Fragment d'un second Mémoire.

Des équations primitives qui sont solubles par radicaux.

Cherchons, en général, dans quel cas une équation primitive est soluble par radicaux. Or nous pouvons de suite établir un caractère général fondé sur le degré même de ces équations. 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. Et de là suivra immédiatement que, lorsqu'on aura à résoudre par radicaux une équation irréductible dont le degré admettrait des facteurs premiers inégaux, on ne pourra le faire que par la méthode de décomposition due à M. Gauss ; sinon l'équation sera insoluble.

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 cesse de l'être par l'adjonction d'un simple radical. En d'autres termes, nous pouvons supposer que, n étant premier, le groupe de l'équation se partage en n groupes irréductibles conjugués, mais non primitifs. Car, à moins que le degré de l'équation soit premier, un pareil groupe se présentera toujours dans la suite des décompositions.

Soit N le degré de l'équation, et supposons qu'après une extraction de racine de degré premier n, elle devienne non primitive et se partage en Q équations primitives de 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 rangeront en systèmes composés de P lettres conjointes chacun. Voyons 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 système de P lettres conjointes, et ne feront partie que d'un seul.

Car, en premier lieu, s'il y avait deux lettres qui ne pussent faire partie d'un même système de P lettres conjointes, le groupe G, qui est tel que l'une quelconque de ses substitutions transforme les unes dans les autres 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 différents, il s'ensuivrait que les groupes qui répondent aux divers systèmes de P lettres conjointes ne seraient pas primitifs ce qui est encore contre l'hypothèse.

Cela posé, soient

$$\begin{array}{cccccc} a_0, & a_1, & a_2, & \ldots, & a_{P-1} \\ b_0, & b_1, & b_2, & \ldots, & b_{P-1} \\ c_0, & c_1, & c_2, & \ldots, & c_{P-1} \end{array}$$

les N lettres : supposons que chaque ligne horizontale représente un système de lettres conjointes.

Soient

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

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

Soient, de même,

$$a_{1,0}, \quad a_{1.1}, \quad a_{1.2}, \quad \ldots, \quad a_{1.P-1}$$

P lettres conjointes toutes situées dans la seconde colonne verticale, en sorte que

$$a_{1.0}, \quad a_{1.1}, \quad a_{1.2}, \quad \ldots, \quad a_{1.P-1}$$

appartiennent respectivement aux mêmes lignes horizontales que

$$a_{0.0}, \quad a_{0.1}, \quad a_{0.2}, \quad \ldots, \quad a_{0.P-1}$$

soient, de même, les systèmes de lettres conjointes

$$\begin{array}{ccccc} a_{2.0}, & a_{2.1}, & a_{2.2}, & \ldots, & a_{2.P-1} \\ a_{3.0}, & a_{3.1}, & a_{3.2}, & \ldots, & a_{3.P-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \end{array}$$

nous obtiendrons ainsi, en tout, P^2 lettres. Si le nombre total des lettres n'est pas épuisé, on prendra un troisième indice, en sorte 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 conjointes ; et l'on parviendra ainsi à cette conclusion, que $N = P^\mu$, μ étant un certain nombre égal à celui des indices différents dont on aura besoin. La forme générale des lettres sera

$$a_{\underset{1}{k}.\underset{2}{k}.\underset{3}{k}.\ldots.\underset{\mu}{k}},$$

$\underset{1}{k}, \underset{2}{k}, \underset{3}{k}, \ldots, \underset{\mu}{k}$ étant des indices qui peuvent prendre chacun les P valeurs $0, 1, 2, 3, \ldots, P-1$.

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

$$\left[a_{\underset{1}{k}.\underset{2}{k}.\underset{3}{k}.\ldots.\underset{\mu}{k}}, \; , \quad a_{\underset{1}{\varphi(k)}.\underset{2}{\psi(k)}.\underset{3}{\chi(k)}.\ldots.\underset{\mu}{\sigma(k)}}, \right],$$

puisque chaque indice correspond à un système de lettres conjointes.

