliaire irréductible, 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'équation auxiliaire. 2° ces groupes jouiront de la propriété remarquable, que l'on passera de l'un à l'autre en opérant dans toutes les permutations du premier une même substitution de lettres.

1° Si, après l'adjonction de r, l'équation en V dont il est question plus haut reste irréductible, il est clair que le groupe de l'équation ne sera pas changé. Si au contraire elle se réduit, alors l'équation en V se décomposera en p facteurs tous de même degré et de la forme

$$f(V,r) \times f(V,r') \times f(V,r'') \times \ldots\ldots$$

$r', r'', r''' \ldots$ étant d'autres valeurs de r. Ainsi le groupe de l'équation proposée se décomposera aussi en groupes chacun d'un même nombre de permutations, puisqu'à chaque valeur de V correspond une permutation. Ces groupes seront respectivement ceux de l'équation proposée, quand on lui adjoindra successivement $r, r', r'' \ldots\ldots$

2° Nous avons vu plus haut que toutes les valeurs de V étaient des fonctions rationnelles les unes des autres. D'après cela, supposons que V étant une racine de $f(V,r)=0$, $F(V)$ en soit une autre. Il est clair que de même si V' est une racine de $f(V,r')=0$, $F(V')$ en sera une autre, car l'on aura

$$f(F(V),r) = \text{une fonction divisible par } f(V,r)$$

---

(1) Ayant à voir la démonstration de ce théorème dans le manuscrit, j'ai trouvé ceci :
« Il y a quelque chose à compléter dans cette démonstration, je n'ai pas le temps ~~[illegible]~~ (note de l'auteur). »
~~[illegible]~~ a été jeté avec une grande rapidité sur le papier ~~[illegible]~~ [illegible] pour le corriger avant d'aller sur le terrain.

[Donc, (Lemme I) $f(F(V'),r')$ est une fonction rationnelle de $f(V,r)$.

Cela posé, je dis que l'on obtient le groupe relatif à r' en opérant partout dans le groupe relatif à r une même substitution de lettres.

[En effet, si l'on a par exemple $\varphi_r F(V) = \varphi_r(V)$ on aura aussi, (Lemme I), $\varphi_{r'} F(V') = \varphi_{r'}(V')$. Donc pour passer de la permutation $(F(V))$ à la permutation $(F(V))$, il faut faire la même substitution que pour passer de la permutation (V) à la permutation (V').

(Le Théorème est donc démontré.

Proposition III.

Théorème. Si l'on adjoint à une équation toutes les racines d'une équation auxiliaire, le groupe dont il est question dans le Théorème II jouissant de plus de cette propriété que les substitutions font toutes les racines de chaque groupe.

(on trouvera la Démonstration. 8)

Proposition IV

Théorème. Si l'on adjoint à une équation la valeur numérique d'une certaine fonction de ses racines, le groupe de l'équation subsistera de manière à devoir être dans une permutation par elle par laquelle cette fonction est invariable.

[En effet, d'après la proposition I, toute fonction semblable doit être invariable par les permutations du groupe de l'équation.

Proposition V

Problème. Dans quels cas une équation est-elle soluble par [illegible] d'Alembert?

J'observerai d'abord que pour résoudre une équation, il faut successivement abaisser les groupes jusqu'à ne contenir plus qu'une seule permutation. Car, quand une équation est résolue, une fonction quelconque de ses racines est connue, même quand elle reste invariable par aucune permutation.

Cela posé, cherchons à quelle condition doit satisfaire le groupe d'une équation, pour qu'il puisse s'abaisser successivement par la adjonction de quantités radicales.

(8) Dans le manuscrit de galois [illegible] où il renvoie. Je trouve en marge de cet [illegible] la Démonstration parfaitement claire. Elle a été effacée, sans doute, [illegible] le Août 1832 et malgré par la mention [illegible] qu'elle est [illegible] parmi celles [illegible] qui [illegible] la note précédente.

A. Ch.

Suivons le nombre des opérations possibles d'une substitution en considérant comme opérations distinctes, l'extraction de chaque racine de degré premier.

8. J'aurais mieux aimé dire que la substitution considérée représentait les permutations de la cinquième classe (Sera modifié)

Puisque = l'opération la plus simple de cet extrait d'une substitution en tirer, cette extraction de racine n'exige plus qu'une simple préparation, le groupe restera le même n'étant pas que simple préparation

Toujours dans le but de opérer un certain nombre fini d'extractions de racines, le groupe devra se trouver dénombré, sans quoi l'équation ne serait pas soluble.

Si arrivés à ce point, il y avait plusieurs manières de dénombrer le groupe de l'équation proposée par une simple extraction de racine, il faudrait, pour ce que nous allons dire, considérer seulement un résultat du degré le moins haut possible parmi tous les simples résultats qui sont tels que la connaissance de chacun d'eux détermine le groupe de l'équation.

Soit donc p le nombre premier qui représente le degré π d'une racine qui par une extraction de racine de degré p, va diminuer le groupe de l'équation.

Nous pouvons toujours supposer, du moins pour ce qui est relatif au groupe de l'équation, que parmi les quantités θ qui jouissent précédemment de la propriété de ne pouvoir être exprimées rationnellement par deux d'entre elles, l'une θ (car comme cette expression rationnelle par deux d'entre elles ne saurait avoir lieu pour plus de p d'entre elles) degré inférieur à p, la connaissance n'altérera en rien le groupe de l'équation.

Par conséquent, d'après le théorème II et III, le groupe de l'équation devra se décomposer en p groupes jouissant les uns par rapport aux autres de cette double propriété : 1° que tous puissent se déduire l'un de l'autre par une seule et même substitution, 2° que tous soient transformés les uns par une même substitution.

Or, dire simplement que le groupe de l'équation puisse se partager en p groupes qui jouissent de cette double propriété, ou pouvoir, par une simple extraction de racine, abaisser le groupe de l'équation à l'un de ces groupes partiels.

Si par l'adjonction de cette racine p ans

Pouvoir en effet une fonction θ sur racines qui soit invariable pour toutes les substitutions d'un des groupes partiels, et ne varie que pour les substitutions (il suffit pour cela de trouver une fonction θ qui ne soit pas invariable pour aucune substitution du groupe total qui ne laisse pas invariable pour toutes les substitutions d'un des groupes partiels, une fonction θ qui ne soit pas invariable par aucune substitution) qui n'est invariable par aucune substitution du groupe total qui opérant sur la fonction θ une des substitutions d'un des groupes partiels, soit θ_1 le résultat, opérant sur la fonction θ_1 la même substitution, soit θ_2 le résultat, et ainsi de suite.

Comme p est un nombre premier, cette suite ne pourra manquer de former θ_{p-1}, autrement dit on aura $\theta_p = \theta$, $\theta_{p+1} = \theta_1$ etc.

Cela posé, il est clair que la fonction

$$(\theta + \theta_1 s + \theta_2 s^2 + \dots + \theta_{p-1} s^{p-1})^p$$

sera invariable par toutes les permutations du groupe total,

et par conséquent sera actuellement connue.

Si l'on extrait la racine $p^{\text{ème}}$ de cette fonction, et qu'on l'adjoigne à l'équation, alors par la proposition IV, le groupe de l'équation ne contiendra plus d'autres substitutions que celles des groupes partiels.

Ainsi, pour que le groupe d'une équation puisse s'abaisser par une simple extraction de racine, la condition ci-dessus est nécessaire et suffisante.

Adjoignons à l'équation le radical en question, nous pourrons raisonner maintenant sur le nouveau groupe comme sur le précédent, et il faudra qu'il se décompose lui-même de la manière indiquée, et ainsi de suite, jusqu'à un certain groupe qui ne contiendra plus qu'une seule permutation.

Scholie. Il est aisé d'observer cette marche dans la résolution connue des équations générales du 4.ème degré. En effet, ces équations se résolvent au moyen d'une équation du 3.ème degré qui exige elle-même l'extraction d'une racine carrée. Dans la suite naturelle des idées, c'est donc par cette racine carrée qu'il faut commencer. Or en adjoignant à l'équation du 4.ème degré cette racine carrée, le groupe de l'équation qui contenait en tout 24 substitutions, se décompose en deux qui n'en contiennent que douze. En désignant par a b c d les racines, voici l'un de ces groupes :

abcd	acdb	adbc
badc	cadb	dacb
cdab	dbac	bcad
dcba	bdca	cbda

maintenant ce groupe se partage lui-même en trois groupes comme il est indiqué aux théorèmes II et III. ainsi par l'extraction d'un seul radical du 3.ème degré, il reste simplement le groupe.

abcd
badc
cdab
dcba

ce groupe se partage de nouveau en deux groupes

abcd	cdab
badc	dcba

ainsi après une simple extraction de racine carrée, il restera,

abcd
badc

ce qui se résoudra enfin par une simple extraction de racine carrée.

On obtient ainsi soit la solution de Descartes, soit celle d'Euler. Car bien qu'après la résolution de l'équation auxiliaire du 3.ème degré, ce dernier extraie trois racines carrées, on sait qu'il suffit de deux, puisque la troisième s'en déduit rationnellement.

Nous allons maintenant appliquer cette condition aux équations irréductibles dont le degré est premier.

Application aux Equations irréductibles [illegible]

De Degré premier

Proposition VI

Lemme. une équation irréductible de degré premier ne peut devenir réductible par la substitution d'une racine [illegible]

Car si $1, \theta, \theta' \ldots$ sont les différentes valeurs d'un radical, et $Fx = 0$ l'équation proposée, il faudra que Fx se partage en facteurs

$$f(x,\theta)\,f(x,\theta')\ldots\ldots\ldots$$

tous de même degré, ce qui ne se peut à moins que $f(x,\theta)$ ne soit du premier degré en x.

Donc une équation irréductible de degré premier ne peut devenir réductible, à moins que les groupes ne se réduisent à une seule permutation.

Proposition VII.

Problème. Quel est le groupe d'une équation irréductible d'un degré premier n, résoluble par radicaux?

D'après la proposition précédente, le plus petit groupe possible auquel celui que j'ai [illegible] une seule permutation, contient n permutations. Or un groupe de permutations d'un nombre premier $= n$ de lettres, ne peut se réduire à m permutations, m moindre que n que si les permutations ne se décomposent les unes par une substitution circulaire de degré n. (voir le mémoire de Mr Cauchy, Journal de l'école 17). Donc le plus petit groupe sera de la forme.

$$\left.\begin{array}{llllll} x_0 & x_1 & x_2 & x_3 & \ldots & x_{n-1} \\ x_1 & x_2 & x_3 & x_4 & \ldots & x_0 \\ x_2 & x_3 & \ldots & \ldots & x_{n-1} & x_0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ x_{n-1} & x_0 & x_1 & \ldots & \ldots & x_{n-2} \end{array}\right\} \quad (G)$$

$x_0, x_1, x_2 \ldots\ldots x_{n-1}$ sont les racines.

Maintenant, le groupe que je viens d'obtenir admet une substitution circulaire, donc le compose d'une certaine nombre de groupes ayant tous la même substitution que celle-ci. Or j'observe que une substitution pareille n'opère ainsi: (je mets en général $x_0 x_\alpha x_{\alpha+\beta} x_\gamma \ldots$ il est clair que chacune des substitutions du groupe (G) substituant en même temps à la place de x_k, $x_{k+\theta}$, θ étant une constante)

Considérons [illegible] quelconque d'un groupe semblable au groupe G. D'après le théorème 22, de [illegible] en général portant dans ce groupe une même substitution, par exemple α en mettant partout dans le groupe (G) x à la place

De x_k , $\chi f(k)$, f étant une certaine fonction. 23

Les substitutions de ce nouveau groupe peuvent être mises sous la forme (6), on aura donc

$$f(k+c) = f(k) + C.$$

C étant indépendant de k

$$\text{Donc } f(k+2c) = f(k) + 2C$$

$$\cdots\cdots\cdots$$

$$f(k+mc) = f(k) + mC$$

si $c=1$, $k=0$ on trouvera

$$f(m) = am + b \quad \text{ou bien}$$

$$f(k) = ak + b$$

a et b étant des constantes.

