VII.

DÉMONSTRATION DE L'IMPOSSIBILITÉ DE LA RÉSOLUTION ALGÉBRIQUE DES ÉQUATIONS GÉNÉRALES QUI PASSENT LE QUATRIÈME DEGRÉ.

Journal für die reine und angewandte Mathematik, herausgegeben von *Crelle*, Bd. 1, Berlin 1826.

On peut, comme on sait, résoudre les équations générales jusqu'au quatrième degré, mais les équations d'un degré plus élevé, seulement dans des cas particuliers, et, si je ne me trompe, on n'a pas encore répondu d'une manière satisfaisante à la question: "Est-il possible de résoudre en général les équations qui passent le quatrième degré?" Ce mémoire a pour but de répondre à cette question.

Résoudre algébriquement une équation ne veut dire autre chose, que d'exprimer ses racines par des fonctions algébriques des coefficiens. Il faut donc considérer d'abord la forme générale des fonctions algébriques, et chercher ensuite s'il est possible de satisfaire à l'équation donnée, en mettant l'expression d'une fonction algébrique au lieu de l'inconnue.

§ 1.

Sur la forme générale des fonctions algébriques.

Soient x', x'', $x'''\ldots$ un nombre fini de quantités quelconques. On dit que v est une fonction *algébrique* de ces quantités, s'il est possible d'exprimer v en x', x'', $x'''\ldots$ à l'aide des opérations suivantes: 1) par l'addition; 2) par la multiplication, soit de quantités dépendant de x', x'', $x'''\ldots$, soit de quantités qui n'en dépendent pas; 3) par la division; 4) par l'extraction de racines d'indices premiers. Parmi ces opérations nous n'avons pas compté la soustraction, l'élévation à des puissances entières et l'extraction de racines de degrés composés, car elles sont évidemment comprises dans les quatre opérations mentionnées.

Lorsque la fonction v peut se former par les trois premières des opérations ci-dessus, elle est dite *algébrique et rationnelle,* ou seulement *rationnelle;* et si les deux premières opérations sont seules nécessaires, elle est dite *algébrique, rationnelle et entière,* ou seulement *entière.*

Soit $f(x', x'', x'''\ldots)$ une fonction quelconque qui peut s'exprimer par la somme d'un nombre fini de termes de la forme

$$Ax'^{m_1}x''^{m_2}\ldots\ldots$$

où A est une quantité indépendante de x', x'' etc. et où m_1, m_2 etc. désignent des nombres entiers positifs; il est clair que les deux premières opérations ci-dessus sont des cas particuliers de l'opération désignée par $f(x', x'', x'''\ldots)$. On peut donc considérer les fonctions entières, suivant leur définition, comme résultant d'un nombre limité de répétitions de cette opération. En désignant par v', v'', v''' etc. plusieurs fonctions des quantités x', x'' $x'''\ldots\ldots$ de la même forme que $f(x', x''\ldots\ldots)$, la fonction $f(v', v''\ldots\ldots)$ sera évidemment de la même forme que $f(x', x''\ldots)$. Or $f(v', v''\ldots)$ est l'expression générale des fonctions qui résultent de l'opération $f(x', x''\ldots\ldots)$ deux fois répétée. On trouvera donc toujours le même résultat en répétant cette opération autant de fois qu'on voudra. Il suit de là, que toute fonction entière de plusieurs quantités x', $x''\ldots\ldots$ peut être exprimée par une somme de plusieurs termes de la forme $Ax'^{m_1}x''^{m_2}\ldots\ldots$

Considérons maintenant les fonctions rationnelles. Lorsque $f(x', x''\ldots)$ et $\varphi(x', x''\ldots)$ sont deux fonctions entières, il est évident, que les trois premières opérations sont des cas particuliers de l'opération désignée par

$$\frac{f(x', x''\ldots)}{\varphi(x', x''\ldots)}.$$

On peut donc considérer une fonction rationnelle comme le résultat de la répétition de cette opération. Si l'on désigne par v', v'', v''' etc. plusieurs fonctions de la forme $\frac{f(x', x''\ldots)}{\varphi(x', x''\ldots)}$, on voit aisément que la fonction $\frac{f(v', v''\ldots)}{\varphi(v', v''\ldots)}$ peut être réduite à la même forme. Il suit de là, que toute fonction rationnelle de plusieurs quantités x', $x''\ldots\ldots$ peut toujours être réduite à la forme

$$\frac{f(x', x''\ldots\ldots)}{\varphi(x', x''\ldots\ldots)},$$

où le numérateur et le dénominateur sont des fonctions entières.

Enfin nous allons chercher la forme générale des fonctions algébriques. Désignons par $f(x', x'' \ldots)$ une fonction rationnelle quelconque, il est clair que toute fonction algébrique peut être composée à l'aide de l'opération désignée par $f(x', x'' \ldots)$ combinée avec l'opération $\sqrt[m]{r}$, où m est un nombre premier. Donc, si $p', p'' \ldots$ sont des fonctions rationnelles de $x', x'' \ldots$,

$$p_1 = f(x', x'' \ldots \sqrt[n']{p'}, \sqrt[n'']{p''} \ldots)$$

sera la forme générale des fonctions algébriques de $x', x'' \ldots$, dans lesquelles l'opération exprimée par $\sqrt[m]{r}$ affecte seulement des fonctions rationnelles. Les fonctions de la forme p_1 seront dites fonctions algébriques *du premier ordre*. En désignant par $p_1', p_1'' \ldots$ plusieurs quantités de la forme p_1, l'expression

$$p_2 = f(x', x'' \ldots \sqrt[n']{p'}, \sqrt[n'']{p''} \ldots \sqrt[n_1']{p_1'}, \sqrt[n_1'']{p_1''} \ldots)$$

sera la forme générale des fonctions algébriques de $x', x'' \ldots$, dans lesquelles l'opération $\sqrt[m]{r}$ affecte seulement des fonctions rationnelles, et des fonctions algébriques du premier ordre. Les fonctions de la forme p_2 seront dites fonctions algébriques *du deuxième ordre*. De la même manière l'expression

$$p_3 = f(x', x'' \ldots \sqrt[n']{p'}, \sqrt[n'']{p''} \ldots \sqrt[n_1']{p_1'}, \sqrt[n_1'']{p_1''}, \ldots \sqrt[n_2']{p_2'}, \sqrt[n_2'']{p_2''} \ldots),$$

dans laquelle $p_2', p_2'' \ldots$ sont des fonctions du deuxième ordre, sera la forme générale des fonctions algébriques de $x', x'' \ldots$, dans lesquelles l'opération $\sqrt[m]{r}$ n'affecte que des fonctions rationnelles, et des fonctions algébriques du premier et du deuxième ordre.

En continuant de cette manière, on obtiendra des fonctions algébriques du troisième, du quatrième ... du $\mu^{ième}$ ordre, et il est clair, que l'expression des fonctions du $\mu^{ième}$ ordre, sera l'expression *générale* des fonctions algébriques.

Donc en désignant par μ l'ordre d'une fonction algébrique quelconque et par v la fonction même, on aura

$$v = f(r', r'' \ldots \sqrt[n']{p'}, \sqrt[n'']{p''} \ldots),$$

où $p', p'' \ldots$ sont des fonctions de l'ordre $\mu - 1$; $r', r'' \ldots$ des fonctions de l'ordre $\mu - 1$ ou des ordres moins élevés, et $n', n'' \ldots$ des nombres premiers; f désigne toujours une fonction rationnelle des quantités comprises entre les parenthèses.

On peut évidemment supposer qu'il est impossible d'exprimer l'une des quantités $\sqrt[n']{p'}, \sqrt[n'']{p''} \ldots$ par une fonction rationnelle des autres et des quantités $r', r'' \ldots$; car dans le cas contraire, la fonction v aurait cette forme plus simple,

$$v = f(r', r'' \ldots \sqrt[n']{p'}, \sqrt[n'']{p''} \ldots),$$

où le nombre des quantités $\sqrt[n']{p'}, \sqrt[n'']{p''} \ldots$ serait diminué au moins d'une unité. En réduisant de cette manière l'expression de v autant que possible, on parviendrait, ou à une expression irréductible, ou à une expression de la forme

$$v = f(r', r'', r''' \ldots);$$

mais cette fonction serait seulement de l'ordre $\mu - 1$, tandis que v doit être du $\mu^{ième}$ ordre, ce qui est une contradiction.

Si dans l'expression de v le nombre des quantités $\sqrt[n']{p'}, \sqrt[n'']{p''} \ldots$ est égal à m, nous dirons que la fonction v est du $\mu^{ième}$ *ordre* et du $m^{ième}$ *degré*. On voit donc qu'une fonction de l'ordre μ et du degré 0 est la même chose qu'une fonction de l'ordre $\mu - 1$, et qu'une fonction de l'ordre 0 est la même chose qu'une fonction rationnelle.

Il suit de là, qu'on peut poser

$$v = f(r', r'' \ldots \sqrt[n]{p}),$$

où p est une fonction de l'ordre $\mu - 1$, mais $r', r'' \ldots$ des fonctions du $\mu^{ième}$ ordre et tout au plus du degré $m - 1$, et qu'on peut toujours supposer qu'il est impossible d'exprimer $\sqrt[n]{p}$ par une fonction rationnelle de ces quantités.