Si P n'est pas un nombre premier, on raisonnera sur le groupe de permutations de l'un quelconque des systèmes de lettres conjointes, comme sur le groupe G, en remplaçant chaque indice par un certain nombre de nouveaux indices, et l'on trouvera $P = R^\alpha$, et ainsi de suite ; d'où enfin $N = p^\nu$, p étant un nombre premier.

Des équations primitives de degré p^2.

Arrêtons-nous un moment pour traiter de suite les équations primitives d'un degré p^2, p étant premier impair. (Le cas de $p = 2$ a été examiné.) Si une équation du degré p^2 est soluble par radicaux, supposons-la d'abord telle, qu'elle devienne non primitive par une extraction de radical.

Soit donc G un groupe primitif de p^2 lettres qui se partage en n groupes non primitifs conjugués à H.

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

$$\begin{array}{cccccc} a_{0.0}, & a_{0.1}, & a_{0.2}, & a_{0.3}, & \ldots, & a_{0.p-1} \\ a_{1.0}, & a_{1.1}, & a_{1.2}, & a_{1.3}, & \ldots, & a_{1.p-1} \\ a_{2.0}, & a_{2.1}, & a_{2.2}, & a_{2.3}, & \ldots, & a_{2.p-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \\ a_{p-1.0}, & a_{p-1.1}, & a_{p-1.2}, & a_{p-1.3}, & \ldots, & a_{p-1.p-1} \end{array}$$

chaque ligne horizontale et chaque ligne verticale étant un système de lettres conjointes.

Si l'on permute entre elles les lignes horizontales, le groupe que l'on obtiendra, étant primitif et de degré premier, ne devra contenir que des substitutions de la forme

$$\left(a_{\substack{k.k \\ 1\ 2}}, a_{\substack{mk+n.k \\ 1\quad 2}}\right),$$

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

$$\left(a_{\substack{k.k \\ 1\ 2}}, a_{\substack{k.qk+r \\ 1\quad 2}}\right),$$

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

$$\left(a_{\substack{k.k \\ 1\ 2}}, a_{\substack{mk+n.mk+n \\ 1\ 1\quad 1\ 2\ 2\quad 2}}\right).$$

Si un groupe G se partage en n groupes conjugués à celui que nous venons de décrire, toutes les substitutions du groupe G devront transformer les unes dans les autres les substitutions circulaires du groupe H, qui sont toutes écrites comme il suit :

(a) $$\left(a_{\substack{k.k \\ 1\ 2}}, \ldots \quad a_{\substack{k+\alpha\ k+\alpha \\ 1\ 1\ 2\ 2}}, \ldots\right),$$

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

$$\begin{array}{ccc} \underset{1}{k} & & \varphi_1\left(\underset{1}{k}, \quad \underset{2}{k}\right) \\ & \text{par} & \\ \underset{2}{k} & & \varphi_2\left(\underset{1}{k}, \quad \underset{2}{k}\right) \end{array}$$

Si, dans les fonctions φ_1, φ_2, on substitue pour $\underset{1}{k}$ et $\underset{2}{k}$ les valeurs $\underset{1}{k}+\underset{1}{\alpha}$, $\underset{2}{k}+\underset{2}{\alpha}$, il devra venir des résultats de la forme

$$\varphi_1 + \vartheta_1, \quad \varphi_2 + \vartheta_2,$$

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

$$(A) \qquad \left(a_{\underset{1}{k}.\underset{2}{k}}, \quad a_{\underset{1}{m}\underset{1}{k}+\underset{1}{n}\underset{2}{k}+\underset{1}{\alpha}.\underset{2}{m}\underset{1}{k}+\underset{2}{n}\underset{1}{k}+\underset{2}{\alpha}}\right).$$

Or nous savons, par le n° [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. Si donc dans le groupe G on ne considère que les permutations où la lettre $a_{0.0}$ par exemple, conserve 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 c'est simplement pour la démonstration, que nous avons supposé que le groupe primitif G se partageât en groupes conjugués non primitifs. Comme cette condition n'est nullement nécessaire, les groupes seront souvent beaucoup plus composés.