Donc le groupe qui possède isomorphiquement le groupe G ne devra contenir que des substitutions telles que

$$x_k \qquad x_{ak+b}$$

et ne contiendra par, par conséquent d'autre substitution semblable que celle du groupe G.

On reconnaîtra sur ce groupe comme sur le précédent, en effectuant que le premier groupe d'une équation de décomposition de $x^n = 1$ est le groupe actuel de l'équation, ne peut contenir que des substitutions de la forme

$$x_k \qquad x_{ak+b}$$

Donc, si une équation irréductible de degré premier est soluble par radicaux, le groupe de cette équation devra contenir que des substitutions de la forme

$$x_k \qquad x_{ak+b}$$

a et b étant des constantes. N

Si dépourvu de cette condition a lieu, je dis que l'équation sera soluble par radicaux. considérons en effet les fonctions :

$$\left(x_0 + \alpha x_1 + \alpha^2 x_2^2 + \cdots\cdots + \alpha^{n-1} x_{n-1}\right)^n = X_1$$

$$\left(x_0 + \alpha x_{\alpha} + \alpha^2 x_{\alpha^2} + \cdots\cdots + \alpha^{n-1} x_{(n-1)\alpha}\right)^n = X_{\alpha}$$

$$\left(x_0 + \alpha x_{\alpha^2} + \alpha^2 x_{\alpha^4} + \cdots\cdots + \alpha^{n-1} x_{(n-1)\alpha^2}\right)^n = X_{\alpha^2}$$

α étant une racine $p^{ième}$ de l'unité, α une racine primitive de n.

Il est clair que toute fonction invariable par les substitutions circulaires des quantités x_1 x_2 x_3 $\cdots$ sera aussi évidemment connue. Donc on pourra trouver x_1 x_2 x_3 $\cdots$ $\cdots$ par la méthode de M. Gauss pour les équations binômes. Donc la

Reste, pour qu'une équation irréductible de degré premier

soit résolue par radicaux, il faut et il suffit que toute fonction invariable par ces substitutions

$$x_k \quad x_{ak+b}$$

soit rationnellement connue.

Considérons la fonction

$$(x_1 - x)(x_a - x)(x_{a^2} - x) \cdots$$

dont quelque soit x est connue.

Il faut donc et il suffit que l'équation qui donne cette fonction donne racines, quelque soit x une valeur rationnelle.

Si l'équation proposée a tous ses coefficients rationnels, l'équation auxiliaire qui donne cette fonction les aura tous aussi, et il suffira de reconnaître si cette équation aura pour degré $1.2.3 \cdots (n-1)$ ou un nombre moindre rationnellement connu, ce qui sera facile.

C'est là le moyen qu'il faudra employer dans la pratique; mais nous allons présenter le théorème sous une autre forme.

Proposition VII

Théorème. Pour qu'une équation irréductible de degré premier soit résoluble par radicaux, il faut et il suffit que deux quelconques de ses racines étant connues, toutes les autres le soient rationnellement.

Premièrement, il le faut: car la substitution

$$x_k \quad x_{ak+b}$$

ne laissant jamais deux lettres à la même place, il est clair qu'en désignant deux racines à l'équation, par la proposition IV, le groupe devra se réduire à une seule permutation.

En second lieu, cela suffit: car dans ce cas, aucune substitution du groupe ne laissera deux lettres aux mêmes places. par conséquent le groupe contient au plus n (ou) permutations. Donc il ne contient que la seule substitution circulaire (sans quoi il y aurait au moins p^2 permutations). Or toute substitution du groupe x_k, x_{ak+b} devra satisfaire à la condition:

$$f(k+c) = fk + c.$$

Donc &c.

Le théorème est donc démontré.

Exemple du théorème VII

Soit n = 5. Le groupe sera le suivant : 25

a b c d e
b c d e a
c d e a b
d e a b c
e a b c d

---

a c e b d
c e b d a
e b d a c
b d a c e
d a c e b

---

a e d c b
e d c b a
d c b a e
c b a e d
b a e d c

---

a d b e c
d b e c a
b e c a d
e c a d b
c a d b e.

MÉMOIRE

SUR

LES CONDITIONS DE RÉSOLUBILITÉ DES ÉQUATIONS PAR RADICAUX;

PAR ÉVARISTE GALOIS.

Le Mémoire ci-joint [*] est extrait d'un ouvrage que j'ai eu l'honneur de présenter à l'Académie il y a un an. Cet ouvrage n'ayant pas été compris, les propositions qu'il renferme ayant été révoquées en doute, j'ai dû me contenter de donner, sous forme synthétique, les principes généraux, et une *seule* application de ma théorie. Je supplie mes juges de lire du moins avec attention ce peu de pages.

On trouvera ici une condition générale à laquelle satisfait toute équation *soluble par radicaux*, et qui réciproquement assure leur résolubilité. On en fait l'application seulement aux équations dont le degré est un nombre premier. Voici le théorème donné par notre analyse :

Pour qu'une équation de degré premier, qui n'a pas de diviseurs commensurables, soit soluble par radicaux, il faut et il suffit que toutes les racines soient des fonctions rationnelles de deux quelconques d'entre elles.

Les autres applications de la théorie sont elles-mêmes autant de théories particulières. Elles nécessitent d'ailleurs l'emploi de la théorie des nombres, et d'un algorithme particulier : nous les réservons pour une autre occasion. Elles sont en partie relatives aux équations modulaires de la théorie des fonctions elliptiques, que nous démontrons ne pouvoir se résoudre par radicaux.

Ce 16 janvier 1831.

E. GALOIS.

[*] J'ai jugé convenable de placer en tête de ce Mémoire la préface qu'on va lire, bien que je l'aie trouvée hâtivement dans le manuscrit. Ce manuscrit est précisément celui que l'auteur présenta à l'Académie.

(Moigno, Chevalier)

Tome VIII. — Bull., mars 1831. 52

PRINCIPES.

Je commencerai par établir quelques définitions et une suite de lemmes qui sont tous connus.

Définitions. Une équation est dite réductible quand elle admet des diviseurs rationnels, irréductible dans le cas contraire.

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

Quand l'équation a *tous* ses coefficients numériques et rationnels, on entend 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.

Il y a plus, on pourra convenir de regarder comme rationnelle toute fonction rationnelle d'un certain nombre de quantités déterminées, supposées connues à 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 fonction rationnelle des coefficients de l'équation et d'un certain nombre de quantités *adjointes* à l'équation et convenues arbitrairement.

Quand nous nous servirons d'équations auxiliaires, elles seront rationnelles, si leurs coefficients sont rationnels en notre sens.

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.

Ainsi, quand on a joint à l'équation

$$\frac{x^n-1}{x-1}=0,\quad \text{où } n \text{ est premier},$$

une racine d'une des équations auxiliaires de M. Gauss, cette équation se décompose en facteurs, et devient par conséquent réductible.

Les substitutions sont le passage d'une permutation à l'autre.

La terminaison 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 on ne peut guère se former l'idée d'une substitution sans se donner 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.

Comme il s'agit toujours 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 nous en avons groupé ou si les substitutions S et T, on est sûr d'avoir la substitution ST.

Telles sont les définitions que nous avons cru devoir rappeler.

LEMME I. 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 et l'autre équation, sera encore rationnel; donc, etc.

LEMME II. Etant donnée une équation quelconque, qui n'a pas de racines égales, dont les racines sont $a, b, c, \ldots$, 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

$$V = Aa + Bb + Cc + \dots,$$

A, B, C étant des nombres entiers convenablement choisis.

LEMME III (*). 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 proposée s'exprimeront rationnellement en fonction de V.

En effet, soit

$$V = \varphi(a, b, c, d, \dots),$$

ou bien

$$V - \varphi(a, b, c, d, \dots) = 0.$$

Multiplions entre elles toutes les équations semblables, que l'on obtient en permutant dans celles-ci toutes les lettres, la première seulement restant fixe; il viendra une expression suivante :

$$[V - \varphi(a, b, c, d, \dots)]\,[V - \varphi(a, c, b, d, \dots)]\,[V - \varphi(a, b, d, c, \dots)]\dots$$

symétrique en $b, c, d, \dots$, laquelle pourra par conséquent s'écrire en fonction de a. Nous aurons donc une équation de la forme

$$F(V, a) = 0.$$

Or je dis que de là on peut tirer la valeur de a. Il suffit pour cela de chercher la solution commune à cette équation et à la proposée. Cette solution est la seule commune, car on ne peut avoir, par exemple,

$$F(V, b) = 0;$$

(*) J'ai trouvé en marge, dans le manuscrit de Galois, la note suivante, tracée au crayon par Poisson :

« La démonstration de ce lemme n'est pas suffisante; mais il est vrai, d'après le n° 100 du Mémoire de Lagrange. Berlin, 1775. »

Immédiatement après, Galois a écrit :

« Nous avons transcrit textuellement la démonstration que nous avons donnée de ce lemme dans le Mémoire présenté en 1831. Nous y joignons, comme documents historique, la note suivante, qu'a cru devoir y apposer M. Poisson. — On jugera. »

M(Argath. Chevalier).

cette équation ayant un facteur commun avec l'équation semblable, sans quoi l'une des fonctions $\varphi(a, \dots)$ serait égale à l'une des fonctions $\varphi(b, \dots)$; ce qui est contre l'hypothèse.

Il suit de là que a s'exprime en fonction rationnelle de V, et il en est de même des autres racines.

Cette proposition (*) est citée sans démonstration, par Abel, dans le Mémoire posthume sur les fonctions elliptiques.

LEMME IV. 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 racines de la proposée, $f(V')$ de même sera une racine de la proposée.

En effet, en multipliant entre eux tous les facteurs de la forme $V - \varphi(a, b, c, \dots, d)$, où l'on aura opéré sur les lettres toutes les permutations possibles, on aura une équation rationnelle en V, laquelle se trouvera nécessairement divisible par l'équation en question; donc V doit s'obtenir par l'échange des lettres dans la fonction V. Soit $F(V, a) = 0$ l'équation qu'on obtient en permutant dans V toutes les lettres, hors la première. On aura donc $F(V, b) = 0$, b pouvant être égal à a, mais étant certainement l'une des racines de l'équation proposée; par conséquent, de même que de la proposée on déduit $F(V, a) = 0$ est résolu $a = f(V)$, de même il résultera de la proposée et de $F(V, b) = 0$ combinées, la suivante $b = f(V)$.

PROPOSITION I.

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

(*) Il est remarquable, que de cette proposition on peut conclure que toute équation dépend d'une équation auxiliaire telle, que toutes les racines de cette nouvelle équation soient des fonctions rationnelles les unes des autres; car l'équation auxiliaire en V est dans ce cas.

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

(L'Auteur du Commentaire).

1°. Que toute fonction des racines invariable [*] par les substitutions de ce groupe, soit rationnellement connue ;

2°. Réciproquement, que toute fonction des racines déterminable rationnellement, soit invariable par les substitutions. Dans le cas des équations algébriques, ce groupe n'est autre chose que l'ensemble des $1, 2, 3, \ldots, n$ permutations possibles sur les n lettres, puisque, dans ce cas, les fonctions symétriques sont seules déterminables rationnellement.)

(Dans le cas de l'équation $\frac{x^m-1}{x-1}=0$, si l'on suppose $a=r$, $b=r^c$, $c=r^d, \ldots$, g étant une racine primitive, le groupe de permutations sera simplement celui-ci :

$$\begin{array}{ll} abcd \ldots\ldots & k \\ bcd \ldots\ldots & ka \\ cd \ldots\ldots & kab \\ \ldots\ldots & \ldots\ldots \\ kabc \ldots\ldots & i \end{array}$$

dans ce cas particulier, le nombre des permutations est égal au degré de l'équation, et la même chose aurait lieu dans les équations dont toutes les racines seraient des fonctions rationnelles les unes des autres.)

Démonstration. Quelle que soit l'équation donnée, on pourra trouver une fonction rationnelle V des racines, telle que toutes les racines soient fonction rationnelle de V. Cela posé, considérons l'équation irréductible dont V est racine. (Lemmes III et IV.) Soient V, V', V'', ... $V^{(m)}$ les racines de cette équation.