Dans ce qui précède nous avons vu qu'une fonction rationnelle de plusieurs quantités peut toujours être réduite à la forme

$$\frac{s}{t},$$

où s et t sont des fonctions entières des mêmes quantités variables. On

conclut de là que v peut toujours être exprimé comme il suit,

$$v = \frac{\varphi(r', r'' \ldots \sqrt[n]{p})}{\tau(r', r'' \ldots \sqrt[n]{p})},$$

où φ et τ désignent des fonctions entières des quantités r', $r''\ldots$ et $\sqrt[n]{p}$. En vertu de ce que nous avons trouvé plus haut, toute fonction entière de plusieurs quantités s, r', $r''\ldots$ peut s'exprimer par la forme

$$t_0 + t_1 s + t_2 s^2 + \cdots + t_m s^m,$$

t_0, $t_1 \ldots t_m$ étant des fonctions entières de r', r'', $r'''\ldots$ sans s. On peut donc poser

$$v = \frac{t_0 + t_1 p^{\frac{1}{n}} + t_2 p^{\frac{2}{n}} + \cdots + t_m p^{\frac{m}{n}}}{v_0 + v_1 p^{\frac{1}{n}} + v_2 p^{\frac{2}{n}} + \cdots + v_{m'} p^{\frac{m'}{n}}} = \frac{T}{V},$$

où t_0, $t_1 \ldots t_m$ et v_0, $v_1 \ldots v_{m'}$ sont des fonctions entières de r', r'', r''' etc.

Soient V_1, $V_2 \ldots V_{n-1}$ les $n-1$ valeurs de V qu'on trouve en mettant successivement $\alpha p^{\frac{1}{n}}$, $\alpha^2 p^{\frac{1}{n}}$, $\alpha^3 p^{\frac{1}{n}} \ldots \alpha^{n-1} p^{\frac{1}{n}}$ au lieu de $p^{\frac{1}{n}}$, α étant une racine différente de l'unité de l'équation $\alpha^n - 1 = 0$; on trouvera en multipliant le numérateur et le dénominateur de $\frac{T}{V}$ par $V_1\, V_2\, V_3 \ldots V_{n-1}$

$$v = \frac{T\, V_1\, V_2 \ldots V_{n-1}}{V\, V_1\, V_2 \ldots V_{n-1}}.$$

Le produit $V V_1 \ldots V_{n-1}$ peut, comme on sait, s'exprimer par une fonction entière de p et des quantités r', $r''\ldots$, et le produit $T V_1 \ldots V_{n-1}$ est, comme on le voit, une fonction entière de $\sqrt[n]{p}$ et de r', $r''\ldots$. En supposant ce produit égal à

$$s_0 + s_1 p^{\frac{1}{n}} + s_2 p^{\frac{2}{n}} + \cdots + s_k p^{\frac{k}{n}},$$

on trouve

$$v = \frac{s_0 + s_1 p^{\frac{1}{n}} + s_2 p^{\frac{2}{n}} + \cdots + s_k p^{\frac{k}{n}}}{m},$$

ou, en écrivant q_0, q_1, $q_2 \ldots$ au lieu de $\frac{s_0}{m}$, $\frac{s_1}{m}$, $\frac{s_2}{m}$ etc.,

$$v = q_0 + q_1 p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \cdots + q_k p^{\frac{k}{n}},$$

où q_0, $q_1 \ldots q_k$ sont des fonctions rationnelles des quantités p, r', $r''\ldots$ etc.

Soit μ un nombre entier quelconque, on peut toujours poser

$$\mu = an + \alpha,$$

a et α étant deux nombres entiers, et $\alpha < n$. Il suit de là, que

$$p^{\frac{\mu}{n}} = p^{\frac{an+\alpha}{n}} = p^a p^{\frac{\alpha}{n}}.$$

En mettant donc cette expression au lieu de $p^{\frac{\mu}{n}}$ dans l'expression de v, on obtiendra

$$v = q_0 + q_1 p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \cdots + q_{n-1} p^{\frac{n-1}{n}},$$

q_0, q_1, q_2 étant encore des fonctions rationnelles de p, r', $r''\ldots$, et par conséquent des fonctions du $\mu^{\text{ième}}$ ordre et au plus du degré $m-1$, et telles qu'il soit impossible d'exprimer $p^{\frac{1}{n}}$ rationnellement par ces quantités.

Dans l'expression de v ci-dessus, on peut toujours faire $q_1 = 1$. Car si q_1 n'est pas nul, on obtiendra, en faisant $p_1 = p q_1^n$,

$$p = \frac{p_1}{q_1^n}, \quad p^{\frac{1}{n}} = \frac{p_1^{\frac{1}{n}}}{q_1},$$

donc

$$v = q_0 + p_1^{\frac{1}{n}} + \frac{q_2}{q_1^2} p_1^{\frac{2}{n}} + \cdots + \frac{q_{n-1}}{q_1^{n-1}} p_1^{\frac{n-1}{n}},$$

expression de la même forme que la précédente, sauf que $q_1 = 1$. Si $q_1 = 0$, soit q_μ une des quantités q_1, $q_2 \ldots q_{n-1}$, qui ne soit pas nulle, et soit $q_\mu^n p^\mu = p_1$. On déduit de là $q_\mu^\alpha p^{\frac{\alpha\mu}{n}} = p_1^{\frac{\alpha}{n}}$. Donc en prenant deux nombres entiers α et β, qui satisfassent à l'équation $\alpha\mu - \beta n = \mu'$, μ' étant un nombre entier, on aura

$$q_\mu^\alpha p^{\frac{\beta n + \mu'}{n}} = p_1^{\frac{\alpha}{n}} \quad \text{et} \quad p^{\frac{\mu'}{n}} = q_\mu^{-\alpha} p^{-\beta} p_1^{\frac{\alpha}{n}}.$$

En vertu de cela et en remarquant que $q_\mu p^{\frac{\mu}{n}} = p_1^{\frac{1}{n}}$, v aura la forme

$$v = q_0 + p_1^{\frac{1}{n}} + q_2 p_1^{\frac{2}{n}} + \cdots + q_{n-1} p_1^{\frac{n-1}{n}}.$$

De tout ce qui précède on conclut: Si v est une fonction algébrique de l'ordre μ et du degré m, on peut toujours poser:

$$v = q_0 + p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + q_3 p^{\frac{3}{n}} + \cdots + q_{n-1} p^{\frac{n-1}{n}},$$

n étant un nombre premier, q_0, $q_2 \cdots q_{n-1}$ des fonctions algébriques de l'ordre μ et du degré $m-1$ au plus, p une fonction algébrique de l'ordre $\mu - 1$, et telle que $p^{\frac{1}{n}}$ ne puisse s'exprimer rationnellement en q_0, $q_1 \cdots q_{n-1}$.

§ II.

Propriétés des fonctions algébriques qui satisfont à une équation donnée.

Soit

$$c_0 + c_1 y + c_2 y^2 + \cdots + c_{r-1} y^{r-1} + y^r = 0 \tag{1}$$

une équation quelconque du degré r, où c_0, c_1 ... sont des fonctions rationnelles de x', x'' ..., x', x'' ... étant des quantités indépendantes quelconques. Supposons qu'on puisse satisfaire à cette équation, en mettant au lieu de y une fonction algébrique de x', x'' .... Soit

$$y = q_0 + p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \cdots + q_{n-1} p^{\frac{n-1}{n}} \tag{2}$$

cette fonction. En substituant cette expression de y, dans l'équation proposée, on obtiendra, en vertu de ce qui précède, une expression de la forme

$$r_0 + r_1 p^{\frac{1}{n}} + r_2 p^{\frac{2}{n}} + \cdots + r_{n-1} p^{\frac{n-1}{n}} = 0, \tag{3}$$

où r_0, r_1, $r_2 \ldots r_{n-1}$ sont des fonctions rationnelles des quantités p, q_0, $q_1 \cdots q_{n-1}$.