Il s'agit donc de reconnaître dans quel cas ces groupes pourront admettre des substitutions où p^2-p lettres seulement varieraient, et cette recherche va nous retenir quelque temps.

Soit donc G un groupe qui contienne quelque substitution de l'ordre 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 l'ordre p^2-1 ; il suffit donc de la démontrer pour celles de l'ordre p^2-p. Ne considérons donc qu'un groupe où les substitutions seraient toutes m de l'ordre p^2 ou de l'ordre p^2-p. (*Voyez* l'endroit cité.)

Alors les p lettres qui, dans une substitution de l'ordre p^2-p, ne varieront pas, devront être des lettres conjointes.

Supposons que ces lettres conjointes soient

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

Nous pouvons déduire toutes les substitutions où ces p lettres ne changent pas de place, nous pouvons les déduire de substitutions de la forme

$$\left(a_{\underset{1}{k}.\underset{2}{k}}, \quad a_{\underset{1}{k}.\underset{2}{\varphi k}}\right),$$

et de substitutions de l'ordre p^2-p, dont la période serait de p termes. (*Voyez* encore l'endroit cité.)

[1] Ce Mémoire faisant suite à un travail de Galois que je ne possède pas, il m'est impossible d'indiquer le Mémoire cité ici et plus bas. A. Ch.

Les premiers doivent nécessairement, pour que le groupe jouisse de la propriété voulue, se réduire à la forme

$$\left(a_{\substack{k.k\\1\ 2}},\ \ a_{\substack{k.mk\\1\ 2}}\right),$$

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

Quant aux substitutions dont la période serait de p termes, comme elles sont conjuguées aux précédentes, nous pouvons supposer un groupe qui les contienne sans contenir celles-ci : donc elles devront transformer les substitutions circulaires (a) les unes dans les autres ; donc elles seront aussi linéaires.

Nous sommes donc arrivés à cette conclusion, que le groupe primitif de permutations de p^2 lettres doit ne contenir que des substitutions de la forme (A).

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

$$a_{\substack{k.k\\1\ 2}}$$

toutes les substitutions linéaires possibles, et cherchons quels sont les diviseurs de ce groupe qui peuvent jouir de la propriété voulue pour la résolubilité des équations.

Quel est d'abord le nombre total des substitutions linéaires ? Premièrement, il est clair que toute transformation de la forme

$$\underset{1\ 2}{k.k},\quad \underset{1\ 1}{mk}+\underset{1\ 2}{nk}+\underset{1}{\alpha}.\underset{2\ 1}{mk}+\underset{2\ 2}{nk}+\underset{2}{\alpha}$$

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 $a_{\substack{l.l\\1\ 2}}$ de la seconde permutation, et que l'on remonte à la lettre correspondante dans la première, on devra trouver une lettre $a_{\substack{k.k\\1\ 2}}$ où les indices $\underset{1\ 2}{k.k}$ seront parfaitement déterminés. Il faut donc que, quels que soient l_1 et l_2, on ait par les deux équations

$$\underset{1\ 1}{mk}+\underset{1\ 2}{nk}+\alpha_1=l_1,\ \ \underset{2\ 1}{mk}+\underset{2\ 2}{nk}+\alpha_{2=l_2,}$$

des valeurs de $\underset{1}{k}$ et $\underset{2}{k}$ finies et déterminées. Ainsi la condition pour qu'une pareille transformation soit réellement une substitution, est que $\underset{1\ 2}{mn}-\underset{2\ 1}{mn}$ ne soit ni nul ni divisible par le module p, ce qui est la même chose.