[*] Nous appelons ici invariable non-seulement une fonction dont la forme est invariable par les substitutions des racines entre elles, mais encore celle dont la valeur numérique ne variera pas par ces substitutions. Par exemple, si $F(x)=0$ est une équation, Fx est une fonction des racines qui ne varie par aucune permutation.

Quand nous dirons qu'une fonction est rationnellement connue, nous voudrons dire que sa valeur numérique est exprimable en fonction rationnelle des coefficients de l'équation et des quantités adjointes.

(Note de l'auteur.)

Soient $\varphi V, \varphi_1 V, \varphi_2 V, \ldots, \varphi_{m-1} V$ les racines de la proposée. Écrivons les n permutations suivantes des racines

$$\begin{array}{llll} \varphi V, & \varphi_1 V, & \varphi_2 V \ldots\ldots & \varphi_{m-1} V, \\ \varphi V', & \varphi_1 V', & \varphi_2 V' \ldots\ldots & \varphi_{m-1} V', \\ \varphi V'', & \varphi_1 V'', & \varphi_2 V'' \ldots\ldots & \varphi_{m-1} V'', \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ \varphi V^{(m-1)}, & \varphi_1 V^{(m-1)}, & \varphi_2 V^{(m-1)} \ldots\ldots & \varphi_{m-1} V^{(m-1)}; \end{array}$$

je dis que ce groupe de permutations jouit de la propriété énoncée.

En effet, 1° toute fonction F des racines, invariable par les substitutions de ce groupe, pourra être écrite ainsi $F=\varphi V$, et l'on aura

$$\varphi V = \varphi V' = \varphi V'' = \ldots = \varphi V^{(m-1)};$$

La valeur de F pourra donc se déterminer rationnellement.

2°. *Réciproquement.* Si une fonction F est déterminable rationnellement, et que l'on pose $F=\varphi V$, on devra avoir

$$\varphi V = \varphi V' = \varphi V'' = \ldots = \varphi V^{(m-1)},$$

puisque l'équation en V n'a pas de diviseur commensurable et que V satisfait à l'équation $F=\varphi V$, F étant une quantité rationnelle. Donc la fonction F sera nécessairement invariable par les substitutions du groupe écrit ci-dessus.

Ainsi, ce groupe jouit de la double propriété dont il s'agit dans le théorème proposé. Le théorème est donc démontré.

Nous appellerons groupe de l'équation, le groupe en question.

Scolie 1°. Il est évident que dans le groupe de permutations dont il s'agit ici, la disposition de lettres n'est point à considérer, mais seulement les substitutions de lettres par lesquelles on passe d'une permutation à l'autre.

Ainsi l'on peut se donner arbitrairement une première permutation, pourvu que les autres permutations s'en déduisent toujours par les mêmes substitutions de lettres. Le nouveau groupe ainsi formé jouira évidemment des mêmes propriétés que le premier, puisque dans le théorème précédent, il ne s'agit que des substitutions que l'on peut faire dans les fonctions.

Seulle 2. Les substitutions sont indépendantes même du nombre des racines.

PROPOSITION II.

THÉORÈME [*]. — Si l'on adjoint à une équation donnée la racine d'une équation auxiliaire irréductible, 1° il arrivera de 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'équation auxiliaire; 2° ces groupes jouiront de la propriété remarquable que l'on passera de l'un à l'autre en opérant dans toutes les permutations du premier une même substitution de lettres.

1°. Si, après l'adjonction de r, l'équation en V, dont il est question plus haut, reste irréductible, il est clair que le groupe de l'équation ne sera pas changé. Si au contraire elle se réduit, alors l'équation en V se décomposera en p facteurs, tous de même degré et de la forme

$$f(V, r) \times f(V, r') \times f(V, r') \times \dots,$$

r, r', r',... étant d'autres valeurs de f. Ainsi le groupe de l'équation proposée se décomposera aussi en groupes chacun d'un même nombre de permutations, puisque à chaque valeur de V correspond une permutation. Ces groupes seront respectivement ceux de l'équation proposée, quand on lui adjoindra successivement r, r', r',...

2°. Nous avons vu plus haut que toutes les valeurs de V étaient des fonctions rationnelles les unes des autres. D'après cela, supposons que V étant une racine de $f(V, r) = 0$, $\Phi(V)$ en soit une autre; il est clair que de même si V' est une racine de $f(V, r') = 0$, $\Phi(V')$ en sera une autre; car l'on aura

$$f[\Phi(V), r] = \text{une fonction divisible par } f(V, r).$$

[*] Via-à-vis la démonstration de ce théorème, dans le manuscrit, j'ai trouvé écrit : « Il y a quelque chose à compléter dans cette démonstration. Je n'ai pas le temps. » (*Commentaires.*)

Cette ligne a été tracée avec une grande rapidité sur le papier; cependant on y lit, jusqu'à ces mots : « Je n'ai pas le temps », ne fait-ce que ce qu'on a vu de mieux pour le développer accord d'abord sur la marche.

(*Augustin Cauchy*).

(**) Ceci montre d'une manière très explicite ce que j'avais dit.

Donc (*lemme 1*)

$$f[\Phi(V), r'] = \text{une fonction divisible par } f(V, r').$$

Cela posé, je dis que l'on obtient le groupe relatif à r' en opérant partout dans le groupe relatif à r une même substitution de lettres.

En effet, si l'on a, par exemple,

$$\psi_2 \Phi(V) = \psi_1(V),$$

on aura encore (*lemme 1*)

$$\psi_2 \Phi(V') = \psi_1(V').$$

Donc, pour passer de la permutation $[\Phi(V)]$ à la permutation $[\Phi(V')]$, il faut faire la même substitution que pour passer de la permutation (V) à la permutation (V').

Le théorème est donc démontré.

PROPOSITION III.

THÉORÈME. — Si l'on adjoint à une équation toutes les racines d'une équation auxiliaire, les groupes dont il est question dans le Théorème II jouiront de plus de cette propriété, que les substitutions semblables dans chaque groupe

On trouvera la démonstration [*].

PROPOSITION IV.

THÉORÈME. — Si l'on adjoint à une équation la valeur numérique d'une certaine fonction de ses racines, le groupe de l'équation s'abaissera de manière à n'avoir plus d'autres permutations que celles par lesquelles cette fonction est invariable.

[*] Dans le manuscrit de Galois l'énoncé du théorème qu'on vient de lire se trouve en marge et vis-à-vis de la démonstration qu'il en avait écrite d'abord. Celle-ci est effacée avec soin; l'énoncé précédent porte la date 1830, et montre par la manière dont il est écrit que l'auteur était extrêmement pressé, ce qui confirme l'assertion que j'ai avancée dans la note précédente.

Tome VIII. — Novembre 1843.

(*Augustin Cauchy*).

En effet, d'après la proposition I, toute fonction connue doit être invariable par les permutations du groupe de l'équation.

PROPOSITION V.

PROBLÈME. Dans quels cas une équation est-elle soluble par de simples radicaux?

J'observerai d'abord que pour résoudre une équation, il faut successivement abaisser son groupe jusqu'à ne contenir plus qu'une seule permutation. Car, quand une équation est résolue, une fonction quelconque de ses racines est connue, même quand elle n'est invariable par aucune permutation.

Cela posé, cherchons à quelle condition doit satisfaire le groupe d'une équation, pour qu'il puisse s'abaisser par l'adjonction de quantités radicales.

Suivons la marche des opérations possibles dans cette solution, en considérant comme opérations distinctes l'extraction de chaque racine de degré premier.

Adjoignons à l'équation le premier radical extrait dans la solution. Il pourra arriver deux cas: ou bien, par l'adjonction de ce radical, le groupe des permutations de l'équation sera diminué; ou bien, cette extraction de racine n'étant qu'une simple préparation, le groupe restera le même.

Toujours sera-t-il qu'après un certain nombre *fini* d'extractions de racines, le groupe devra se trouver diminué, sans quoi l'équation ne serait pas soluble.

Si, arrivé à ce point, il y avait plusieurs manières de diminuer le groupe de l'équation proposée par une simple extraction de racine, il faudrait, pour ce que nous allons dire, considérer seulement un radical du degré le moins haut possible parmi tous les simples radicaux qui sont tels que la connaissance de chacun d'eux diminue le groupe de l'équation.

Soit donc p le nombre premier qui représente ce degré minimum, en sorte que par une extraction de racine de degré p, on diminue le groupe de l'équation.

Nous pouvons toujours supposer, du moins pour ce qui est relatif

au groupe de l'équation, que parmi les quantités adjointes précédemment à l'équation se trouve une racine $p^{ième}$ de l'unité a. Car, comme cette expression s'obtient par des extractions de racines de degré inférieur à p, sa connaissance n'altérera en rien le groupe de l'équation.

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

Je dis réciproquement, que si le groupe de l'équation peut se partager en p groupes qui jouissent de cette double propriété, on pourra, par une simple extraction de racines $p^{ième}$, et par l'adjonction de cette racine $p^{ième}$, réduire le groupe de l'équation à l'un de ces groupes partiels.

Prenons en effet une fonction des racines qui soit invariable pour toutes les substitutions de l'un des groupes partiels, et ne varie pour aucune autre substitution. (Il suffit, pour cela, de choisir une fonction symétrique des diverses valeurs que prend, par toutes les permutations de l'un des groupes partiels, une fonction qui n'est invariable par aucune substitution.)

Soit θ cette fonction des racines.

Opérons sur la fonction θ une des substitutions du groupe total qui ne lui sont pas communes avec les groupes partiels. Soit θ_1 le résultat. Opérons sur la fonction θ_1 la même substitution, et soit θ_2 le résultat, et ainsi de suite.

Comme p est un nombre premier, cette suite ne pourra s'arrêter qu'au terme θ_{p-1}, ensuite l'on aura $\theta=\theta_p$, $\theta_1=\theta_{p+1}$, et ainsi de suite.

Cela posé, il est clair que la fonction

$$(\theta+a\theta_1+a^2\theta_2+\ldots+a^{p-1}\theta_{p-1})^p$$

sera invariable par toutes les permutations du groupe total, et, par conséquent, sera actuellement connue.

Si l'on extrait la racine $p^{ième}$ de cette fonction, et qu'on l'adjoigne à l'équation, alors, par la proposition IV, le groupe de l'équation ne contiendra plus d'autres substitutions que celles des groupes partiels.

Ainsi, pour que le groupe d'une équation puisse s'abaisser par une simple extraction de racine, la condition ci-dessus est nécessaire et suffisante.

Adjoignons à l'équation le radical en question, nous pourrons raisonner maintenant sur le nouveau groupe comme sur le précédent, et il faudra qu'il se décompose lui-même de la manière indiquée, et ainsi de suite, jusqu'à un certain groupe qui ne contiendra plus qu'une seule permutation.

Scolie. Il est ainsi d'observer cette marche dans la résolution connue des équations générales du quatrième degré. En effet, ces équations se résolvent au moyen d'une équation du troisième degré, qui s'aide elle-même l'extraction d'une racine carrée. Dans la suite naturelle des idées, c'est donc par cette racine carrée qu'il faut commencer. Opérons adjoignant à l'équation du quatrième degré cette racine carrée, le groupe de l'équation qui contenait en tout vingt-quatre substitutions, se décompose en deux qui n'en contiennent que douze. En désignant par a, b, c, d les racines, voici l'un de ces groupes :

abcd,	*acdb*,	*adbc*,	
bcda,	*cdab*,	*dacb*,	
cdab,	*dbac*,	*bcad*,	
dcba,	*bdca*,	*cbda*.	

Maintenant ce groupe se partage lui-même en trois groupes, comme il est indiqué aux Théorèmes II et III. Ainsi, par l'extraction d'un seul radical du troisième degré, il reste simplement le groupe

abcd,
bacl,
cdal,
dcba;

ce groupe se partage de nouveau en deux groupes

abcd, *cdab*,
bacl, *dcba*.

Ainsi, après une simple extraction de racine carrée, il restera

abcd,
bacl;

ce qui se résoudra enfin par une simple extraction de racine carrée.

On obtient ainsi, soit la solution de Descartes, soit celle d'Euler; car, bien qu'après la résolution de l'équation auxiliaire du troisième degré, ce dernier extraye trois racines carrées, on sait qu'il suffit de deux, puisque la troisième s'en déduit naturellement.

