JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

CAMILLE JORDAN

Mémoire sur la résolution des équations algébriques les unes par les autres

Journal de mathématiques pures et appliquées 2^e série, tome 16 (1871), p. 1-20.
<http://www.numdam.org/item?id=JMPA_1871_2_16__1_0>

JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES.

Mémoire sur la résolution des équations algébriques les unes par les autres;

PAR M. CAMILLE JORDAN.

1. D'après la théorie des substitutions, on doit considérer toutes les équations dont le groupe est contenu dans un groupe donné T comme constituant un *type* caractérisé par ce groupe.

Les divers groupes t, t',... contenus dans le groupe T caractériseront autant de types particuliers, contenus dans le type plus général T.

Cela posé, l'une des questions les plus générales que l'on puisse se proposer sur les équations sera la suivante :

PROBLÈME. — *Déterminer les types les plus généraux d'équations irréductibles dont la résolution équivaut à celle d'équations auxiliaires appartenant à un type donné* T (*ou à certains types donnés* T, T',...).

En spécifiant le choix des types T, T',..., ce problème général donnera lieu à une infinité de questions particulières. On peut supposer, par exemple :

1° Que le degré des équations auxiliaires ne surpasse pas une limite donnée m;

2° Que leur ordre ne surpasse pas une limite donnée n;

3° Qu'aucun des facteurs premiers qui divisent cet ordre ne surpasse un nombre donné p;

4° Que chacun de leurs facteurs de composition soit un produit de facteurs premiers dont le nombre ne surpasse pas une limite donnée q. (Si $q = 1$, on aura le problème de la résolution par radicaux, dont nous avons donné ailleurs la solution.)

Etc.

Chacune de ces questions exige naturellement, pour être résolue, des considérations spéciales. On peut néanmoins établir certains théorèmes généraux, applicables à tous les cas, et qui resserrent notablement le problème. Ce sera l'objet du présent Mémoire.

Réduction du problème au cas des équations primitives.

2. Nous appellerons, pour abréger, *équations résolubles* celles dont la résolution équivaut à celle d'équations auxiliaires appartenant aux types donnés T, T',...; *groupes résolubles* ceux qui caractérisent ces équations.

3. LEMME. — *Si une équation* X, *ayant pour groupe* G, *est résoluble, toute équation* Y, *dont le groupe* H *est contenu dans* G, *ou isomorphe à* G, *le sera également.*

Supposons d'abord que H soit contenu dans G. Soient E, E',... les équations auxiliaires dont la résolution équivaut à celle de X; leurs racines seront, par définition, des fonctions rationnelles de celles de X, et, en les adjoignant à cette dernière équation, on réduira son groupe à celles de ses substitutions qui laissent ces fonctions invariables (*voir* notre *Traité des Substitutions*, n° **362**). Mais cette adjonction résout l'équation; donc G, et *à fortiori* H, ne contient aucune substitution qui laisse ces fonctions invariables, sauf la substitution 1. Cela posé, considérons les fonctions analogues aux précédentes, formées avec les racines de Y. Les équations e, e',... dont elles dépendent, ayant évidemment leurs groupes contenus dans ceux des équations E, E'..., appartiendront aux types T, T'.... D'autre

part, il est clair que leur adjonction résoudra Y, en réduisant son groupe à la substitution 1.

Supposons, en second lieu, que H soit isomorphe à G. Soit I le groupe formé par celles des substitutions de G auxquelles correspond dans H la substitution 1. Une fonction φ des racines de X, invariable par les substitutions de I et variable par toute autre substitution, dépendra d'une équation Z, dont le groupe K sera isomorphe à H sans mériédrie. On pourra donc déterminer une fonction rationnelle des racines de Z, qui ait pour groupe H (*Traité des Substitutions*, n^os^ **69-73**). L'équation U, dont dépend cette fonction, sera résolue par les équations E, E', ..., qui résolvent X; car ses racines sont des fonctions rationnelles de celles de X. L'équation Y, ayant le même groupe, sera résoluble par des équations appartenant aux mêmes types.

4. Soient maintenant X une équation résoluble, irréductible, mais non primitive; m le nombre des systèmes $x_1, y_1, \ldots; \ldots; x_m, y_m, \ldots$ entre lesquels se partagent ses racines; n le nombre des racines de chacun d'eux; G le groupe de X. Les substitutions de G seront, par définition, de la forme

$$U = RS_1 \ldots S_m, \quad U' = R'S'_1 \ldots S'_m, \ldots,$$

R, R', ... étant des substitutions qui permutent les systèmes entre eux, en remplaçant les unes par les autres les racines correspondantes, et S_α, S'_α, ... des substitutions qui permutent entre elles les racines du $\alpha^{ième}$ système, sans déplacer les autres. L'équation X étant irréductible, les substitutions de G permuteront transitivement les racines, et *à fortiori* les systèmes. On pourra d'ailleurs supposer que $x_\rho, y_\rho, \ldots$ représentent respectivement celles des racines du $\rho^{ième}$ système qui succèdent à $x_1, y_1, \ldots$ en vertu de l'une A_ρ des substitutions qui remplacent le premier système par le $\rho^{ième}$.

Cela posé, le groupe H_α formé par celles des substitutions de G qui ne déplacent pas le $\alpha^{ième}$ système, étant contenu dans G, sera résoluble (**3**). Le groupe Γ_α formé par les déplacements que ces substitutions font subir aux racines $x_\alpha, y_\alpha, \ldots$, étant isomorphe à H_α, sera

également résoluble (3). Il contient d'ailleurs chacune des substitutions $S_\alpha, S'_\alpha, \ldots$. En effet, supposons que U fasse succéder le système α au système β. La substitution $A_\alpha^{-1}A_\beta U$ appartient à H_α, et fait subir aux racines du $\alpha^{ième}$ système le déplacement S_α.