Or je dis que l'équation (3) ne peut avoir lieu, à moins qu'on n'ait séparement

$$r_0 = 0, \quad r_1 = 0 \ldots\ldots r_{n-1} = 0.$$

En effet, dans le cas contraire, on aurait en posant $p^{\frac{1}{n}} = z$ les deux équations

$$z^n - p = 0$$

et

$$r_0 + r_1 z + r_2 z^2 + \cdots + r_{n-1} z^{n-1} = 0,$$

qui auraient une ou plusieurs *racines communes*. Soit k le nombre de ces racines, on peut, comme on sait, trouver une équation qui a pour racines les k racines mentionnées, et dont les coefficiens sont des fonctions rationnelles de p, r_0, $r_1 \ldots r_{n-1}$. Soit

$$s_0 + s_1 z + s_2 z^2 + \cdots + s_{k-1} z^{k-1} + z^k = 0$$

cette équation, et

$$t_0 + t_1 z + t_2 z^2 + \cdots + t_{\mu-1} z^{\mu-1} + z^\mu$$

un facteur de son premier membre, où t_0, t_1 etc. sont des fonctions rationnelles de p, r_0, $r_1 \ldots r_{n-1}$, on aura de même

$$t_0 + t_1 z + t_2 z^2 + \cdots + t_{\mu-1} z^{\mu-1} + z^\mu = 0,$$

et il est clair qu'on peut supposer qu'il est impossible de trouver une équation de la même forme d'un degré moins élevé. Cette équation a ses μ racines communes avec l'équation $z^n - p = 0$. Or toutes les racines de l'équation $z^n - p = 0$, sont de la forme αz, où α est une racine quelconque de l'unité. Donc en remarquant que μ ne peut être moindre que 2, parce qu'il est impossible d'exprimer z en fonction rationnelle des quantités p, r_0, $r_1 \ldots r_{n-1}$, il s'ensuit, que deux équations de la forme

$$t_0 + t_1 z + t_2 z^2 + \cdots + t_{\mu-1} z^{\mu-1} + z^\mu = 0,$$

et

$$t_0 + \alpha t_1 z + \alpha^2 t_2 z^2 + \cdots + \alpha^{\mu-1} t_{\mu-1} z^{\mu-1} + \alpha^\mu z^\mu = 0$$

doivent avoir lieu. De ces équations on tire, en éliminant z^μ,

$$t_0(1 - \alpha^\mu) + t_1(\alpha - \alpha^\mu) z + \cdots + t_{\mu-1}(\alpha^{\mu-1} - \alpha^\mu) z^{\mu-1} = 0.$$

Mais cette équation étant du degré $\mu - 1$, et l'équation

$$z^\mu + t_{\mu-1} z^{\mu-1} + \cdots = 0$$

étant irréductible, et par conséquent t_0 ne pouvant être égal à zéro, on doit avoir $\alpha^\mu - 1 = 0$, ce qui n'a pas lieu. On doit donc avoir

$$r_0 = 0, \; r_1 = 0 \ldots r_{n-1} = 0.$$

Maintenant, ces équations ayant lieu, il est clair que l'équation proposée sera satisfaite par toutes les valeurs de y qu'on obtient en attribuant à $p^{\frac{1}{n}}$ toutes les valeurs $\alpha p^{\frac{1}{n}}$, $\alpha^2 p^{\frac{1}{n}} \ldots \alpha^{n-1} p^{\frac{1}{n}}$. On voit aisément que toutes

ces valeurs de y seront différentes entre elles; car dans le cas contraire on aurait une équation de la même forme que (3), mais une telle équation conduit, comme on vient de le voir, à des contradictions.

En désignant donc par $y_1, y_2 \ldots y_n$ n racines différentes de l'équation (1), on aura

$$y_1 = q_0 + p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \cdots + q_{n-1} p^{\frac{n-1}{n}},$$
$$y_2 = q_0 + \alpha p^{\frac{1}{n}} + \alpha^2 q_2 p^{\frac{2}{n}} + \cdots + \alpha^{n-1} q_{n-1} p^{\frac{n-1}{n}},$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$y_n = q_0 + \alpha^{n-1} p^{\frac{1}{n}} + \alpha^{n-2} q_2 p^{\frac{2}{n}} + \cdots + \alpha q_{n-1} p^{\frac{n-1}{n}}.$$

De ces n équations on tirera sans peine

$$q_0 = \frac{1}{n}(y_1 + y_2 + y_3 + \cdots + y_n),$$
$$p^{\frac{1}{n}} = \frac{1}{n}(y_1 + \alpha^{n-1} y_2 + \alpha^{n-2} y_3 + \cdots + \alpha y_n),$$
$$q_2 p^{\frac{2}{n}} = \frac{1}{n}(y_1 + \alpha^{n-2} y_2 + \alpha^{n-4} y_3 + \cdots + \alpha^2 y_n),$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$q_{n-1} p^{\frac{n-1}{n}} = \frac{1}{n}(y_1 + \alpha y_2 + \alpha^2 y_3 + \cdots + \alpha^{n-1} y_n).$$

On voit par là que toutes les quantités $p^{\frac{1}{n}}$, q_0, $q_2 \ldots q_{n-1}$ sont des fonctions rationnelles des racines de l'équation proposée. En effet on a

$$q_\mu = n^{\mu-1} \frac{y_1 + \alpha^{-\mu} y_2 + \alpha^{-2\mu} y_3 + \cdots + \alpha^{-(n-1)\mu} y_n}{(y_1 + \alpha^{-1} y_2 + \alpha^{-2} y_3 + \cdots + \alpha^{-(n-1)} y_n)^\mu}.$$

Considérons maintenant l'équation générale du degré m,

$$0 = a + a_1 x + a_2 x^2 + \cdots + a_{m-1} x^{m-1} + x^m,$$

et supposons qu'elle soit résoluble algébriquement. Soit

$$x = s_0 + v^{\frac{1}{n}} + s_2 v^{\frac{2}{n}} + \cdots + s_{n-1} v^{\frac{n-1}{n}};$$

en vertu de ce qui précède, les quantités v, s_0, s_2 etc. peuvent s'exprimer rationnellement en $x_1, x_2 \ldots x_m$, en désignant par $x_1, x_2 \ldots x_m$ les racines de l'équation proposée.

Considérons l'une quelconque des quantités v, s_0, s_2 etc. par exemple v. Si l'on désigne par $v_1, v_2 \ldots v_{n'}$ les valeurs différentes de v, qu'on trouve lorsqu'on échange entre elle les racines $x_1, x_2 \ldots x_m$ de toutes les manières possibles, on pourra former une équation du degré n' dont les coefficiens sont des fonctions rationnelles de a, $a_1 \ldots a_{m-1}$, et dont les racines sont les quantités $v_1, v_2 \ldots v_{n'}$, qui sont des fonctions rationnelles des quantités $x_1, x_2 \ldots x_m$.

Donc si l'on pose

$$v = t_0 + u^{\frac{1}{\nu}} + t_2 u^{\frac{2}{\nu}} + \cdots + t_{\nu-1} u^{\frac{\nu-1}{\nu}},$$

toutes les quantités $u^{\frac{1}{\nu}}$, t_0, $t_2 \ldots t_{\nu-1}$ seront des fonctions rationnelles de $v_1, v_2 \ldots v_{n'}$, et par conséquent de $x_1, x_2 \ldots x_m$. En traitant les quantités u, t_0, t_2 etc. de la même manière, on en conclut que

si une équation est résoluble algébriquement, on peut toujours donner à la racine une forme telle, que toutes les fonctions algébriques dont elle est composée puissent s'exprimer par des fonctions rationnelles des racines de l'équation proposée.

§ III.

Sur le nombre des valeurs différentes qu'une fonction de plusieurs quantités peut acquérir, lorsqu'on échange entre elles les quantités qu'elle renferme.

Soit v une fonction rationnelle de plusieurs quantités indépendantes $x_1, x_2 \ldots x_n$. Le nombre des valeurs différentes dont cette fonction est susceptible par l'échange des quantités dont elle dépend, ne peut surpasser le produit $1.2.3 \ldots n$. Soit μ ce produit.

Soit maintenant

$$v\begin{pmatrix} \alpha\beta\gamma\delta\ldots. \\ a\,b\,c\,d\ldots. \end{pmatrix}$$

la valeur qu'une fonction quelconque v reçoit, lorsqu'on y substitue x_a, x_b, x_c, x_d etc. au lieu de $x_\alpha, x_\beta, x_\gamma, x_\delta$ etc., il est clair qu'en désignant par $A_1, A_2 \ldots A_\mu$ les diverses permutations en nombre de μ que l'on peut former avec les indices 1, 2, 3 $\ldots n$, les valeurs différentes de v pourront être exprimées par

$$v\begin{pmatrix} A_1 \\ A_1 \end{pmatrix}, \quad v\begin{pmatrix} A_1 \\ A_2 \end{pmatrix}, \quad v\begin{pmatrix} A_1 \\ A_3 \end{pmatrix} \ldots . \; v\begin{pmatrix} A_1 \\ A_\mu \end{pmatrix}.$$

Supposons que le nombre des valeurs différentes de v soit moindre que μ, il faudra que plusieurs valeurs de v soient égales entre elles, en sorte qu'on ait par exemple

$$v\begin{pmatrix}A_1\\A_1\end{pmatrix}=v\begin{pmatrix}A_1\\A_2\end{pmatrix}=\cdots=v\begin{pmatrix}A_1\\A_m\end{pmatrix}.$$

Si l'on fait subir à ces quantités la substitution désignée par $\begin{pmatrix}A_1\\A_{m+1}\end{pmatrix}$, on aura cette nouvelle série de valeurs égales

$$v\begin{pmatrix}A_1\\A_{m+1}\end{pmatrix}=v\begin{pmatrix}A_1\\A_{m+2}\end{pmatrix}=\cdots=v\begin{pmatrix}A_1\\A_{2m}\end{pmatrix},$$

valeurs qui sont différentes des premières, mais en même nombre. En changeant de nouveau ces quantités par la substitution désignée par $\begin{pmatrix}A_1\\A_{2m+1}\end{pmatrix}$, on aura un nouveau système de quantités égales, mais différentes des précédentes. En continuant ce procédé jusqu'à ce qu'on ait épuisé toutes les permutations possibles, les μ valeurs de v seront partagées en plusieurs systèmes, dont chacun contiendra un nombre de m valeurs égales. Il suit de là que si l'on représente le nombre des valeurs différentes de v par ϱ, nombre égal à celui des systèmes, on aura

$$\varrho m=1.2.3\ldots n,$$

c'est-à-dire:

Le nombre des valeurs différentes qu'une fonction de n quantités peut acquérir par toutes les substitutions possibles entre ces quantités, est nécessairement un diviseur du produit $1.2.3\ldots n$. Cela est connu.