Nous allons maintenant appliquer cette condition aux équations irréductibles dont le degré est premier.

Application aux équations irréductibles de degré premier.

PROPOSITION VI.

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

Car si r, r', r'',... sont les diverses valeurs du radical, et $Fx = 0$ l'équation proposée, il faudrait que Fx se partageât en facteurs

$$f(x, r) \times f(x, r') \times \ldots,$$

tous de même degré, ce qui ne se peut, à moins que $f(x, r)$ ne soit du premier degré en x.

Ainsi une équation irréductible de degré premier ne peut devenir réductible, à moins que son groupe ne se réduise à une seule permutation.

PROPOSITION VII.

Problème. Quel est le groupe d'une équation irréductible d'un degré premier n, soluble par radicaux?

D'après la proposition précédente, le plus petit groupe possible avant celui qui n'a qu'une seule permutation, contiendra n permutations. Or un groupe de permutations d'un nombre premier n de lettres ne peut se réduire à n permutations, à moins que l'une de ces permu-

tations ne se déduise de l'autre par une substitution circulaire de l'ordre n. (Voir le Mémoire de M. Cauchy, *Journal de l'École Polytechnique*, XVII^e cahier.) Ainsi l'avant-dernier groupe sera

$$(G)\qquad \begin{array}{|cccccc|} \hline x_0 & x_1 & x_2 & x_3 & \dots & x_{n-1} \\ x_1 & x_2 & x_3 & x_4 & \dots & x_0 \\ x_2 & x_3 & \dots & \dots & x_{n-1} & x_0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ x_{n-1} & x_0 & x_1 & \dots & \dots & x_{n-2} \\ \hline \end{array}$$

$x_0, x_1, x_2, \dots, x_{n-1}$ étant les racines.

Maintenant, le groupe qui précédera immédiatement celui-ci dans l'ordre des décompositions devra se composer d'un certain nombre de groupes ayant tous les mêmes substitutions que celui-ci. Or, j'observe que ces substitutions peuvent s'exprimer ainsi. (Faisons en général $x_n = x_0, x_{n+1} = x_1, \dots$, il est clair que chacune des substitutions du groupe (G) s'obtient en mettant partout à la place de x_k, x_{k+c} c étant une constante.)

Considérons l'un quelconque des groupes semblables au groupe (G). D'après le Théorème II, il devra s'obtenir en opérant partout dans ce groupe une même substitution; par exemple, en mettant partout dans le groupe (G), à la place de x_k, x_{k+c}, f étant une certaine fonction.

Les substitutions de ces nouveaux groupes devant être les mêmes que celles du groupe (G), on devra avoir

$$f(k+c) = f(k) + C,$$

C étant indépendant de k.

Donc

$$\begin{aligned} f(k+2c) &= f(k) + 2C, \\ &\dots\dots\dots\dots\dots \\ f(k+mc) &= f(k) + mC. \end{aligned}$$

Si $c = 1$, $k = 0$, on trouvera

$$f(m) = am + b,$$

ou bien

$$f(k) = ak + b,$$

a et b étant des constantes.

Comme ceci :

[redacted]

Donc le groupe qui précède immédiatement le groupe (G), ne devra contenir que des substitutions telles que

$$x_k,\ x_{ak+b};$$

et ne contiendra pas, par conséquent, d'autre substitution circulaire que celle du groupe (G).

On rencontrera sur ce groupe comme sur le précédent, et il s'ensuivra que le premier groupe dans l'ordre des décompositions, c'est-à-dire le groupe *actuel* de l'équation, ne peut contenir que des substitutions de la forme

$$x_k,\ x_{ak+b}.$$

Donc, « si une équation irréductible de degré premier est soluble par radicaux, le groupe de cette équation ne saurait contenir que des substitutions de la forme

$$x_k,\ x_{ak+b},$$

a et b étant des constantes. »

Réciproquement, si cette condition a lieu, je dis que l'équation sera soluble par radicaux. Considérons en effet les fonctions

$$\begin{aligned} (x_0 + \alpha x_1 + \alpha^2 x_2 + \dots\dots + \alpha^{n-1} x_{n-1})^n &= X_1, \\ (x_0 + \alpha x_2 + \alpha^2 x_4 + \dots\dots + \alpha^{n-1} x_{n-2})^n &= X_2, \\ (x_0 + \alpha x_3 + \alpha^2 x_6 + \dots\dots + \alpha^{n-1} x_{n-3})^n &= X_3, \end{aligned}$$

α étant une racine $n^{ième}$ de l'unité, n une racine primitive de n.

Il est clair que toute fonction invariable par les substitutions circulaires des quantités $X_1, X_2, X_3, \dots$ sera, dans ce cas, immédiatement connue. Donc on pourra trouver $X_1, X_2, X_3, \dots$, par la méthode de M. Gauss pour les équations binômes. Donc, etc.

Ainsi, pour qu'une équation irréductible de degré premier soit soluble par radicaux, il *faut* et il *suffit* que toute fonction invariable par les substitutions

$$x_k,\ x_{ak+b}$$

soit rationnellement connue.

Ainsi la fonction

$$(X_1 - X)(X_2 - X)(X_3 - X)\ldots$$

devra, quelque soit X, être connue.

Il *faut* donc et il *suffit* que l'équation qui donne cette fonction des racines, admette, quel que soit X, une valeur rationnelle.

Si l'équation proposée a tous ses coefficients rationnels, l'équation auxiliaire qui donne cette fonction les aura tous aussi, et il suffira de reconnaître si cette équation auxiliaire du degré $1.2.3\ldots(n-2)$ a ou non une racine rationnelle, ce que l'on sait faire.

C'est là le moyen qu'il faudrait employer dans la pratique. Mais nous allons présenter le théorème sous une autre forme.

PROPOSITION VIII.

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

Premièrement, il le faut, car la substitution

$$x_1,\ x_{ak+b}$$

ne laissant jamais deux lettres à la même place, il est clair qu'en adjoignant deux racines à l'équation, par la proposition IV, son groupe devra se réduire à une seule permutation.

En second lieu, cela suffit; car, dans ce cas, aucune substitution du groupe ne laissera deux lettres aux mêmes places. Par conséquent, le groupe contiendra tout au plus $n(n-1)$ permutations. Donc, il ne contiendra qu'une seule substitution circulaire (sans quoi il y aurait au moins p^2 permutations). Donc, toute substitution du groupe x_1, x_k devra satisfaire à la condition

$$f(k+c) = fk + c.$$

Donc, etc.

Le théorème est donc démontré.

Exemple du Théorème VII.

Soit $n = 5$; le groupe sera le suivant :

abcde
bcdea
cdeab
deabc
eabcd
———
acebd
cebda
ebdac
bdace
daceb
———
aedcb
edcba
dcbae
cbaed
baedc
———
adbec
dbeca
becad
ecadb
cadbe.

~~Ensuite~~ [redacted]

(**) Désignons par $\psi(V)=0$ l'équation en V dont il est parlé, et soient $f(V,r)$, $f_1(V,r) \ldots f_{i-1}(V,r)$ les facteurs irréductibles dans lesquels $\psi(V)$ devient décomposable par l'adjonction de r, en sorte que 36

$$\psi(V) = f(V,r)\, f_1(V,r) \ldots f_{i-1}(V,r).$$

Comme [redacted] r est racine d'une équation irréductible, on pourra dans le second membre remplacer r par r', r'', … $r^{(p-1)}$. [redacted] $\psi(V)^p$ est le produit des i quantités suivantes

$$f(V,r)\, f(V,r') \ldots f(V,r^{(p-1)})$$

$$f_1(V,r)\, f_1(V,r') \ldots f_1(V,r^{(p-1)})$$

$$\text{— — — — —}$$

$$f_{i-1}(V,r)\, f_{i-1}(V,r') \ldots f_{i-1}(V,r^{(p-1)})$$

dont chacune symétrique en $r, r', \ldots r^{(p-1)}$ [redacted] par conséquent ~~est~~ fonction rationnelle [redacted] par toute adjonction doit ~~être~~ indépendamment de toute adjonction, doit diviser $\psi(V)^p$ et se réduire en conséquence à une puissance du polynôme $\psi(V)$ qui est le [?] ... les facteurs lorsqu'on [redacted] les adjonctions r, r', &c. Supposons que le degré de la puissance est le même pour toutes; en effet les équations $f(V,r)=0$, $f_1(V,r)=0 \ldots f_{i-1}(V,r)=0$ qui sont issues de $\psi(V)=0$ et dont les racines ~~sont fonctions~~ rationnelles les unes des autres ne peuvent être ~~changer~~ d'un de même degré. Il faudra donc

$$f(V,r)\, f(V,r') \ldots f(V,r^{(p-1)}) = \psi(V)^{\mu}$$

on en conclura $p = i\mu$. Mais p est premier et $i>1$, donc on a $i=p$, d'où $\mu=1$, et ~~enfin~~

$$\psi(V) = f(V,r)\, f(V,r') \ldots f(V,r^{(p-1)}).$$

[redacted] ce qu'il fallait démontrer. (~~[illegible]~~)

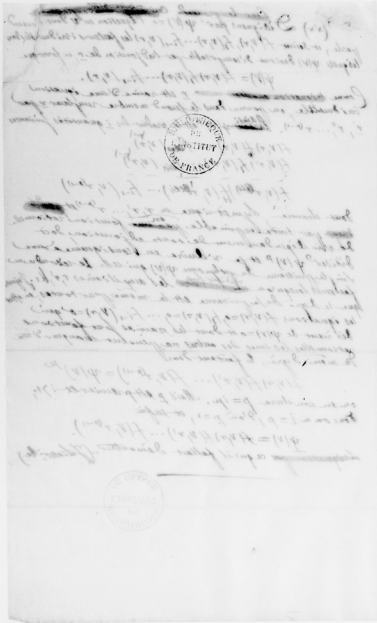
Bertrand feuilles 27

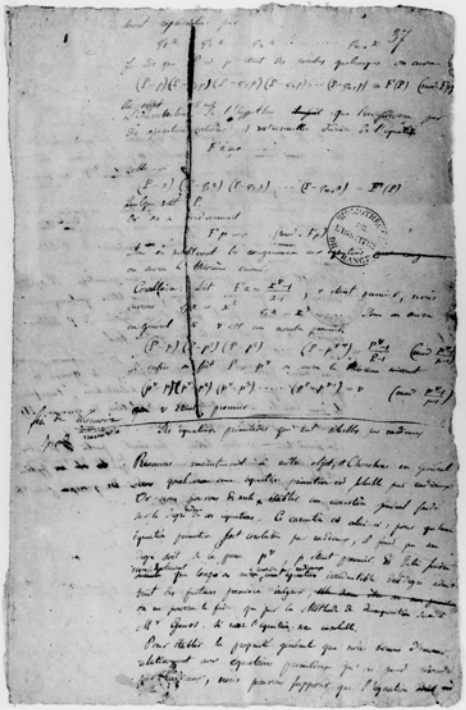
36 bis

4

Des équations primitives qui sont
solubles par radicaux.
(Journ. de M).

Texte de Galois.





tout exposant fini

$g^x \quad g_1^x \quad g_2^x \quad \dots \quad g_{n-2}^x$

Je dis que $P = p$ étant des nombres quelconques on aura

$(P-1)(P-g_1)(P-g_2)(P-g_3)\dots(P-g_{n-2}) = F(P) \pmod{F p}$

En effet la démonstration de l'hypothèse suppose que les fonctions par des quantités entières il naturellement lieu à l'équation

$F x = 0$

dont les racines sont

$(P-x)(P-g_1 x)(P-g_2 x)\dots(P-g_{n-2} x) = F'(P)$

Lorsque $x = 1$

Or on a évidemment

$F p = 0 \pmod{F p}$

Donc en substituant la congruence ci-dessus on aura le théorème énoncé.