Je dis maintenant que, bien que ce groupe à substitutions linéaires n'appartienne pas toujours, comme on le verra, à des équations solubles par radicaux, il jouira toutefois de cette propriété, que si dans une quelconque de ses substitutions il y a n lettres de fixes, n divisera le nombre des lettres. Et, en effet, quel que soit le nombre des lettres qui restent fixes, on pourra exprimer cette circonstance par des équations linéaires qui donneront tous les indices de l'une des lettres fixes, au moyen d'un certain nombre d'entre eux. Donnant à chacun de ces indices, restés arbitraires, p valeurs, on aura p^m systèmes de valeurs, m étant un certain nombre. Dans le cas qui nous occupe,

m est nécessairement < 2, et se trouve par conséquent être 0 ou 1. Donc le nombre des substitutions ne saurait être plus grand que

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

Ne considérons maintenant que les substitutions linéaires où la lettre $a_{0.0}$ ne varie pas ; si, dans ce cas, nous trouvons le nombre total des permutations du groupe qui contient toutes les substitutions linéaires possibles, il nous suffira de multiplier ce nombre par p^2.

Or, premièrement, en substituant p à l'indice k_2, toutes les substitutions de la forme

$$\left(a_{\substack{k.k\\1\ 2}},\quad a_{\substack{mk.k\\1\ 1\ 2}}\right)$$

donneront en tout $p-1$ substitutions. On en aura p^2-p en ajoutant au terme k_2, le terme $\underset{2}{mk}$, ainsi qu'il suit :

$$(m') \qquad \left(\underset{1\ 2}{k.k},\quad \underset{1\ 1\ \ 2\ 1}{mk.mk} + \underset{2}{k}\right).$$

D'un autre côté, il est aisé de trouver un groupe linéaire de p^2-1 permutations, tel que, dans chacune de ses substitutions, toutes les lettres, à l'exception de $a_{0.0}$, varient. Car, en remplaçant le double indice $\underset{1\ 2}{kk}$ par l'indice simple $k_1 + ik_2$, i étant une racine primitive de

$$x^{p^2-1} - 1 = 0 \text{ (mod. } p),$$

il est clair que toute substitution de la forme

$$\left[a_{\substack{k+ki\\1\quad 2}},\quad a_{(\underset{1}{m}+\underset{2}{mi})(\underset{1}{k}+\underset{2}{ki})}\right]$$

sera 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 $a_{0.0}$. Combinant ces substitutions avec les p^2-p dont il est parlé plus haut, nous aurons

$$(p^2-1)(p^2-p) \text{ substitutions.}$$

Or, nous avons vu à priori que le nombre des substitutions où $a_{0.0}$ reste fixe 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 en tout

$$p^2(p^2-1)(p^2-p) \text{ permutations.}$$

Il reste à chercher les diviseurs de ce groupe, qui peuvent jouir de la propriété d'être solubles par radicaux. Pour cela, nous allons faire une transformation qui a pour but d'abaisser autant que possible les équations générales de degré p^2 dont le groupe serait linéaire.

Premièrement, comme les substitutions circulaires d'un pareil groupe sont telles, que toute autre substitution du groupe les transforme les unes dans les autres, on pourra abaisser l'équation d'un

degré, et considérer une équation de degré p^2-1 dont le groupe n'aurait que des substitutions de la forme

$$\left(b_{\substack{k,k\\1\,2}},\quad b_{\substack{mk+nk.mk+nk\\1\,1\quad 1\,2\quad 2\,1\quad 2\,2}}\right),$$

les p^2-1 lettres étant

$$\begin{array}{ccccc} & b_{0.1}, & b_{0.2}, & b_{0.3}, & \ldots, \\ b_{1.0}, & b_{1.1}, & b_{1.2}, & b_{1.3}, & \ldots, \\ b_{2.0}, & b_{2.1}, & b_{2.2}, & b_{2.3}, & \ldots, \\ \ldots & \ldots & \ldots & \ldots & \ldots \end{array}$$