Soit maintenant $\begin{pmatrix}A_1\\A_m\end{pmatrix}$ une substitution quelconque. Supposons qu'en appliquant celle-ci plusieurs fois de suite à la fonction v on obtienne la suite des valeurs

$$v,\ v_1,\ v_2\ldots v_{p-1},\ v_p,$$

il est clair que v sera nécessairement répété plusieurs fois. Lorsque v revient après un nombre p de substitutions, nous disons que $\begin{pmatrix}A_1\\A_m\end{pmatrix}$ est une *substitution récurrente de l'ordre* p. On a donc cette série périodique

$$v,\ v_1,\ v_2\ldots v_{p-1},\ v,\ v_1,\ v_2\ldots$$

ou bien, si l'on représente par $v\begin{pmatrix}A_1\\A_m\end{pmatrix}^r$ la valeur de v qu'on obtient après

avoir répété r fois de suite la substitution désignée par $\begin{pmatrix}A_1\\A_m\end{pmatrix}$, on a la série

$$v\begin{pmatrix}A_1\\A_m\end{pmatrix}^0,\ v\begin{pmatrix}A_1\\A_m\end{pmatrix}^1,\ v\begin{pmatrix}A_1\\A_m\end{pmatrix}^2\ldots v\begin{pmatrix}A_1\\A_m\end{pmatrix}^{p-1},\ v\begin{pmatrix}A_1\\A_m\end{pmatrix}^0\ldots$$

Il suit de là que

$$v\begin{pmatrix}A_1\\A_m\end{pmatrix}^{\alpha p+r}=v\begin{pmatrix}A_1\\A_m\end{pmatrix}^r$$

$$v\begin{pmatrix}A_1\\A_m\end{pmatrix}^{\alpha p}=v\begin{pmatrix}A_1\\A_m\end{pmatrix}^0=v.$$

Or soit p le plus grand nombre premier contenu dans n, si le nombre des valeurs différentes de v est moindre que p, il faut qu'entre p valeurs quelconques, deux soient égales entre elles.

Il faut donc que des p valeurs,

$$v\begin{pmatrix}A_1\\A_m\end{pmatrix}^0,\ v\begin{pmatrix}A_1\\A_m\end{pmatrix}^1,\ v\begin{pmatrix}A_1\\A_m\end{pmatrix}^2\ldots v\begin{pmatrix}A_1\\A_m\end{pmatrix}^{p-1},$$

deux soient égales entre elles. Soit par exemple

$$v\begin{pmatrix}A_1\\A_m\end{pmatrix}^r=v\begin{pmatrix}A_1\\A_m\end{pmatrix}^{r'},$$

on en conclut que

$$v\begin{pmatrix}A_1\\A_m\end{pmatrix}^{r+p-r}=v\begin{pmatrix}A_1\\A_m\end{pmatrix}^{r'+p-r}$$

Écrivant r au lieu de $r'+p-r$ et remarquant que $v\begin{pmatrix}A_1\\A_m\end{pmatrix}^p=v$, on en tire

$$v=v\begin{pmatrix}A_1\\A_m\end{pmatrix}^r,$$

où r évidemment n'est pas multiple de p. La valeur de v n'est donc pas changée par la substitution $\begin{pmatrix}A_1\\A_m\end{pmatrix}^r$, ni par conséquent non plus par la répétition de la même substitution. On a donc

$$v=v\begin{pmatrix}A_1\\A_m\end{pmatrix}^{r\alpha},$$

α étant un nombre entier. Maintenant si p est un nombre premier, on pourra évidemment toujours trouver deux nombres entiers α et β tels que

$$r\alpha=p\beta+1,$$

donc

$$v = v\begin{pmatrix} A_1 \\ A_m \end{pmatrix}^{p\beta+1},$$

et puisque

$$v = v\begin{pmatrix} A_1 \\ A_m \end{pmatrix}^{p\beta},$$

on aura

$$v = v\begin{pmatrix} A_1 \\ A_m \end{pmatrix}.$$

La valeur de v ne sera donc pas changée par la substitution récurrente $\begin{pmatrix} A_1 \\ A_m \end{pmatrix}$ de l'ordre p.

Or il est clair que

$$\begin{pmatrix} \alpha\beta\gamma\delta\ldots\zeta\eta \\ \beta\gamma\delta\varepsilon\ldots\eta\alpha \end{pmatrix} \text{ et } \begin{pmatrix} \beta\gamma\delta\varepsilon\ldots\eta\alpha \\ \gamma\alpha\beta\delta\ldots\zeta\eta \end{pmatrix}$$

sont des substitutions récurrentes de l'ordre p, lorsque p est le nombre des indices $\alpha, \beta, \gamma \ldots \eta$. La valeur de v ne sera donc pas changée non plus par la combinaison de ces deux substitutions. Ces deux substitutions sont évidemment équivalentes à cette unique

$$\begin{pmatrix} \alpha\beta\gamma \\ \gamma\alpha\beta \end{pmatrix},$$

et celle-ci aux deux suivantes, appliquées successivement,

$$\begin{pmatrix} \alpha\beta \\ \beta\alpha \end{pmatrix} \text{ et } \begin{pmatrix} \beta\gamma \\ \gamma\beta \end{pmatrix}.$$

La valeur de v ne sera donc pas changée par la combinaison de ces deux substitutions. Donc

$$v = v\begin{pmatrix} \alpha\beta \\ \beta\alpha \end{pmatrix}\begin{pmatrix} \beta\gamma \\ \gamma\beta \end{pmatrix};$$

de même

$$v = v\begin{pmatrix} \beta\gamma \\ \gamma\beta \end{pmatrix}\begin{pmatrix} \gamma\delta \\ \delta\gamma \end{pmatrix},$$

d'où l'on tire

$$v = v\begin{pmatrix} \alpha\beta \\ \beta\alpha \end{pmatrix}\begin{pmatrix} \gamma\delta \\ \delta\gamma \end{pmatrix}.$$

On voit par là que la fonction v n'est pas changée par deux substitutions successives de la forme $\begin{pmatrix} \alpha\beta \\ \beta\alpha \end{pmatrix}$, α et β étant deux indices quelconques. Si l'on désigne une telle substitution par le nom de *transposition*, on peut conclure qu'une valeur quelconque de v ne sera pas changée par un nombre pair de transpositions, et que par conséquent toutes les valeurs de v qui résultent d'un nombre impair de transpositions sont égales. Tout échange des élémens d'une fonction peut s'opérer à l'aide d'un certain nombre de transpositions; donc la fonction v ne peut avoir plus de deux valeurs différentes. De là on tire le théorème suivant:

Le nombre des valeurs différentes que peut obtenir une fonction de n quantités, ne peut être abaissé au dessous du plus grand nombre premier qui ne surpasse pas n, à moins qu'il ne se réduise à 2 ou à 1.

Il est donc impossible de trouver une fonction de 5 quantités qui ait 3 ou 4 valeurs différentes.

La démonstration de ce théorème est prise d'un mémoire de M. *Cauchy* inséré dans le 17ième cahier du Journal de l'école polytechnique p. 1.

Soient v et v' deux fonctions dont chacune ait deux valeurs différentes, il suit de ce qui précède qu'en désignant par v_1, v_2 et v_1', v_2' ces doubles valeurs, les deux expressions

$$v_1 + v_2 \quad \text{et} \quad v_1v_1' + v_2v_2'$$

seront des fonctions symétriques. Soit

$$v_1 + v_2 = t \quad \text{et} \quad v_1v_1' + v_2v_2' = t_1,$$

on en tire

$$v_1 = \frac{tv_2' - t_1}{v_2' - v_1'}.$$

Soit maintenant le nombre des quantités $x_1, x_2 \ldots x_m$ égal à cinq, le produit

$$\varrho = (x_1-x_2)(x_1-x_3)(x_1-x_4)(x_1-x_5)(x_2-x_3)(x_2-x_4)(x_2-x_5)(x_3-x_4)(x_3-x_5)(x_4-x_5)$$

sera évidemment une fonction qui a deux valeurs différentes; la seconde valeur étant la même fonction avec le signe opposé. Donc en posant $v_1' = \varrho$, on aura $v_2' = -\varrho$. L'expression de v_1 sera donc

$$v_1 = \frac{t_1 + \varrho t}{2\varrho},$$

ou bien

$$v_1 = \tfrac{1}{2}t + \frac{t_1}{2\varrho^2}\varrho,$$

où $\frac{1}{2}t$ est une fonction symétrique; ϱ a deux valeurs qui ne diffèrent que par le signe, de sorte que $\frac{t_1}{2\varrho^2}$ est également une fonction symétrique.

Donc, en posant $\frac{1}{2}t = p$ et $\frac{t_1}{2\varrho^5} = q$, il s'ensuit que

toute fonction de cinq quantités qui a deux valeurs différentes pourra être mise sous la forme $p + q\varrho$, où p et q sont deux fonctions symétriques et $\varrho = (x_1 - x_2)(x_1 - x_3)\ldots(x_4 - x_5)$.