Corollaire. Soit $F x = \frac{x^\nu - 1}{x-1}$, ν étant premier, nous aurons $g x = x^1$ $g_1 x = x^2$ $\dots$ Donc on aura en général si ν est un nombre premier

$(P-1)(P-p^1)(P-p^2)\dots(P-p^{\nu-2}) = \frac{P^\nu - 1}{P-1} \pmod{\frac{p^\nu - 1}{p-1}}$

Si enfin on fait $P = p^\nu$ on aura le théorème suivant

$(p^\nu - 1)(p^\nu - p^1)(p^\nu - p^2)\dots(p^\nu - p^{\nu-2}) = \nu \pmod{\frac{p^\nu - 1}{p-1}}$

ν étant premier.

Des équations primitives qui sont résolubles par radicaux

Reprenons maintenant notre objet, et cherchons en général quelle sera une équation primitive résoluble par radicaux. Or nous avons établi un caractère général fondé sur la forme de ses racines. Ce caractère est celui-ci : pour qu'une équation primitive soit résoluble par radicaux, il faut que son degré soit de la forme p^ν, p étant premier. Si cette forme n'appartient pas au degré d'une équation irréductible, le degré de toutes les fonctions primitives inégales, elle ne peut se résoudre que par la méthode de transformation de M^r Gauss. Si non l'équation est irrésoluble.

Pour établir la propriété générale que nous venons d'énoncer relativement aux équations primitives qui se peuvent résoudre par radicaux, nous pouvons supposer que l'équation

$a_{10}\ a_{11}\ a_{12}\ a_{13}\ \dots\ a_{1,p-1}$

P lettres conjointes toutes obtenues dans la seconde colonne verticale, excepté celle qui a

$a_{20}\ a_{21}\ a_{22}\ a_{23}\ \dots\ a_{2,p-1}$

appartiennent respectivement aux colonnes ligne horizontale formée

$a_{00}\ a_{01}\ a_{02}\ a_{03}\ \dots\ a_{0,p-1}$

avec l'ordre de la même système de lettres conjointes

$a_{00}\ a_{01}\ a_{02}\ a_{03}\ \dots\ a_{0,p-1}$

$a_{10}\ a_{11}\ a_{12}\ a_{13}\ \dots\ a_{1,p-1}$

$a_{20}\ a_{21}\ a_{22}\ a_{23}\ \dots\ a_{2,p-1}$

$\dots\ \dots\ \dots\ \dots\ \dots\ \dots$

$a\ \ \ \ \ \ \ \ \ \ a_{p-1,p-1}$

Nous désignerons cet ensemble de p^2 lettres conjointes par le symbole (a), et nous désignerons une quelconque de ces lettres par $a_{\alpha\beta}$, α et β étant deux entiers inférieurs à p, de sorte que

$a_{00}, a_{01}, a_{02}, a_{03}, \dots, a_{0,p-1}$

$a_{10}, a_{11}, a_{12}, a_{13}, \dots, a_{1,p-1}$

$a_{20}, a_{21}, a_{22}, a_{23}, \dots, a_{2,p-1}$

$\dots\ \dots\ \dots\ \dots\ \dots\ \dots$

$a_{p-1,0}, a_{p-1,1}, a_{p-1,2}, a_{p-1,3}, \dots, a_{p-1,p-1}$

Soit en général un système de n lettres conjointes. Si l'on remarque que n est au plus égal à p^2, on pourra toujours poser $N = p^2 - n$, N étant un entier positif ou nul. Désignons par $\alpha, \beta, \gamma, \dots \lambda$ des indices qui peuvent prendre chacun les p valeurs $0, 1, 2, 3, \dots p-1$. Le système de n lettres conjointes pourra être représenté par

$$a_{\alpha,\beta}, a_{\gamma,\delta}, a_{\varepsilon,\zeta}, \dots a_{\kappa,\lambda}$$

$\alpha, \beta, \gamma, \delta, \dots \kappa, \lambda$ étant $2n$ indices qui peuvent prendre chacun les p valeurs $0, 1, 2, 3, \dots p-1$. Le système de n lettres conjointes pourra être représenté par $a_{\alpha,\beta}, a_{\gamma,\delta}, a_{\varepsilon,\zeta}, \dots a_{\kappa,\lambda}$, étant entendu que, dans le groupe H, toutes les substitutions faisant sortir de la forme

$$\left(a_{\alpha,\beta}, a_{\gamma,\delta}, a_{\varepsilon,\zeta}, \dots a_{\kappa,\lambda}\right)$$

puissent changer tous les indices chacun à chacun en des fonctions linéaires entières de $x, y, z, \dots t$, à coefficients entiers pris suivant le module p.

Chaque substitution du groupe H correspond à un système de p^2 lettres conjointes.

Si P n'est pas un nombre premier, on démontrera aisément que le groupe H peut se décomposer en P groupes partiels $H_1, H_2, \dots H_P$, tels que H_1 soit un groupe holoédrique isomorphe au groupe G_1 des substitutions linéaires entières à coefficients entiers pris suivant le module p, H_2 un groupe holoédrique isomorphe au groupe G_2 des substitutions linéaires entières à coefficients entiers pris suivant le module p, $\dots$ H_P un groupe holoédrique isomorphe au groupe G_P des substitutions linéaires entières à coefficients entiers pris suivant le module p.

Si $P = R^A$, et ainsi de suite, R étant un nombre premier.

Si l'on sait résoudre, soit générale, soit particulière, une équation d'un degré premier, on sait résoudre [illegible] équation d'un degré quelconque.

En d'autres termes, nous pouvons supposer que N est premier, le groupe de l'équation se partage en n groupes conjugués, mais non primitifs. Car si le groupe de l'équation fût primitif, un pareil groupe ne pourrait exister dans le fait de l'impossibilité.

Soit N le degré de l'équation, si supposons qu'après une opération de degré moindre que N, elle devienne une primitive, et se partage en Q équations primitives du degré P, au moyen d'une seule équation de degré Q.

Si nous appelons G le groupe de l'équation, ce groupe devra se partager en n groupes conjugués non-primitifs, dans lesquels les lettres se trouvent rangées en systèmes composés de P lettres conjointes chacun. Voyons d'abord de manière à pouvoir s'en servir plus tard.

1° Il n'est pas possible que deux lettres quelconques soient à volonté faites partie d'un même système de P lettres conjointes, à moins qu'elles ne fassent partie que d'un seul.

Car si cela était, deux lettres qui ne peuvent faire partie d'un même système de P lettres conjointes, le groupe G qui est tel que l'une quelconque de ses substitutions, transforme l'une dans l'autre toutes les substitutions du groupe H, serait non-primitif : ce qui est contre l'hypothèse.

En second lieu, si deux lettres faisaient partie de plusieurs systèmes conjoints, il s'ensuivrait que [illegible] de toutes les lettres conjointes ne pourraient pas à de groupe primitif, ce qui est encore contre l'hypothèse.

Cela posé, soient

$$\begin{matrix} a_0 & a_1 & a_2 & \dots & a_{P-1} \\ b_0 & b_1 & b_2 & \dots & b_{P-1} \\ c_0 & c_1 & c_2 & \dots & c_{P-1} \end{matrix}$$

Les N lettres : supposons que chaque ligne horizontale représente un système de lettres conjointes : soient

$$a_0 \quad a_{0.1} \quad a_{0.2} \quad \dots \quad a_{0.P-1}$$

P lettres conjointes toutes situées dans la première colonne verticale (il est clair que nous pouvons faire qu'il en soit ainsi, en intervertissant seul l'ordre des lignes horizontales).

Soit α une

$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$ ... $a_{1,p-1}$

p lettres conjuguées toutes obtenues dans la seule classe notable ~~ainsi~~ avec que =

$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$ ... $a_{1,p-1}$

appartiennent respectivement au même type hexadécimal que

$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$ ... $a_{0,p-1}$

sont toutes les ~~lignes~~ systèmes de lettres conjuguées

$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$ ... $a_{2,p-1}$

$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$ ... $a_{3,p-1}$

...

α

Nous obtenons ainsi en tout p^n lettres à l'exclusion tout de lettres ~~n~~ pour lequel, on prendra toutes indices, on fait que

$a_{m,n,0}$ $a_{m,n,1}$ $a_{m,n,2}$ $a_{m,n,3}$ ... $a_{m,n,p-1}$

fait en général un système de lettres conjuguées. Et la première ainsi à cette conclusion que $N = P^{\mu}$, μ étant un certain nombre égal à celui des indices différents dont on entre en besoin. La forme générale des lettres sera

$$a_{k_1, k_2, k_3, \ldots k_\mu}$$

$k_1, k_{2,1}, k_{3,1}, \ldots k_\mu$ étant des indices qui peuvent prendre chacun les p valeurs $0, 1, 2, 3 \ldots p-1$

On voit aussi que dans le groupe H, toutes les substitutions seront de la forme

$$\left(a_{k_1, k_2, k_3 \ldots k_\mu} \right) \; a_{\varphi(k_1), \psi(k_2), \chi(k_3), \ldots \sigma(k_\mu)}$$

puisque ~~chaque indice obtient chaque système conjugué à celui~~ chaque indice correspond à un système de lettres conjuguées.

Si P n'est pas un nombre premier, on raisonnera sur le groupe de permutations de l'un quelconque des systèmes de lettres conjuguées, comme sur le groupe G, et l'on trouvera $P = R^{\alpha}$ et ainsi de suite, d'où enfin $N = p^{\nu}$, p étant un nombre premier.

Après avoir désigné chaque indice par un entier à plusieurs chiffres

un nombre premier

On voit qu'alors cette question pourra dans la pratique se décomposer pour arriver à un groupe intransitif dont les substitutions seront toutes impossibles comme il faut.

Des Equations primitives de degré p^2.

$\left(a_{\alpha,\beta}, a_{\alpha+\gamma,\beta+\delta}\right)$

Les x et y étant pris relativement au module p, et $\alpha, \beta, \gamma, \delta$ des nombres entiers.

Nous allons chercher maintenant quelles peuvent être les substitutions d'un groupe primitif qui appartient à une équation résoluble par radicaux. Les Equations

Cherchons-nous en premier, pour classer par degrés de simplicité les équations, à trouver d'abord la équation primitive de degré p^2 résoluble par radicaux, p étant premier impair. (Le cas $p=2$ étant connu)

Si une équation de degré p^2 est résoluble par radicaux, supposons d'abord qu'elle soit, qu'elle devienne non primitive par l'extraction d'un radical.

Soit donc G le groupe primitif de p^2 lettres qui la possède, ou le groupe non primitif conjugué à H.

Les lettres devront nécessairement, dans le groupe H, se ranger ainsi,

$$\begin{array}{ccccccc} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} & \cdots & a_{0,p-1} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} & \cdots & a_{1,p-1} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} & \cdots & a_{2,p-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{p-1,0} & a_{p-1,1} & a_{p-1,2} & a_{p-1,3} & \cdots & a_{p-1,p-1} \end{array}$$

Chaque ligne horizontale et chaque ligne verticale étant un système de lettres conjuguées.

Si l'on permute entre elles les lignes horizontales le groupe de la substitution reste le même et le degré premier, on aura toutes les substitutions de la forme

$$\left(a_{\alpha,\beta}, a_{m\alpha+n,\beta}\right)$$

Les indices étant pris relativement au module p.