J'observe maintenant que ce groupe est non primitif, en sorte que toutes les lettres où le rapport des deux indices est le même sont des lettres conjointes. Si l'on remplace par une seule lettre chaque système de lettres conjointes, on aura un groupe dont toutes les substitutions seront de la forme

$$\left(b_{\frac{k_1}{k_2}},\quad b_{\frac{m_1k_1+n_1k_2}{m_2k_2+n_2k_1}}\right),$$

$\frac{k_1}{k_2}$ étant les nouveaux indices. En remplaçant ce rapport par un seul indice k, on voit que les $p+1$ lettres seront

$$b_0,\quad b_1,\quad b_2,\quad b_3,\quad \ldots,\quad b_{p-1},\quad b_{\frac{1}{0}},$$

et les substitutions seront de la forme

$$\left(k,\quad \frac{mk+n}{rk+s}\right)$$

Cherchons combien de lettres, dans chacune de ces substitutions, restent à la même place ; il faut pour cela résoudre l'équation

$$(rk+s)k-m(mk+n)=0,$$

qui aura deux, ou une, ou aucune racine, suivant que $(m-s)^2+4nr$ sera résidu quadratique, nul ou non résidu quadratique. Suivant ces trois cas, la substitution sera de l'ordre $p-1$, ou p, ou $p+1$.

On peut prendre pour type des deux premiers cas les substitutions de la forme

$$(k, mk+n),$$

où la seule lettre $b_{\frac{1}{0}}$ ne varie pas, et de là on voit que le nombre total des substitutions du groupe réduit est

$$(p+1)p(p-1).$$

C'est après avoir ainsi réduit ce groupe, que nous allons le traiter généralement. Nous chercherons d'abord dans quel cas un diviseur de ce groupe, qui contiendrait des substitutions de l'ordre p, pourrait appartenir à une équation soluble par radicaux.

Dans ce cas, l'équation serait primitive et elle ne pourrait être soluble par radicaux, à moins que l'on n'eût $p+1=2^n$, n étant un certain nombre.

Nous pouvons supposer que le groupe ne contienne que des substitutions de l'ordre p et de l'ordre $p+1$. Toutes les substitutions de l'ordre $p+1$ seront par conséquent semblables, et leur période

sera de deux termes.

Prenons donc l'expression

$$\left(k, \quad \frac{mk+n}{rk+s}\right),$$

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

$$\left(k, \quad \frac{-sk+n}{rk-m}\right).$$

Donc on doit avoir $m = -s$, et toutes les substitutions en question seront

$$\left(k, \quad \frac{mk+n}{k-m}\right),$$

ou encore

$$k, \quad m + \frac{N}{k-m},$$

N étant un certain nombre qui est le même pour toutes les substitutions, puisque ces substitutions doivent être transformées les unes dans les autres par toutes les substitutions de l'ordre p, $(k, k+m)$; or ces substitutions doivent, de plus, être conjuguées les unes des autres. Si donc

$$\left(k, \quad m + \frac{N}{k-m}\right), \quad \left(k, \quad n + \frac{N}{k-n}\right)$$

sont deux pareilles substitutions, il faut que l'on ait

$$n + \frac{N}{\frac{N}{k-m} + m - n} = m + \frac{N}{\frac{N}{k-n} + n - m},$$

savoir,

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

Donc la différence entre deux valeurs de m ne peut acquérir que deux valeurs différentes ; donc m ne peut avoir plus de trois valeurs ; donc enfin $p = 3$. Ainsi, c'est seulement dans ce cas que le groupe réduit pourra contenir des substitutions de l'ordre p.

Et, en effet, la réduite sera alors du quatrième degré, et par conséquent soluble par radicaux.

Nous savons par là qu'en général, parmi les substitutions de notre groupe réduit, il ne devra pas se trouver de substitutions de l'ordre p. Peut-il y en avoir de l'ordre $p-1$? C'est ce que je vais rechercher[2].

---

[2] J'ai cherché inutilement dans les papiers de Galois la continuation de ce qu'on vient de lire.
A. Ch.