Pour atteindre notre but nous avons encore besoin de la forme générale des fonctions de cinq quantités qui ont cinq valeurs différentes. On peut la trouver comme il suit:

Soit v une fonction rationnelle des quantités x_1, x_2, x_3, x_4, x_5, qui ait la propriété d'être invariable lorsqu'on échange entre elles quatre des cinq quantités, par exemple x_2, x_3, x_4, x_5. Dans cette condition v sera évidemment symétrique par rapport à x_2, x_3, x_4, x_5. On peut donc exprimer v par une fonction rationnelle de x_1 et par des fonctions symétriques de x_2, x_3, x_4, x_5. Mais toute fonction symétrique de ces quantités peut s'exprimer par une fonction rationnelle des coefficiens d'une équation du quatrième degré, dont les racines sont x_2, x_3, x_4, x_5. Donc en posant

$$(x - x_2)(x - x_3)(x - x_4)(x - x_5) = x^4 - px^3 + qx^2 - rx + s,$$

la fonction v peut s'exprimer rationnellement en x_1, p, q, r, s. Mais si l'on pose

$$(x - x_1)(x - x_2)(x - x_3)(x - x_4)(x - x_5) = x^5 - ax^4 + bx^3 - cx^2 + dx - e,$$

on aura

$$\begin{aligned}(x - x_1)(x^4 - px^3 + qx^2 - rx + s) &= x^5 - ax^4 + bx^3 - cx^2 + dx - e\\ &= x^5 - (p + x_1)x^4 + (q + px_1)x^3 - (r + qx_1)x^2 + (s + rx_1)x - sx_1,\end{aligned}$$

d'où l'on tire

$$\begin{aligned}p &= a - x_1,\\ q &= b - ax_1 + x_1^2,\\ r &= c - bx_1 + ax_1^2 - x_1^3,\\ s &= d - cx_1 + bx_1^2 - ax_1^3 + x_1^4;\end{aligned}$$

la fonction v peut donc s'exprimer rationnellement en x_1, a, b, c, d.

Il suit de là que la fonction v peut être mise sous la forme

$$v = \frac{t}{\varphi x_1},$$

où t et φx_1 sont deux fonctions entières de x_1, a, b, c, d. En multipliant

le numérateur et le dénominateur de cette fonction par $\varphi x_2 . \varphi x_3 . \varphi x_4 . \varphi x_5$, on aura

$$v = \frac{t . \varphi x_2 . \varphi x_3 . \varphi x_4 . \varphi x_5}{\varphi x_1 . \varphi x_2 . \varphi x_3 . \varphi x_4 . \varphi x_5}.$$

Or $\varphi x_2 . \varphi x_3 . \varphi x_4 . \varphi x_5$ est, comme on le voit, une fonction entière et symétrique de x_2, x_3, x_4, x_5. On peut donc exprimer ce produit en fonction entière de p, q, r, s et par suite en fonction entière de x_1, a, b, c, d. Le numérateur de la fraction ci-dessus est donc une fonction entière des mêmes quantités; le dénominateur est une fonction symétrique de x_1, x_2, x_3, x_4, x_5 et par conséquent il peut s'exprimer en fonction rationnelle de a, b, c, d, e. On peut donc poser

$$v = r_0 + r_1 x_1 + r_2 x_1^2 + \cdots + r_m x_1^m.$$

En multipliant l'équation

$$x_1^5 = ax_1^4 - bx_1^3 + cx_1^2 - dx_1 + e$$

successivement par x_1, $x_1^2 \ldots x_1^{m-5}$, il est clair qu'on obtiendra $m - 4$ équations, desquelles on tirera pour x_1^5, $x_1^6 \ldots x_1^m$ des expressions de la forme

$$\alpha + \beta x_1 + \gamma x_1^2 + \delta x_1^3 + \varepsilon x_1^4,$$

où α, β, γ, δ, ε sont des fonctions rationnelles de a, b, c, d, e.

On peut donc réduire v à la forme

(a) $$v = r_0 + r_1 x_1 + r_2 x_1^2 + r_3 x_1^3 + r_4 x_1^4,$$

où r_0, r_1, r_2 etc. sont des fonctions rationnelles de a, b, c, d, e, c'est-à-dire des fonctions symétriques de x_1, x_2, x_3, x_4, x_5.

Voilà la forme générale des fonctions qui ne sont pas altérées lorsqu'on y échange entre elles les quantités x_2, x_3, x_4, x_5. Ou elles ont cinq valeurs différentes, ou elles sont symétriques.

Soit maintenant v une fonction rationnelle de x_1, x_2, x_3, x_4, x_5, qui ait les cinq valeurs suivantes v_1, v_2, v_3, v_4, v_5. Considérons la fonction $x_1^m v$. En y échangeant entre elles de toutes les manières possibles les quatre quantités x_2, x_3, x_4, x_5, la fonction $x_1^m v$ aura toujours une des valeurs suivantes

$$x_1^m v_1,\ x_1^m v_2,\ x_1^m v_3,\ x_1^m v_4,\ x_1^m v_5.$$

Or je dis, que le nombre des valeurs distinctes de $x_1^m v$ résultant de ces changements sera moindre que cinq. En effet, si toutes les cinq valeurs

avaient lieu, on tirerait de ces valeurs en échangeant x_1 successivement avec x_2, x_3, x_4, x_5, 20 valeurs nouvelles, qui seraient nécessairement différentes entre elles et des précédentes. La fonction aurait donc en tout 25 valeurs différentes, ce qui est impossible, car 25 n'est pas diviseur du produit 1.2.3.4.5. En désignant donc par μ le nombre des valeurs que peut prendre v lorsqu'on y échange entre elles les quantités x_2, x_3, x_4, x_5 de toutes les manières possibles, μ doit avoir l'une des quatre valeurs suivantes 1, 2, 3, 4.

1. Soit $\mu = 1$, d'après ce qui précède v sera de la forme (a).

2. Soit $\mu = 4$, la somme $v_1 + v_2 + v_3 + v_4$ sera une fonction de la forme (a). Or on a $v_5 = (v_1 + v_2 + v_3 + v_4 + v_5) - (v_1 + v_2 + v_3 + v_4) =$ une fonction symétrique moins $(v_1 + v_2 + v_3 + v_4)$; donc v_5 est de la forme (a).

3. Soit $\mu = 2$, $v_1 + v_2$ sera une fonction de la forme (a). Soit donc

$$v_1 + v_2 = r_0 + r_1 x_1 + r_2 x_1^2 + r_3 x_1^3 + r_4 x_1^4 = \varphi x_1 .$$

En échangeant successivement x_1 avec x_2, x_3, x_4, x_5, on aura

$$\begin{aligned} v_1 + v_2 &= \varphi x_1 , \\ v_2 + v_3 &= \varphi x_2 , \\ &\cdots\cdots\cdots \\ v_{m-1} + v_m &= \varphi x_{m-1} , \\ v_m + v_1 &= \varphi x_m , \end{aligned}$$

où m est un des nombres 2, 3, 4, 5. Pour $m = 2$, on aura $\varphi x_1 = \varphi x_2$, ce qui est impossible, car le nombre des valeurs de φx_1 doit être cinq. Pour $m = 3$ on aura

$$v_1 + v_2 = \varphi x_1 , \quad v_2 + v_3 = \varphi x_2 , \quad v_3 + v_1 = \varphi x_3 ,$$

d'où l'on tire

$$2v_1 = \varphi x_1 - \varphi x_2 + \varphi x_3 .$$

Mais le second membre de cette équation a plus de 5 valeurs, car il en a 30. On prouvera de la même manière que m ne peut être égal à 4 ni à 5. Il suit de là que μ n'est pas égal à 2.

4. Soit $\mu = 3$. Dans ce cas $v_1 + v_2 + v_3$ et par conséquent $v_4 + v_5 = (v_1 + v_2 + v_3 + v_4 + v_5) - (v_1 + v_2 + v_3)$ aura cinq valeurs. Mais on vient de voir que cette supposition est inadmissible. Donc μ ne peut non plus être égal à 3.

De tout cela on déduit ce théorème:

Toute fonction rationnelle de cinq quantités, qui a cinq valeurs différentes, aura nécessairement la forme

$$r_0 + r_1 x + r_2 x^2 + r_3 x^3 + r_4 x^4 ,$$

où r_0, r_1, r_2 etc. sont des fonctions symétriques, et x l'une quelconque des cinq quantités.

De l'équation

$$r_0 + r_1 x + r_2 x^2 + r_3 x^3 + r_4 x^4 = v$$

on déduira aisément, en faisant usage de l'équation proposée, pour la valeur de x, une expression de la forme suivante

$$x = s_0 + s_1 v + s_2 v^2 + s_3 v^3 + s_4 v^4 ,$$

où s_0, s_1, s_2 etc., de même que r_0, r_1, r_2 etc., sont des fonctions symétriques.