Il en sera de même pour les lignes verticales, qui ne pourront donner que des substitutions de la forme

$$\left(a_{\alpha,\beta}, a_{\alpha,q\beta+r}\right)$$

Donc enfin toutes les substitutions du groupe H seront de la forme

$$\left(a_{\alpha,\beta}, a_{m\alpha+n,\, m\beta+q}\right)$$

Si un groupe G de perdre ou a groupe conjugué à lui-même
que nous nous avons à écrire, toutes les substitutions du groupe G
devant transformer [illegible] dans [illegible] les substitutions semblables
du groupe H qui sont toutes écrites comme il suit

$$\left(\begin{matrix} x_1 & x_2 & x_3 & \dots & x_p \\ x_1 & x_2 & x_3 & \dots & x_p \end{matrix} \quad \begin{matrix} x_1 & x_2 & x_3 & \dots & x_p \\ x_2 & x_3 & x_4 & \dots & x_1 \end{matrix} \quad \dots \right) \qquad (A)$$

Supposons donc que l'une des substitutions du groupe G [illegible]
se forme en remplaçant respectivement

x_1 par $\varphi_1(x_1, x_2)$
x_2 par $\varphi_2(x_1, x_2)$
[illegible]
x_p par $\varphi_p(x_1, x_2, \dots, x_p)$

Si dans les fonctions φ_1 φ_2 [illegible] on substitue pour x_1 et x_2 [illegible]
les valeurs x_1+y, x_1+z [illegible] il devra venir des résultats de la forme

$$\varphi_1 + b_1 \qquad \varphi_2 + b_2$$

et de là il est aisé de conclure immédiatement que la substitution du groupe G devant être toutes conjuguées dans le premier

$$\left(\begin{matrix} x_1 & x_2 & \dots \\ x_1 & x_2 & \dots \end{matrix} \quad \begin{matrix} x_1 & x_2 & \dots \\ x_1+\alpha & x_2+\alpha & \dots \end{matrix} \right) \qquad (A)$$

Or nous avons vu au n° [illegible] que les substitutions du
groupe G ne peuvent contenir que p^2-1 ou p^2-p
lettres. Il en faut donc p^2-p, puisque le groupe G devient
non primitif si dans le groupe G on [illegible] ne considère
[illegible] que les substitutions où la lettre x_1 est [illegible] conservée
restent toujours la même place, on n'aura que des substitutions
de l'ordre p^2-1 entre les p^2-1 autres lettres.

Mais rappelons-nous ici que [illegible] n'est simplement pour la
démonstration que nous avons supposé que le groupe primitif
se partageât en groupes conjugués non-primitifs. [illegible] Comme
cette condition n'est nullement [illegible] les groupes
devant devenir beaucoup plus compliqués.

Il s'agit donc de rechercher dans quel cas les groupes
peuvent admettre des substitutions où p^2-p lettres
seulement varieraient, et cette recherche va nous

obtenir quelque chose.

Soit donc G un groupe qui contient quelque substitution de l'ordre $p^2 - p$, mais qui ne contient pas de groupe conjugué d'ordre p, et supposons que ce groupe conjugué ne contienne que de pareilles substitutions. Nous prouverons d'abord que toutes les substitutions de ce groupe sont linéaires, ou à peu près de la forme

(A) $\quad x_0' \equiv \alpha x_0 + \beta x_1 + \gamma, \quad x_1' \equiv \alpha' x_0 + \beta' x_1 + \gamma' \pmod p$

La chose est vraie pour les substitutions d'ordre $p^2 - 1$.

Il faut bien de la compter pour celles d'ordre $p^2 - p$.

Ces substitutions donnent ou bien le substitutions groupe où les substitutions soient entre elles de l'ordre p^2 ou de l'ordre $p^2 - p$. (Voyez Vandermonde).

Alors les p lettres qui dans une substitution de l'ordre $p^2 - p$ se varient pas, doivent être des lettres conjuguées. Supposons que substitution conjuguée soit

$$a_{0,0} \quad a_{0,1} \quad a_{0,2} \quad \ldots \quad a_{0,p-1}$$

Cela posé, il y aura autant de substitutions de l'ordre $p^2 - p$ dont le premier est $a_{0,0}$ que

il y a de manières de prendre parmi les p lettres restantes p lettres différentes de $a_{0,0}$, c'est-à-dire $p(p-1)\ldots 2$. Ces substitutions sont toutes de la forme

$$\left(a_{0,0} \quad a_{m_1,n_1} \quad a_{m_2,n_2} \quad \ldots\right)$$

Si maintenant il y avait des substitutions d'ordre $p^2 - p$ dont le premier est $a_{0,0}$ aussi, elles seraient de la forme

$$\left(a_{0,0} \quad a_{m_1',n_1'} \quad a_{m_2',n_2'} \quad \ldots\right)$$

Nous prouvons d'abord que toutes les substitutions où p lettres ne changent pas de place, nous prouvons les substitutions de la forme

$$\left(a_{k,x} \quad a_{k,\varphi x}\right)$$

Si la substitution d'ordre $p^2 - p$ est de première espèce (Voyez ce qu'on a dit ci-dessus), les premières doivent nécessairement, pour que le groupe jouisse de la propriété voulue, se réduire à la forme

$$\left(a_{k,x} \quad a_{k,mx}\right)$$

D'après ce qu'on a vu pour les équations d'ordre p.

Quant aux substitutions dont le premier est $a_{0,2}$ et dont nous avons reconnu plus haut comme elles sont conjuguées aux précédentes, nous prouverons également que le groupe qui les contient ne contient que celles-ci. Car elles devront transformer les substitutions circulaires et leurs

[illegible] de ces autres. De cette sorte [illegible] [illegible] être [illegible] des [illegible] il est [illegible] à le groupe primitif de permutations de p^2 lettres qui ne contient que des substitutions de la forme (a).

Maintenant, prenons le groupe total que l'on obtient en posant sur l'expression

$$a_{k_1,k_2}$$

toutes les substitutions linéaires possibles, ~~qui sont au nombre de $p^2(p^2-1)(p^2-p)$~~, et cherchons quels sont les diviseurs de ce groupe qui peuvent jouir de la propriété voulue pour la résolubilité des équations.

~~Et d'abord~~ ~~~~ Et d'abord le nombre total des substitutions linéaires *. Premièrement, il est clair que toute transformation de la forme

$$k_1\ k_2 \qquad m k_1 + n k_2 + \alpha_1,\ m_1 k_1 + n_1 k_2 + \alpha_2$$

ne sera pas pour cela une substitution, car il faut dans une substitution qu'à chaque lettre de la première permutation il ne réponde qu'une seule lettre de la seconde et réciproquement. Si donc on prend une lettre quelconque a_{l_1,l_2} de la seconde permutation, et que l'on veuille remonter à la lettre correspondante dans la première, on devra trouver une lettre a_{k_1,k_2} où les indices k_1, k_2 soient parfaitement déterminés. Il faut donc ~~que quelque~~ que quelles que soient l_1 et l_2 on ait par les deux équations

$$m_1 k_1 + n_1 k_2 + \alpha_1 = l_1, \qquad m_2 k_1 + n_2 k_2 + \alpha_2 = l_2$$

des valeurs de k_1 et k_2 finies et déterminées. ~~[illegible]~~ La condition pour qu'une pareille transformation soit réellement une substitution est que $m_1 n_2 - m_2 n_1$ ne soit ni nul ni divisible par le module p, ce qui est la même chose.

Considérons maintenant que les substitutions linéaires où la lettre $a_{0,0}$ ne varie pas, nous trouverons le nombre total des permutations du groupe ~~[illegible]~~ qui contient toutes les substitutions linéaires possibles, il nous suffira de multiplier ce nombre par p^2.

Or premièrement, en supposant que l'indice k_2 ne varie pas ~~[illegible]~~, toutes les substitutions de la forme

$$\left(a_{k_1,k_2} \quad a_{m_1 k_1, k_2}\right)$$

donneront en tout $p-1$ substitutions. On ajoutera de plus au terme k_2 le terme $n_2 k_1$ ainsi qu'il faut

* Nous montrerons que bien que ce groupe de substitutions linéaires n'appartienne ~~[illegible]~~ pas toujours, comme on le verra, à des équations solubles par radicaux, il jouit ~~[illegible]~~ toutefois de cette propriété, que si dans une de ses substitutions il y a n lettres de fixes, n divisera le nombre des lettres. Et en effet, quelque soit le nombre des lettres qui restent fixes, on pourra exprimer cette circonstance par ~~[illegible]~~ ~~[illegible]~~ d'équations linéaires, qui donneront toutes les indices des lettres fixes ~~[illegible]~~ un certain nombre ~~[illegible]~~ d'indices, donnant à chacun de ces indices toutes ses p valeurs, on aura p^n systèmes de valeurs, ce nombre étant un certain nombre. Dans le cas qui nous occupe il est évidemment [illegible]. Il est par conséquent 0 ou 1. Donc le nombre des ~~[illegible]~~ substitutions ne saurait être plus grand que $p^2(p^2-1)(p^2-p)$

$(k_1 k_2 \; , \; m_1 k_1 + n_1 k_2 + k_1 \; , \; m_2 k_1 + n_2 k_2 + k_2)$ (m)

[illegible] chacune des substitutions (k) et appelé [illegible]

D'un autre côté, il est aisé de trouver un groupe de p^2-1 permutations tel que dans chacune de ses substitutions toutes les lettres à l'exception de a_{00} varient. Car en remplaçant pour le double indice $k_1 . k_2$ par l'indice simple $k_1 + ik_2$ i étant une racine primitive de la congruence

$$x^{p^2-1} - 1 = 0 \pmod p$$

il est clair que toute substitution de la forme

$$\left(k_1 + k_2 i \;\; , \;\; a(m_1 + m_2 i) + (k_1 + k_2 i) \right)$$

est une substitution linéaire ; mais dans ces substitutions aucune lettre ne reste à la même place, et elles sont au nombre de p^2-1. Nous avons donc un système de p^2-1 permutations tel que dans chacune de ses substitutions toutes les lettres varient à l'exception de a_{00}. Combinons ces substitutions avec les $p^2 p$ dont il est parlé plus haut nous aurons

$(p^2-1)(p^2-p)$ substitutions

Or nous avons vu à priori que le nombre des substitutions ne pouvait être plus grand que $(p^2-1)(p^2-p)$. Donc il est précisément égal à $(p^2-1)(p^2-p)$, et le groupe linéaire total aura autant

$$p^2 (p^2-1)(p^2-p)$$

Permutations. Il reste à chercher les divisions de ce groupe qui jouent pour lui la propriété d'être semblable par isomorphisme. Pour cela nous allons faire une transformation qui a pour but d'obtenir autant que possible les équations primitives de degré p^2 dont le groupe soit linéaire.

Premièrement comme les substitutions [illegible] forment un groupe tel que toute substitution [illegible] le transforme lui-même en autres de même nature, l'équation [illegible] de degré p^2 dont le groupe est linéaire, et contient [illegible] l'équation [illegible] le groupe n'aura pour substitutions que les substitutions de la forme

$$\left(k_1 k_2 \;\; , \;\; b_{m_1 k_1 + n_1 k_2} \;\; , \;\; m_2 k_1 + n_2 k_2 + k_2 \right)$$

5

Les $p+2$ lettres sont

$$\begin{matrix} b_{0,1} & b_{0,1} & b_{0,2} & \dots \\ b_{1,0} & b_{1,1} & b_{1,2} & \dots \\ b_{2,0} & b_{2,1} & b_{2,2} & \dots \end{matrix}$$

J'observe maintenant que ce groupe est un primitif, parce que toutes les lettres où le rapport des deux indices est le même, sont des lettres conjointes. En effet toutes ces lettres étant remplacées par une seule lettre chaque système de lettres conjointes on aura un groupe de la forme dont toutes les substitutions sont de la forme

$$\left(b_{\frac{K_1}{K_2}} \; , \; b_{\frac{n_1 K_1 + n_2 K_2}{n_2 K_1 + n_3 K_2}} \right)$$

$\frac{K_1}{K_2}$ étant la nouvelle indice de remplacement a rapport par $\frac{K_1}{K_2}$ une seule lettre K, ce qui que les $p+1$ lettres sont

$$b_0 \quad b_1 \quad b_2 \quad b_3 \quad \dots \quad b_{p-1} \quad b_\infty$$

et les substitutions sont de la forme

$$\left(K \; , \; \frac{nK+n}{rK+s} \right)$$

Il cherche à combien d'ordre sont chacune de ces substitutions, mais à la même place ; il faut pour cela résoudre l'équation

$$(rK+s)K - (nK+n) = 0$$

qui aura deux racines, excepté que $(n-s)^2 + 4nr$ sera réduit quadratique, nul, ou non réduit quadratique, suivant ces cas on la substitution sera de l'ordre le plus grand ou le plus petit pour deux des deux premières ou les substitutions de la forme

$$(K \; , \; nK+n)$$

où la sub lettre b_K ne varie pas. [illegible] qui contiendrait des substitutions de l'ordre p, pourvu [illegible] dans ce cas, il faudrait d'après l'équation voulu précédemment. Mais elle ne pourrait être plus [illegible] que lorsque $p+1 = 2^n$, ce qui est un cas particulier.