Soit v une fonction rationnelle qui ait m valeurs différentes v_1, v_2, $v_3 \ldots v_m$. En posant

$$\begin{aligned} &(v - v_1)(v - v_2)(v - v_3) \ldots (v - v_m) \\ &\quad = q_0 + q_1 v + q_2 v^2 + \cdots + q_{m-1} v^{m-1} + v^m = 0 , \end{aligned}$$

on sait que q_0, q_1, $q_2 \ldots$ sont des fonctions symétriques, et que les m racines de l'équation sont v_1, v_2, $v_3 \ldots v_m$. Or je dis, qu'il est impossible d'exprimer la valeur de v comme racine d'une équation de la même forme, mais d'un degré moins élevé. En effet soit

$$t_0 + t_1 v + t_2 v^2 + \cdots + t_{\mu-1} v^{\mu-1} + v^\mu = 0$$

une telle équation, t_0, t_1 etc. étant des fonctions symétriques, et soit v_1 une valeur de v qui satisfasse à cette équation, on aura

$$v^\mu + t_{\mu-1} v^{\mu-1} + \cdots = (v - v_1) P_1 .$$

En échangeant entre eux les élémens de la fonction, on trouvera la série suivante d'équations:

$$\begin{aligned} v^\mu + t_{\mu-1} v^{\mu-1} + \cdots &= (v - v_2) P_2 , \\ v^\mu + t_{\mu-1} v^{\mu-1} + \cdots &= (v - v_3) P_3 , \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ v^\mu + t_{\mu-1} v^{\mu-1} + \cdots &= (v - v_m) P_m . \end{aligned}$$

On en conclut que $v-v_1$, $v-v_2$, $v-v_3 \ldots v-v_m$ seront des facteurs de $v^\mu + t_{\mu-1}v^{\mu-1} + \cdots$ et que par conséquent μ doit nécessairement être égal à m. On en tire le théorème suivant:

Lorsqu'une fonction de plusieurs quantités a m valeurs différentes, on peut toujours trouver une équation du degré m, dont les coefficiens soient des fonctions symétriques, et qui ait ces valeurs pour racines; mais il est impossible de trouver une équation de la même forme d'un degré moins élevé qui ait une ou plusieurs de ces valeurs pour racines.

§ IV.

Démonstration de l'impossibilité de la résolution générale de l'équation du cinquième degré.

En vertu des propositions trouvées plus haut on peut énoncer ce théorème:

"Il est impossible de résoudre en général les équations du cinquième "degré."

D'après le § II, toutes les fonctions algébriques dont une expression algébrique des racines est composée, peuvent s'exprimer par des fonctions rationnelles des racines de l'équation proposée.

Comme il est impossible d'exprimer d'une manière générale la racine d'une équation par une fonction rationnelle des coefficiens, on doit avoir

$$\sqrt[m]{R} = v,$$

où m est un nombre premier et R une fonction rationnelle des coefficiens de l'équation proposée, c'est-à-dire une fonction symétrique des racines; v est une fonction rationnelle des racines. On en conclut

$$v^m - R = 0.$$

En vertu du § II, il est impossible d'abaisser le degré de cette équation; la fonction v doit donc, d'après le dernier théorème du paragraphe précédent, avoir m valeurs différentes. Le nombre m devant être diviseur du produit 1.2.3.4.5, ce nombre peut être égal à 2 ou à 3 ou à 5. Or (§ III) il n'existe pas de fonction de cinq variables qui ait 3 valeurs: il faut donc qu'on ait $m=5$, ou $m=2$. Soit $m=5$, on aura, ainsi qu'il résulte du paragraphe précédent

$$\sqrt[5]{R} = r_0 + r_1 x + r_2 x^2 + r_3 x^3 + r_4 x^4,$$

d'où

$$x = s_0 + s_1 R^{\frac{1}{5}} + s_2 R^{\frac{2}{5}} + s_3 R^{\frac{3}{5}} + s_4 R^{\frac{4}{5}}.$$

On en tire (§ II)

$$s_1 R^{\frac{1}{5}} = \tfrac{1}{5}(x_1 + \alpha^4 x_2 + \alpha^3 x_3 + \alpha^2 x_4 + \alpha x_5)$$

où $\alpha^5 = 1$. Cette équation est impossible, attendu que le second membre a 120 valeurs et que pourtant il doit être racine d'une équation du cinquième degré $z^5 - s_1^5 R = 0$. On doit donc avoir $m = 2$.

On aura donc (§ II)

$$\sqrt{R} = p + qs,$$

où p et q sont des fonctions symétriques, et

$$s = (x_1 - x_2) \ldots (x_4 - x_5).$$

On en tire, en échangeant x_1 et x_2 entre eux,

$$-\sqrt{R} = p - qs,$$

d'où l'on déduit $p=0$ et $\sqrt{R} = qs$. On voit par là, que toute fonction algébrique du premier ordre qui se trouve dans l'expression de la racine, doit nécessairement avoir la forme $\alpha + \beta\sqrt{s^2} = \alpha + \beta s$, où α et β sont des fonctions symétriques. Or il est impossible d'exprimer les racines par une fonction de la forme $\alpha + \beta\sqrt{R}$; il doit donc y avoir une équation de la forme

$$\sqrt[m]{\alpha + \beta\sqrt{s^2}} = v,$$

où α et β ne sont pas nuls, m est un nombre premier, α et β sont des fonctions symétriques, et v est une fonction rationnelle des racines. Cela donne

$$\sqrt[m]{\alpha + \beta s} = v_1, \quad \sqrt[m]{\alpha - \beta s} = v_2,$$

où v_1 et v_2 sont des fonctions rationnelles. On aura en multipliant v_1 par v_2,

$$v_1 v_2 = \sqrt[m]{\alpha^2 - \beta^2 s^2}.$$

Or $\alpha^2 - \beta^2 s^2$ est une fonction symétrique. Si maintenant $\sqrt[m]{\alpha^2 - \beta^2 s^2}$

n'est pas une fonction symétrique, le nombre m, d'après ce qui précède, doit être égal à deux. Mais dans ce cas v sera égal à $\sqrt{\alpha+\beta\sqrt{s^2}}$; v aura donc quatre valeurs différentes, ce qui est impossible.

Il faut donc que $\sqrt[m]{\alpha^2-\beta^2 s^2}$ soit une fonction symétrique. Soit γ cette fonction, on aura

$$v_2 v_1 = \gamma, \quad \text{et} \quad v_2 = \frac{\gamma}{v_1}.$$

Soit

$$v_1 + v_2 = \sqrt[m]{\alpha+\beta\sqrt{s^2}} + \frac{\gamma}{\sqrt[m]{\alpha+\beta\sqrt{s^2}}} = p = \sqrt[m]{R} + \frac{\gamma}{\sqrt[m]{R}} = R^{\frac{1}{m}} + \frac{\gamma}{R}R^{\frac{m-1}{m}}.$$

Désignons par $p_1, p_2, p_3 \ldots p_m$ les valeurs différentes de p qui résultent de la substitution successive de $\alpha R^{\frac{1}{m}}$, $\alpha^2 R^{\frac{1}{m}}$, $\alpha^3 R^{\frac{1}{m}} \ldots \alpha^{m-1} R^{\frac{1}{m}}$ à la place de $R^{\frac{1}{m}}$, α satisfaisant à l'équation

$$\alpha^{m-1} + \alpha^{m-2} + \cdots + \alpha + 1 = 0,$$

et faisons le produit

$$(p-p_1)(p-p_2)\ldots(p-p_m) = p^m - Ap^{m-1} + A_1 p^{m-2} - \cdots = 0.$$

On voit sans peine que A, A_1 etc. sont des fonctions rationnelles des coefficiens de l'équation proposée et par conséquent des fonctions symétriques des racines. Cette équation est évidemment irréductible. Il faut donc d'après le dernier théorème du paragraphe précédent que p, consideré comme fonction des racines, ait m valeurs différentes. On en conclut que $m=5$. Mais dans ce cas p sera de la forme (a) du paragraphe précédent. Donc on aura

$$\sqrt[5]{R} + \frac{\gamma}{\sqrt[5]{R}} = r_0 + r_1 x + r_2 x^2 + r_3 x^3 + r_4 x^4 = p,$$

d'où

$$x = s_0 + s_1 p + s_2 p^2 + s_3 p^3 + s_4 p^4,$$

c'est-à-dire, en mettant $R^{\frac{1}{5}} + \frac{\gamma}{R}R^{\frac{4}{5}}$ à la place de p,

$$x = t_0 + t_1 R^{\frac{1}{5}} + t_2 R^{\frac{2}{5}} + t_3 R^{\frac{3}{5}} + t_4 R^{\frac{4}{5}}$$

où t_0, t_1, t_2 etc. sont des fonctions rationnelles de R et des coefficiens de l'équation proposée. On en tire (§ II)

$$t_1 R^{\frac{1}{5}} = \tfrac{1}{5}(x_1 + \alpha^4 x_2 + \alpha^3 x_3 + \alpha^2 x_4 + \alpha x_5) = p',$$

où

$$\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = 0.$$

De l'équation $p' = t_1 R^{\frac{1}{5}}$ on tire $p'^5 = t_1^5 R$. Or $t_1^5 R$ étant de la forme $u + u'\sqrt{s^2}$ on aura $p'^5 = u + u'\sqrt{s^2}$, ce qui donne

$$(p'^5 - u)^2 = u'^2 s^2.$$

Cette équation donne p' par une équation du dixième degré, dont tous les coefficiens sont des fonctions symétriques; mais d'après le dernier théorème du paragraphe précédent cela est impossible; car puisque

$$p' = \tfrac{1}{5}(x_1 + \alpha^4 x_2 + \alpha^3 x_3 + \alpha^2 x_4 + \alpha x_5),$$

p' aurait 120 valeurs différentes, ce qui est une contradiction.

Nous concluons donc qu'il est impossible de résoudre algébriquement l'équation générale du cinquième degré.

Il suit immédiatement de ce théorème, qu'il est de même impossible de résoudre algébriquement les équations générales des degrés supérieurs au cinquième. Donc les équations des quatre premiers degrés sont les seules qui puissent être résolues algébriquement d'une manière générale.

APPENDICE.

ANALYSE DU MÉMOIRE PRÉCÉDENT.

Bulletin des sciences math., astr., phys. et chim. publié par le B^on *de Férussac*, t. 6, p. 347; Paris 1826.

L'auteur démontre, dans ce mémoire, qu'il est impossible de résoudre algébriquement l'équation générale du cinquième degré; car toute fonction

algébrique des coefficiens de la proposée, étant substituée à la place de l'inconnue, conduit à une absurdité. Dans un premier paragraphe, l'auteur cherche l'expression générale des fonctions algébriques de plusieurs quantités, d'après la définition qu'une fonction algébrique résulte, 1° d'additions, 2° de multiplications, 3° de divisions, et 4° d'extractions de racines dont les exposans sont des nombres *premiers*. Les soustractions, les élévations aux puissances et l'extraction des racines avec des exposans *composés* rentrent dans les opérations précédentes. D'où il résulte, 1° que toute fonction *rationnelle et entière* des quantités x_1, x_2, x_3 etc. c'est-à-dire, toute fonction qui peut être formée au moyen des *deux* premières opérations mentionnées, peut s'exprimer par une somme d'un nombre *fini* de termes de la forme $Ax_1^{m_1} x_2^{m_2} \ldots$, A étant une constante et m_1, m_2, ... des nombres entiers; 2° que toute fonction *rationnelle* des mêmes quantités, c'est-à-dire, toute fonction qui peut être formée au moyen des *trois* premières opérations, peut s'exprimer par un quotient de deux fonctions *entières*; 3° que toute fonction algébrique peut être formée par des répétitions des opérations indiquées par

$$(1) \qquad p' = f(x_1, x_2, x_3 \ldots p_1^{\frac{1}{n_1}}, p_2^{\frac{1}{n_2}}, \ldots),$$

où f désigne une fonction rationnelle des quantités entre les parenthèses; p_1, p_2, ... des fonctions rationnelles de x_1, x_2 ..., et n_1, n_2 ... des nombres premiers. On nommera, pour abréger, *fonction algébrique du premier ordre*, une fonction telle que p'. Si maintenant on formait une nouvelle fonction dans laquelle des fonctions du premier ordre entrassent de la même manière que p_1, p_2 ... entrent dans p', on aurait une *fonction algébrique du second ordre;* et, en général, une fonction de l'ordre μ serait celle qui pourrait contenir des fonctions de tous les ordres, jusqu'à l'ordre $\mu - 1$, combinées entre elles *algébriquement*. Bien entendu que cette fonction de l'ordre μ ne peut pas s'abaisser à un ordre inférieur, par des réductions des fonctions qui la composent. En outre, si cette même fonction de l'ordre μ contient m quantités de cet ordre, on dira qu'elle est du *$m^{\text{ième}}$ degré;* et en la désignant par v, on pourra poser

$$(2) \qquad v = q_0 + p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \ldots + q_{n-1} p^{\frac{n-1}{n}}$$

c'est-à-dire que l'on a ce premier *théorème: Toute fonction algébrique v de l'ordre μ et du degré m, peut être représentée par la formule* (2), *où n est un nombre premier, q_0, q_2, ... q_{n-1} des fonctions algébriques de l'ordre μ et du degré $m - 1$ tout au plus, et p une fonction algébrique de l'ordre $\mu - 1$,*

telle qu'il est impossible d'exprimer $p^{\frac{1}{n}}$ par une fonction rationnelle de p, q_0, q_2 ... q_{n-1}.

Après avoir ainsi trouvé l'expression générale des fonctions algébriques, l'auteur considère, dans un deuxième paragraphe, une équation quelconque dont les coefficiens sont des fonctions rationnelles des quantités x_1, x_2 ... et qu'on suppose résoluble algébriquement. En désignant donc par y l'inconnue, et par

$$(3) \qquad \varphi(x_1, x_2, x_3 \ldots y) = 0$$

l'équation même, il faut que le premier membre se réduise à zéro, en mettant pour y une certaine fonction de la forme (2). Par cette substitution l'équation (3) se changera en une autre de la forme

$$(4) \qquad r_0 + r_1 p^{\frac{1}{n}} + r_2 p^{\frac{2}{n}} + \ldots + r_{n-1} p^{\frac{n-1}{n}} = 0,$$

où r_0, r_1, r_2, r_3 ... sont des fonctions rationnelles de x_1, x_2, x_3 ... et de q_0, q_2, q_3 ... Cette équation entraine les suivantes:

$$(5) \qquad r_0 = 0,\ r_1 = 0,\ r_2 = 0, \ldots r_{n-1} = 0;$$

car dans le cas contraire, l'équation (4) pourrait donner la valeur de $p^{\frac{1}{n}}$ en fonction *rationnelle* de p, r_0, r_1 ... r_{n-1}, ce qui est contre l'énoncé du théorème précédent. Si les équations (5) ont lieu, l'équation (4) et par suite l'équation (3), seront de même satisfaites par toutes les valeurs de y qu'on obtiendra en mettant, au lieu de $p^{\frac{1}{n}}$ les $n-1$ valeurs $\alpha p^{\frac{1}{n}}$, $\alpha^2 p^{\frac{1}{n}}$, ... $\alpha^{n-1} p^{\frac{1}{n}}$, où α est une racine imaginaire de l'unité. Par là on aura les valeurs de n racines de l'équation (3), savoir

$$y_1 = q_0 + p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \ldots + q_{n-1} p^{\frac{n-1}{n}},$$
$$y_2 = q_0 + \alpha p^{\frac{1}{n}} + \alpha^2 q_2 p^{\frac{2}{n}} + \ldots + \alpha^{n-1} q_{n-1} p^{\frac{n-1}{n}},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$y_n = q_0 + \alpha^{n-1} p^{\frac{1}{n}} + \alpha^{n-2} q_2 p^{\frac{2}{n}} + \ldots + \alpha q_{n-1} p^{\frac{n-1}{n}};$$

ces équations donnent les n quantités $p^{\frac{1}{n}}$, q_0, q_2 ... q_{n-1} en fonctions *rationnelles* des racines y_1, y_2 ... y_n.

Si maintenant $fx = 0$ est une équation algébrique générale, résoluble *algébriquement*, et x_1, x_2 ... les racines de cette équation, on doit avoir

$$x = s_0 + v^{\frac{1}{n}} + s_2 v^{\frac{2}{n}} + \cdots + s_{n-1} v^{\frac{n-1}{n}},$$

cette formule étant analogue à la formule (2). D'après ce qu'on vient de voir $v^{\frac{1}{n}}$, s_0, $s_2 \ldots s_{n-1}$ seront des fonctions rationnelles des racines de l'équation proposée. Cela posé, considérons l'une quelconque des quantités v, s_0, $s_2 \ldots s_{n-1}$, par exemple v; en désignant par n' le nombre de toutes les valeurs *différentes* de v, qu'on obtiendra en échangeant entre elles de toutes les manières possibles les racines de l'équation proposée, on peut former une équation du degré n' qui ait toutes ces valeurs pour racines, et dont les coefficiens soient des fonctions rationnelles et symétriques des valeurs de v, et par suite des fonctions rationnelles de x_1, $x_2 \ldots$ En faisant donc

$$v = t_0 + u^{\frac{1}{\nu}} + t_2 u^{\frac{2}{\nu}} + \cdots + t_{\nu-1} u^{\frac{\nu-1}{\nu}},$$

toutes les quantités u, t_0, $t_2 \ldots t_{\nu-1}$ seront des fonctions rationnelles des valeurs de v, et par suite de x_1, $x_2 \ldots$ En poursuivant ce raisonnement, on établira le théorème suivant:

Deuxième théorème: Si une équation algébrique est résoluble algébriquement, on peut toujours donner à la racine une forme telle, que toutes les expressions algébriques dont elle est composée pourront s'exprimer par des fonctions rationnelles des racines de l'équation proposée.

Dans le troisième paragraphe on démontre, d'après un mémoire de M. *Cauchy*, inséré dans le cahier XVII^e du *Journal de l'École Polytechnique*, que, 1° le nombre des valeurs d'une fonction rationnelle de n quantités, ne peut s'abaisser au-dessous du plus grand nombre premier contenu dans n, sans devenir égal à 2 ou à 1; 2° que toute fonction rationnelle qui a deux valeurs différentes aura la forme

$$p + q(x_1 - x_2)(x_1 - x_3) \cdots (x_2 - x_3) \cdots (x_3 - x_4) \cdots$$

et que, si elle contient 5 quantités, elle deviendra

$$p + q(x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_1 - x_5)(x_2 - x_3)(x_2 - x_4)$$
$$(x_2 - x_5)(x_3 - x_4)(x_3 - x_5)(x_4 - x_5),$$

où p et q sont des fonctions invariables.