Nous pouvons supposer que le groupe ne contient que des substitutions de l'ordre p et 2 l'ordre $2p+1$. Toutes les substitutions d'ordre p [illegible]

* Il est clair qu'avec le mode de substitutions du groupe réduit est $(p+1)p(p-1)$.

Premier Cas. Equation

$$\left(K\ ,\ \frac{mk+n}{k+1}\right)$$

Il reste donc quelle est celle substitution qui doit avoir un pareil diviseur. Il faut pour cela que la substitution soit conjointe avec elle. La substitution inverse est

$$\left(K\ ,\ \frac{-1K+n}{+K-m}\right)$$

Donc on doit avoir $m=-1$, et toute substitution conjointe devra être de la forme

$$\left(K\ ,\ \frac{nK+n}{K-n}\right)$$

ou encore

$$\left(K\ ,\ n+\frac{N}{K-n}\right)$$

Il reste une certaine manière de voir ces substitutions. Or ces substitutions devront diviser [illegible] comme [illegible] pour former le coefficient [illegible]

[illegible] $\frac{N}{K-n}$

[illegible] que n est une racine [illegible] n est une racine primitive. 2° elle devient la conjointe de deux autres. Soient

$$\left(K\ ,\ n+\frac{N}{K-n}\right) \qquad \left(K\ ,\ n+\frac{N'}{K-n}\right)$$

deux substitutions, il faut que l'on ait

$$n+\frac{N}{K-n}+n-n = n+\frac{N'}{K-n}+n-n$$

ou $(n-n)^2 = N$.

Donc la différence entre deux valeurs de n ne peut acquérir que deux valeurs différentes. Donc K ne peut avoir plus de deux valeurs. Donc enfin $p=2$. Ainsi ce seulement dans ce cas que le groupe étant premier [illegible] les substitutions de l'ordre p.

Et en effet le résultat nous donne $\frac{p-1}{2}$ [illegible] pour chaque valeur par exemple

Mais réciproquement [illegible] pour que les substitutions [illegible] [illegible] il faut et il suffit que [illegible] soit [illegible] Or puisque [illegible] il ne reste que à trouver [illegible] substitutions de l'ordre p. Peut-il y en avoir d'autres ? C'est que je vais rechercher et je [illegible]

Il [illegible] le même pour toutes les substitutions, puisque en [illegible] une substitution donnée on [illegible] les mêmes [illegible] que toutes les autres par toutes les substitutions de [illegible]

$(K,\ K+n)$ [illegible]

5

Des équations primitives
qui sont solubles par radicaux
(Copie par Chevalier)

Second mémoire

Des équations primitives qui sont solubles par radicaux.

Cherchons en général dans quel cas une équation primitive est abaissable par Abel ; on nous pourrons par la suite établir un caractère général fondé sur le Degré même de cette équation. ce caractère est celui-ci : pour qu'une équation primitive soit abaissable par Abel, il faut que son Degré soit de la forme $p^{\alpha}.q^{\beta}$ etant premier. et de la sorte l'équation résultante que Lagrange aura à résoudre par Abel, [illegible] sera abaissable. une équation irréductible dont le Degré démontrait d'un facteurs premiers inégaux, on ne pourra la faire voir par la méthode de Décomposition due à Mr Gauss. d'une équation sera irréductible.

Pour établir la propriété générale que nous venons d'énoncer relativement aux équations primitives qu'on peut résoudre par radicaux, nous pouvons supposer que l'équation que l'on veut résoudre, soit primitive, mais cela résulte par la définition d'une simple Abel. En effet en effet nous pouvons supposer que ne soit pas primitive, le groupe de l'équation de partage en 2 groupes irréductibles conjugués, mais non primitifs. car à moins que le Degré de l'équation soit premier, un pareil groupe de substitutions existe dans la théorie de décomposition.

Soit θ le Degré de l'équation, et supposons qu'après une infinité de radicaux de Degrés premiers, elle devienne non primitive, et se partage en θ équations primitives du Degré 1, on suppose donc toute équation d'Degré Q.

Si nous appelons G le groupe de l'équation, ce groupe pourra se partager en θ groupes conjugués non primitifs, donc laquelle les lettres de rang quelconque en hypothèse composée de I lettres conjuguées chacun. Donc de combien de manières cela pourra se faire.

Soit H l'un des groupes conjugués non primitifs. il est aisé de voir que dans ce groupe, deux lettres quelconques prises à volonté feront partie d'un certain hypothèse de I lettres conjuguées, et ne feront partie que d'une seule.

Car il est évident deux lettres qui ne pourront faire partie d'une même hypothèse de P lettres conjuguées, le groupe G qui est tel que la substitution quelconque de ses lettres transforme les unes dans les autres toutes les lettres du groupe H seront non primitif ; ce qui est contre l'hypothèse.

En second lieu, si deux lettres faisaient partie de plusieurs hypothèses différentes, il s'ensuivrait que les groupes qui répondent aux divers hypothèses de I lettres conjuguées ne seraient pas primitifs : ce qui est encore contre l'hypothèse.

414.

ala puissance, soient $a_0\ a_1\ a_2 \ldots\ a_{p-1}$

$b_0\ b_1\ b_2 \ldots\ b_{p-1}$

$c_0\ c_1\ c_2 \ldots\ c_{p-1}$

Les N lettres supposons que chaque ligne horizontale, représente un système de lettres conjuguées. Soient

$$a_0\quad a_{0.1}\quad a_{0.2}\quad \ldots\quad a_{0.p-1}$$

p lettres conjuguées toutes trouvées dans la 1ère première colonne verticale, (il est clair que nous pouvons faire qu'il en soit ainsi, en intervertissant l'ordre des lignes horizontales.)

Soient de même

$$a_{1.0}\quad a_{1.1}\quad a_{1.2}\quad a_{1.3}\quad \ldots\quad a_{1.p-1}$$

p lettres conjuguées toutes trouvées dans la seconde colonne verticale, inscrite que

$$a_{2.0}\quad a_{2.1}\quad a_{2.2}\quad a_{2.3}\quad \ldots\quad a_{2.p-1}$$

appartiennent respectivement aux mêmes lignes horizontales que

$$a_{0.0}\quad a_{0.1}\quad a_{0.2}\quad a_{0.3}\quad \ldots\quad a_{0.p-1}$$

Soient de même les systèmes de lettres conjuguées

$$a_{2.0}\quad a_{2.1}\quad a_{2.2}\quad a_{2.3}\quad \ldots\quad a_{2.p-1}$$

$$a_{3.0}\quad a_{3.1}\quad a_{3.2}\quad a_{3.3}\quad \ldots\quad a_{3.p-1}$$

$$\ldots\ldots\ldots\ldots$$

nous obtiendrons ainsi en tout p^2 lettres, le nombre total des lettres n'est pas épuisé, on prendra une troisième indice, inscrite que

$$a_{m.n.0}\quad a_{m.n.1}\quad a_{m.n.2}\quad a_{m.n.3}\quad \ldots\quad a_{m.n.p-1}$$

soit en général un système de lettres conjuguées. et l'on parviendra ainsi à cette conclusion que $N = p^p$, p étant un certain nombre égal à celui des indices différentes dont on aura besoin. la forme générale des lettres sera:

$$a_{\substack{K.K.K.\ldots K\\ 1\ 2\ 3\quad\ p}}$$

$K_1, K_2, K_3, \ldots\ldots K_p$ étant des indices qui peuvent prendre chacun les p valeurs $0, 1, 2, 3 \ldots\ldots p-1$

[On voit aussi par la manière dont nous avons posé les choses que dans le groupe H, toutes les substitutions seront de la forme

$$\left(a_{\substack{K.K.K.\ldots K\\ 1\ 2\ 3\quad\ p}},\ a_{\varphi(\delta)\cdot\psi(\delta)\cdot\chi(\delta)\ldots\sigma(\delta)}\right)$$

puisque chaque indice correspond à un système de p lettres conjuguées.

(Si p n'est pas un nombre premier on raisonnera sur le groupe de permutations de p ou plusieurs des systèmes de p lettres conjuguées, comme sur le groupe G, en remplaçant chaque indice par un certain nombre de nouveaux indices, et l'on trouvera $N = P^q$, P étant un nombre premier.)

Des équations primitives de degré p^n

Arrêtons nous un moment, pour traiter de toutes les équations primitives d'un degré p^n, p étant premier impair. (Le cas de $p = 2$ a été examiné.) Si une équation d'un degré p^n est abaissée par indices, supposons que l'abaissé soit telle, qu'elle devienne non primitive par une extraction de radical.

(Soit donné G un groupe primitif de p^n lettres qui se partage en p groupes non primitifs conjugués H.

Les p^n lettres peuvent naturellement former le groupe H de rangées telles,

$$\begin{array}{cccccc} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} & \cdots & a_{0,p-1} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} & \cdots & a_{1,p-1} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} & \cdots & a_{2,p-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{p-1,0} & a_{p-1,1} & a_{p-1,2} & a_{p-1,3} & \cdots & a_{p-1,p-1} \end{array}$$

Chaque ligne horizontale et chaque ligne verticale forme un système de p lettres conjuguées.

Si l'on permute entr'elles les lignes horizontales, le groupe que l'on obtient est encore primitif et de degré premier, nécessairement contenu dans les substitutions de la forme :

$$\left(a_{\alpha,\beta} \; , \; a_{m\alpha+n,\beta} \right)$$

Les indices étant pris relativement au module p.

Il en sera de même pour les lignes verticales qui ne peuvent admettre que des substitutions de la forme :

$$\left(a_{\alpha,\beta} \; , \; a_{\alpha,\gamma\beta+\gamma} \right)$$

Donc enfin toutes les substitutions du groupe H seront de la forme

$$\left(a_{\alpha,\beta} \; , \; a_{m\alpha+n,\; m\beta+\gamma} \right)$$

Si un groupe G se partage en n groupes conjugués H selon un nombre n diviseur, toutes les substitutions du groupe G devront se transformer les unes dans les autres les

substitutions circulaires du groupe H qui font toutes entrer comme il faut :

$$\left(a_{k,\kappa} \quad , \quad a_{k+\gamma,\kappa+\gamma} \cdots \right) \qquad (a)$$

Supposons donc que l'une des substitutions du groupe G de forme en remplaçant respectivement

$$\begin{matrix} k \\ i \end{matrix} \quad \text{par} \quad \varphi_1(k,\kappa)$$

$$\begin{matrix} k \\ 2 \end{matrix} \quad \text{par} \quad \varphi_2(k,\kappa)$$

Donne les fonctions φ_1 φ_2 on substitue pour k et κ les valeurs $k+\gamma$, $\kappa+\gamma$, il devra venir des substitutions de la forme.

$$\varphi_1 + f_1 \qquad \varphi_2 + f_1$$

et de là il est aisé de conclure immédiatement que les substitutions du groupe G devront être toutes comprises dans la formule

$$\left(a_{k,\kappa} \quad , \quad a_{\varphi_1 + m f_1 + n f_2 + \gamma,\ \varphi_2 + m f_1 + n f_2 + \gamma} \right) \qquad (A)$$

où nous savons que (1) que les substitutions du groupe G ne peuvent embrasser que p^2-1 ou p^2-p lettres, ce n'est point p^2-p puisque dans ce cas le groupe G serait non primitif. Donc dans le groupe G on ne considère que les permutations où la lettre $a_{\alpha,\beta}$ par exemple occupe toujours la même place, on aura donc des substitutions de bordre p^2-1 entre les p^2-1 autres lettres.

Mais rappelons nous ici que c'est simplement pour la démonstration que nous avons supposé que le groupe primitif G le partageait en groupes conjugués non primitifs, comme cette condition n'est nullement nécessaire, les groupes trouvés tout à l'heure peuvent former plus composés

Il reste donc à reconnaître dans quel cas ces groupes pourront donner des substitutions où p^2-p lettres seulement resteraient, et cette recherche va nous retenir quelques temps.

Soit donc G un groupe qui contienne quelques substitutions de bordre p^2-p, je dis d'abord que toutes les substitutions de ce groupe seront linéaires, c'est à dire de la forme (A)

(La chose est reconnue vraie pour les substitutions de bordre p^2-1. il suffit donc de la démontrer pour celles de bordre p^2-p. Or considérons donc p'un groupe où les substitutions restant toutes m de bordre p^2 ou de bordre p^2-p (voyez haut ci-dessus.)