On démontre ensuite que toute fonction rationnelle de cinq quantités qui a cinq valeurs différentes peut être mise sous la forme

$$v = r_0 + r_1 x + r_2 x^2 + r_3 x^3 + r_4 x^4,$$

où r_0, $r_1 \ldots r_4$ sont des fonctions invariables, et x une des cinq quantités en question.

En combinant cette équation avec l'équation

$$(x - x_1)(x - x_2)(x - x_3)(x - x_4)(x - x_5)$$
$$= x^5 - ax^4 + bx^3 - cx^2 + dx - e = 0,$$

on en peut tirer les valeurs de x sous la forme

$$x = s_0 + s_1 v + s_2 v^2 + s_3 v^3 + s_4 v^4,$$

s_0, $s_1 \ldots$ étant des fonctions invariables de x_1, $x_2 \ldots$ Finalement on arrive à ce théorème connu: *Troisième théorème: Si une fonction rationnelle de plusieurs quantités x_1, $x_2 \ldots$ a m valeurs différentes, on pourra toujours trouver une équation du degré m dont tous les coefficiens sont des fonctions invariables de x_1, $x_2 \ldots$ et qui ont les m valeurs de la fonction pour racines; mais il est impossible de trouver une équation de la même forme d'un degré moins élevé, qui aura une ou plusieurs de ces valeurs pour racines.*

Au moyen des théorèmes établis dans les trois premiers paragraphes, l'auteur démontre ensuite, dans le quatrième, qu'il est impossible de résoudre algébriquement l'équation générale du cinquième degré.

En effet, en supposant que l'équation générale du cinquième degré soit résoluble algébriquement, on pourra, en vertu du théorème (1), exprimer toutes les fonctions algébriques dont une racine est composée, par des fonctions rationnelles des racines; donc, puisqu'il est impossible d'exprimer une racine d'une équation générale par une fonction rationnelle des coefficiens, il faut qu'on ait

$$R^{\frac{1}{m}} = v,$$

où $R^{\frac{1}{m}}$ est une des fonctions du premier ordre qui se trouvent dans l'expression de la racine, R étant une fonction rationnelle des coefficiens de l'équation proposée, c'est-à-dire, une fonction invariable des racines, et v une fonction rationnelle des mêmes racines. Cette équation donne $v^m - R = 0$; et pour v, m valeurs différentes, résultant du changement des racines entre elles. Maintenant le nombre des valeurs d'une fonction rationnelle de cinq variables, doit être diviseur du produit 2. 3. 4. 5; il faut donc que m, qui est un nombre premier, soit un des trois nombres 2, 3, 5; mais selon le

théorème cité de M. *Cauchy*, le nombre 3 sera exclu, et par conséquent il ne restera pour m que les deux valeurs 5 et 2.

1. Soit d'abord $m=5$; on aura, d'après ce qu'on a vu précédemment,

$$v=R^{\frac{1}{5}}=r_0+r_1x+r_2x^2+r_3x^3+r_4x^4,$$

et de là

$$x=s_0+s_1R^{\frac{1}{5}}+s_2R^{\frac{2}{5}}+s_3R^{\frac{3}{5}}+s_4R^{\frac{4}{5}},$$

s_0, s_1, ... étant, de même que R, des fonctions invariables des racines. Cette valeur donne, selon ce qui a été établi dans le deuxième paragraphe, pour $s_1R^{\frac{1}{5}}$, une fonction rationnelle des racines, savoir:

$$s_1R^{\frac{1}{5}}=\tfrac{1}{5}(x_1+\alpha^4x_2+\alpha^3x_3+\alpha^2x_4+\alpha x_5)=z,$$

α étant une racine imaginaire de l'équation $\alpha^5-1=0$; mais cela est impossible, car le second membre a 120 valeurs différentes, tandis qu'il doit être racine de l'équation $z^5-s_1^5R=0$, qui n'est que du cinquième degré. Le nombre m ne peut donc être égal à 5.

2. Soit $m=2$. Alors v aura deux valeurs qui, selon ce que M. *Cauchy* a démontré, doivent avoir la forme

$$v=p+qs=\sqrt{R},$$

où

$$s=(x_1-x_2)(x_1-x_3)\cdots(x_4-x_5),$$

et p et q sont des fonctions invariables.

En échangeant entre elles les deux racines x_1 et x_2, on aura $p-qs=-\sqrt{R}$, et par conséquent $p=0$, et par suite

$$\sqrt{R}=qs.$$

De là il suit que toutes les fonctions algébriques du premier ordre qui se trouvent dans l'expression de la racine, doivent être de la forme $\alpha+\beta\sqrt{s^2}$, où α et β sont des fonctions invariables. Maintenant il est impossible d'exprimer une racine de l'équation générale du cinquième degré, par une fonction de cette forme; par conséquent il faut qu'il y ait, dans l'expression de la racine, des fonctions du deuxième ordre, et qui doivent contenir un radical de la forme

$$\sqrt[m]{\alpha+\beta\sqrt{s^2}}=v,$$

où β n'est pas égal à zéro; m est un nombre premier et v une fonction rationnelle des racines. En changeant x_1 en x_2 on aura

$$\sqrt[m]{\alpha-\beta\sqrt{s^2}}=v_1,$$

ce qui donne $vv_1=\sqrt[m]{\alpha^2-\beta^2s^2}$. Maintenant $\alpha^2-\beta^2s^2$ est une fonction invariable; si donc vv_1 n'est pas de même une fonction invariable, il faut que m soit égal à 2; mais alors on aura $v=\sqrt{\alpha+\beta\sqrt{s^2}}$, ce qui donne pour v quatre valeurs différentes; or cela est impossible: donc il faut que vv_1 soit une fonction invariable. Soit cette fonction représentée par γ, on aura $v_1=\frac{\gamma}{v}$. Cela posé, considérons l'expression

$$v+v_1=\sqrt[m]{\alpha+\beta\sqrt{s^2}}+\frac{\gamma}{\sqrt[m]{\alpha+\beta\sqrt{s^2}}}=p=\sqrt[m]{R}+\frac{\gamma}{\sqrt[m]{R}}.$$

Cette valeur de p peut être racine d'une équation du $m^{\text{ième}}$ degré, et, comme cette équation sera nécessairement irréductible, p aura m valeurs différentes; donc m sera égal à 5.

Alors on aura

$$R^{\frac{1}{5}}+\gamma R^{-\frac{1}{5}}=r_0+r_1x+r_2x^2+r_3x^3+r_4x^4=p,$$

d'où

$$x=s_0+s_1p+\cdots+s_4p^4=t_0+t_1R^{\frac{1}{5}}+t_2R^{\frac{2}{5}}+t_3R^{\frac{3}{5}}+t_4R^{\frac{4}{5}},$$

t_0, t_1 ... t_4 étant des fonctions invariables. De là on tire, comme auparavant,

$$t_1R^{\frac{1}{5}}=\tfrac{1}{5}(x_1+\alpha^4x_2+\alpha^3x_3+\alpha^2x_4+\alpha x_5)=y,$$

$$y^5=t_1^5R=t_1^5(\alpha+\beta\sqrt{s^2}),$$

et

$$(y^5-\alpha t_1^5)^2-t_1^{10}\beta^2s^2=0.$$

Cette équation, dont les coefficiens sont des fonctions invariables, est du dixième degré par rapport à y; mais cela est contraire au théorème (3), parce que y a 120 valeurs différentes.

Nous concluons donc en dernier lieu, qu'il est impossible de résoudre algébriquement l'équation *générale* du cinquième degré. De là il suit immédiatement qu'il est, en général, impossible de résoudre algébriquement les équations générales d'un degré supérieur au quatrième.

VIII.

REMARQUE SUR LE MÉMOIRE N° 4 DU PREMIER CAHIER DU JOURNAL DE M. CRELLE.

Journal für die reine und angewandte Mathematik, herausgegeben von *Crelle*, Bd. I, Berlin 1826.

L'objet du mémoire est de trouver l'effet d'une force sur trois points donnés. Les résultats de l'auteur sont très justes, quand les trois points ne sont pas placés sur une même ligne droite; mais dans ce cas ils ne le sont pas. Les trois équations, par lesquelles les trois inconnues Q, Q', Q'' se déterminent, sont les suivantes

$$(1)\qquad \begin{cases} P = Q + Q' + Q'', \\ Q'b\sin\alpha = {}_{\alpha}{}''c\sin\beta, \\ Qa\sin\alpha = -Q''c\sin(\alpha+\beta). \end{cases}$$

Celles-ci ont lieu pour des valeurs quelconques de P, a, b, c, α et β. Elles donnent en général, comme l'auteur l'a trouvé,

$$(2)\qquad \begin{cases} Q = -\dfrac{bc\sin(\alpha+\beta)}{r}P, \\ Q' = \dfrac{ac\sin\beta}{r}P, \\ Q'' = \dfrac{ab\sin\alpha}{r}P, \end{cases}$$

où

$$r = ab\sin\alpha + ac\sin\beta - bc\sin(\alpha+\beta).$$

Or les équations (2) cessent d'être déterminées lorsque l'une ou l'autre des