(1) Ce théorème faisait partie d'un mémoire de Galois que j'ai été chargé par M. Liouville de publier dans le numéro de juillet 1846 de son journal.

A Ch.

Soient les p lettres qui dans une substitution de α lettres $\alpha > p$ ne varient pas, $\alpha - p$ étant $> p$ des lettres conjuguées. Supposons que ces lettres conjuguées soient :

$$a_{0,0}\ a_{0,1}\ a_{0,2}\ \ldots\ a_{0,p-1}$$

Nous pourrons déduire toutes les substitutions où ces p lettres se changent par de pareilles, nous pourrons les déduire de — substitutions de la forme

$$\left(a_{k,x}\ ,\ a_{1,\varphi x}\right)$$

et de substitution φ = borde $p-p$ dont la période devra être p pour former (voyez encore l'individu cité)

Les premières devront nécessairement, pour que le groupe jouisse de la propriété voulue, se réduire à la forme.

$$\left(a_{k,x}\ ,\ a_{1,mx}\right)$$

— D'après ce qu'on a vu pour les équations d'degré p.

Quant aux substitutions dont la période devra être p — former, comme elles sont conjuguées aux précédentes nous pourrons supposer un groupe qui les contiendra toutes contenir celles-ci. Or elles devront transformer les substitutions circulaires (a) les unes dans les autres. Donc elles devront être linéaires.

Nous bornerons donc ici notre attention à celles qui contiennent que le groupe primitif de permutations de p lettres doit se contenir que

Les substitutions de la forme (A)

Maintenant prenons le groupe total que les substitutions opérant sur l'expression

$$a_{k,x}$$

toutes les substitutions linéaires pour bien, et cherchons quels sont les deviseurs de ce groupe qui pourront jouir de la propriété voulue pour la résolubilité des équations.

Quel est d'abord le nombre total de — substitutions linéaires? Premièrement il est clair que toute — transformation de la forme

$$\begin{matrix} x, x \\ k, k \end{matrix} \qquad mx + n,\ \gamma \cdot mx + n,\ \gamma x + \zeta$$

ne peut pas être une substitution, car il faut que une substitution puisse changer tout de la première permutation il ne reste qu'une seule lettre de la seconde et réciproquement.

Il faut en outre qu'à une lettre quelconque $a_{k,x}$ de la seconde permutation, il ne lui corresponde à la lettre correspondante d'une autre, et ne lui en corresponde qu'une. Donc il faut que les deux équations

$$m_1 k_1 + n_1 k_1 + \gamma_1 = l_1 \qquad m_2 k_2 + n_2 k_2 + \gamma_2 = l_2$$

Des valeurs de K et K_1 trivia et dissemblables, avoir la condition pour qu'une quelle transformation linéaire entre elles ne donne pas une substitution, que $m_1 n - m n_1$ ne soit ni nul ni divisible par le module p, ce qui est la même chose.

Je dis maintenant que bien que le groupe des substitutions linéaires n'appartienne pas toujours, comme on le verra à l'équation abaissée par des équations linéaires qui donnent toutes les valeurs de deux des lettres prises, au moyen d'une certaine racine d'une autre, pourvu à chacune de ces racines restée arbitraires p valeurs, on aura p^m systèmes de valeurs, m étant un certain nombre. Donc le cas qui nous occupe m est nécessairement < 2 et se trouve par conséquent $= 0$ ou $= 1$. Donc le nombre des substitutions ne saurait être plus grand que

$$p^2(p^2-1)(p^2-p)$$

Il me reste à voir maintenant que les substitutions linéaires en les lettres A_{ik} ne varie pas; et donc on aura trouvé le nombre total des permutations du groupe qui contient toutes les substitutions linéaires possibles, il nous reste à multiplier ce nombre par p^2.

Or premièrement, une substitution S à indices K_k, sera les substitutions de la forme

$$\left(a_{\xi,\xi} \quad , \quad a_{m K + \xi,\, n K + \xi} \right)$$

Donnons à tout $p-1$ substitutions, on en aura $p^2(p-1)$ en ajoutant au terme K_k le terme $m K_k$ ainsi qu'il suit

$$\left(K_k \cdot K_k \,,\; m_1 K \cdot m K + K_k \right) \qquad (m')$$

D'une autre côté, il est aisé de trouver un groupe linéaire de p^2-1 permutations tel que donne chacune à des substitutions toutes les lettres à l'exception de deux variants car en remplaçant le double indice K_k par le double $K_k + i K_k$, i étant une racine primitive de

$$x^{p^2-1} - 1 = 0 \qquad (\mathrm{mod}\ p)$$

il est clair que toute substitution de la forme

$$\left(a_{K_k + K_k i} \quad , \quad a_{(m_1 + m_1 i)(K_k + K_k i)} \right)$$

sera une substitution linéaire; mais donne une substitution, aucune lettre ne reste à la même place, et elles sont en nombre de p^2-1;

Si l'on a un Groupe de $p^{2\lambda}$ permutations tel que par chacune de ses substitutions toutes les lettres restent à l'exception de α_{∞}. Combinant ces substitutions avec les $p^{\lambda}-p$ dont il est parlé plus haut, nous aurons

$$(p^{\lambda}-1)(p^{\lambda}-p) \text{ substitutions.}$$

Si nous avons vu à priori que le nombre des substitutions où α_{∞} reste fixe, ne pouvait être plus grand que $(p^{\lambda}-1)(p^{\lambda}-p)$ on n'est pas assuré que $= (p^{\lambda}-1)(p^{\lambda}-p)$, et le groupe linéaire total aura en tout

$$p^{\lambda}(p^{\lambda}-1)(p^{\lambda}-p) \text{ permutations.}$$

~~Le reste~~ Il reste à chercher le Théorème de ce groupe qui pourrait jouir de la propriété d'être établi par induction. Pour de nouvelles transformations qui n'aient pas l'objet d'abaisser autant que possible les équations générales de degré p^{λ} dont le groupe serait établi.

Premièrement, comme les substitutions circulaires d'un pareil groupe sont telles que toutes autres substitutions du groupe les transforment les unes dans les autres, on pourra abaisser l'équation d'un degré, et considérer une équation de degré $p^{\lambda}-1$ dont le groupe s'obtient par des substitutions de la forme

$$\left(\alpha_{K_1 \cdot K_2} \quad , \quad \alpha_{\frac{mK+n}{rK+s}}\right)$$

les $p^{\lambda}-1$ lettres étant

$$\begin{array}{ccccc} \alpha_{0,1} & \alpha_{0,2} & \alpha_{0,3} & \cdots & \\ \alpha_{1,0} & \alpha_{1,1} & \alpha_{1,2} & \alpha_{1,3} & \cdots \\ \alpha_{2,0} & \alpha_{2,1} & \alpha_{2,2} & \alpha_{2,3} & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \end{array}$$

J'observe maintenant que ce groupe ne sera primitif en toute que toutes les lettres α lorsque l'un d'eux indices est le même, tandis que deux lettres conjuguées α ont remplacé par une seule lettre. Dans chaque système de lettres conjuguées, on aura un groupe dont toutes les substitutions seront de la forme

$$\left(\alpha_{\frac{K_1}{K_2}} \quad , \quad \alpha_{\frac{mK_1+nK_2}{mK_2+nK_1}}\right)$$

$\frac{K_1}{K_2}$ étant un nouveau système de remplacement pour un seul indice K, on voit que les $p+1$ lettres seront

$$\alpha_0 \; \alpha_1 \; \alpha_2 \; \alpha_3 \cdots \text{ jusqu'à } \alpha_{\frac{1}{0}}$$

— et les substitutions seront de la forme

$$\left(K, \quad \frac{mK+n}{rK+s}\right)$$

Cherchons combien de fois on trouve dans chacune de ces substitutions, mettons-y la même place, il faut pour cela résoudre l'équation

$$(rK+s)K-(mK+n)\equiv 0$$

qui aura deux ou une ou aucune racine, suivant que $(m-s)^2+4nr$ sera > 0, = 0 ou < 0, c'est-à-dire suivant que le discriminant de l'équation du second degré sera résidu quadratique, nul ou non résidu quadratique. Suivant ces trois cas la substitution élevée à la puissance $p-1$ donnera p ou p^2.

On peut prendre pour type d'une des premières sortes de substitutions celles de la forme

$$(K, mK+n)$$

où le coefficient $\frac{b}{a}$ ne varie pas, et dont le nombre est évidemment p. Le nombre total des substitutions du groupe cherché sera donc

$$(p+1)p(p-1).$$

C'est après avoir réduit ce groupe que nous allons le traiter généralement. Nous chercherons d'abord quel sera le nombre de ceux de ce groupe qui contiendront des substitutions dont l'ordre p pourra appartenir à une équation soluble par radicaux.

Dans ce cas, l'équation étant primitive et elle ne pouvant être soluble par radicaux à moins que son ordre $p^{\alpha+1}=q^n$, n étant un certain nombre.

Nous pouvons supposer que le groupe ne contiendra que des substitutions de l'ordre p et de l'ordre $p^{\alpha+1}$, toutes les substitutions de l'ordre p^{α} devant par conséquent doubler, et leur période être de 2 termes.

Prenons donc l'expression

$$\left(K, \frac{mK+n}{rK+s}\right),$$

et voyons dans quel cas cette substitution peut avoir une période de deux termes. Il faut pour cela que la substitution inverse se confonde avec elle. La substitution inverse est:

$$\left(K, \frac{sK+n}{rK-m}\right)$$

Donc on doit avoir $m=-s$, et toutes les substitutions en question seront:

$$\left(K, \frac{mK+n}{K-m}\right)$$

ou encore

$$\left(K, m+\frac{N}{K-m}\right)$$

N étant un certain nombre qui est le même pour toutes les substitutions, puisque une substitution doit être transformée en elle-même par toutes les substitutions de l'ordre p, $(K, K+m)$, or une substitution doit être changée en elle-même par une infinité de puissances de

$$\left(K, \; x + \frac{N}{K-x}\right), \qquad \left(K, \; x + \frac{N}{K-x}\right)$$

toutes deux pareilles substitutions, il faut que l'on ait :

$$x + \frac{N}{\frac{N}{K-x} + m - x} = m + \frac{N}{\frac{N}{K-x} + x - m}$$

savoir $(m-x)^2 = \pm N$

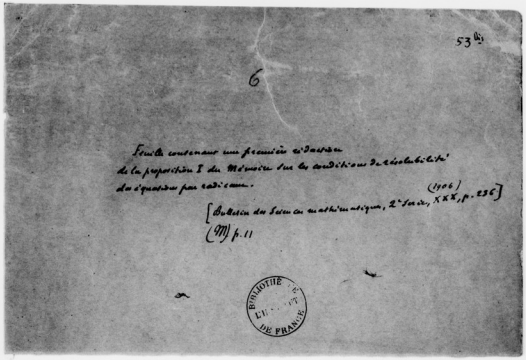
Donc la différence entre deux valeurs de m ne peut exprimer que deux valeurs différentes. Donc m ne peut avoir plus de trois valeurs. Donc enfin $p \geq 3$. Ainsi, c'est seulement dans ce cas que le groupe résolu pourra contenir des substitutions de l'ordre p.

Et on effectue la réduite sera alors du $4^{ème}$ degré, elle pourra conséquent résoluble par radicaux.

Pour trouver par là quelque général parmi les substitutions d'un autre groupe résolu, il ne devra pas se trouver de substitution de l'ordre p. Mais il y en aura de l'ordre $p-1$! c'est ce que j'ai vainement rechercher. (1)

. . . . . .

(1) J'ai cherché vainement à la combattre ainsi que quelques autres objections, ce qui me vient de dire.
(Note de M. A. Chevalier)


53 bis
6
Feuille contenant une première démonstration
de la proposition I du Mémoire sur la condition nécessaire et suffisante
de séparation pour soi-même.
(1906)
[Bulletin des Sciences mathématiques, 2e Série, t. XLV, p. 256]
(M) f. 11
BIBLIOTHÈQUE DE FRANCE