D'autre part, G étant résoluble, le groupe $\Delta = (R, R', \ldots)$, qui lui est isomorphe, sera résoluble. Enfin chacune des substitutions de Δ permute les uns dans les autres les groupes $\Gamma_\alpha, \Gamma_\beta, \ldots$. En effet, la substitution $U = RS_1 \ldots S_m$, remplaçant le système β par le système α, transformera H_β en H_α, et Γ_β en Γ_α; mais $S_1, \ldots, S_m$ sont évidemment permutables à Γ_α; donc R transforme Γ_β en Γ_α. C. Q. F. D.

Cela posé, le groupe dérivé de la combinaison des groupes Δ, $\Gamma_1, \ldots, \Gamma_m$ (ou, plus simplement, de Δ et de Γ_1, puisque $\Gamma_2, \ldots, \Gamma_m$ sont les transformés de Γ_1 par les substitutions de Δ) sera évidemment résoluble. Il contient d'ailleurs toutes les substitutions de G. Il se confondra donc avec G; sinon il caractériserait un type résoluble, plus général que le proposé, lequel ne satisferait plus à l'énoncé du problème.

On a donc cette proposition :

Théorème I. — *La construction des groupes résolubles, mais non primitifs, les plus généraux de degré* $M = mn$ *se ramène à la construction de deux groupes résolubles partiels, dont l'un* Δ *permute les m systèmes en remplaçant les unes par les autres les racines correspondantes, l'autre* Γ_1 *ne déplaçant que les racines du premier système, qu'il permute exclusivement entre elles.*

5. Réciproquement, étant donné deux groupes résolubles Δ et Γ_1, de degrés m et n, on pourra évidemment déduire de leur combinaison un groupe résoluble non primitif G de degré mn. Pour que G soit général, il faut évidemment que Δ et Γ_1 le soient également, chacun dans son espèce.

Si l'un des deux groupes Δ et Γ_1 n'est pas primitif, on ramènera de même sa construction à celle de deux groupes partiels; continuant ainsi, on pourra énoncer le théorème suivant :

Théorème II. — *La construction des groupes résolubles, mais non primitifs, les plus généraux de degré* M, *se ramène à la construction*

des groupes résolubles et primitifs les plus généraux ayant pour degrés les diviseurs de M.

Réduction du problème au cas des groupes primitifs et indécomposables.

6. Une équation X de degré n^m est dite *décomposable* lorsque, en caractérisant ses racines par m indices, $x_1, \ldots, x_m$, variables de 0 à $n-1$, les substitutions de son groupe G se réduisent toutes à la forme

$$U = | x_r \quad \varphi_r[x_{f(r)}] | ,$$

remplaçant ainsi chaque indice par une fonction d'un seul indice.

On aura évidemment $U = RS_1 \ldots S_m$, R étant la substitution qui remplace en général x_r par $x_{f(r)}$, et S_α la substitution qui remplace x_α par $\varphi_\alpha(x_\alpha)$ sans altérer les autres indices.

Soient donc $U = RS_1 \ldots S_m$, $U' = R'S'_1 \ldots S'_m, \ldots$ les substitutions de G. Les substitutions partielles R, R', ..., considérées isolément, permuteront transitivement les indices $x_1, \ldots, x_m$, si G est primitif, comme nous devons maintenant le supposer. En effet, si ces substitutions ne permutaient x_1 qu'avec les indices $x_1, \ldots, x_\alpha$, on pourrait répartir les racines en systèmes d'après les valeurs de ces indices, et chaque substitution de G remplacerait les racines de chaque système par celles d'un même système; donc G ne serait pas primitif.

On peut d'ailleurs supposer que, parmi celles des substitutions de G qui remplacent x_1 par des fonctions de x_ρ, il y en ait une, A_ρ, qui le remplace simplement par x_ρ; car, si A_ρ remplaçait x_1 par $\varphi_1(x_\rho)$, il suffirait, pour obtenir le résultat voulu, de prendre pour indice indépendant, à la place de x_ρ, l'expression $\varphi_1(x_\rho)$.

Cela posé, le groupe H_α, formé par celles des substitutions de G qui remplacent x_α par une fonction de x_α, étant contenu dans G, sera résoluble. Le groupe Γ_α, formé par les substitutions qui altèrent x_α de la même manière que celles de H_α, mais n'altèrent pas les autres indices, étant isomorphe à H_α, sera résoluble (3). Il contient d'ailleurs chacune des substitutions S_α, S'_α, ... En effet, soit, pour abréger, $f(\alpha) = \beta$. La substitution $A_\alpha A_\beta^{-1} U$ appartient à H_α, et fait subir à x_α l'altération S_α.

D'autre part, G étant résoluble, le groupe $\Delta = (R, R', \ldots)$, qui lui est isomorphe, sera résoluble. Enfin chacune des substitutions de Δ permute les uns dans les autres les groupes Γ_α, Γ_β, ... En effet, la substitution U, remplaçant x_α par une fonction de x_β, transformera évidemment H_β en H_α, et Γ_β en Γ_α; mais $S_1, \ldots, S_m$ sont évidemment permutables à Γ_α; donc R transforme Γ_β en Γ_α. C. Q. F. D.

Cela posé, le groupe dérivé de la combinaison des groupes Δ, $\Gamma_1, \ldots, \Gamma_m$ (ou, plus simplement, de Δ et de Γ_1) sera évidemment résoluble, et contiendra G. Ce dernier groupe étant supposé aussi général que possible, il se confondra avec lui.

On a donc cette proposition :

THÉORÈME. — *La construction des groupes résolubles, primitifs mais décomposables les plus généraux de degré n^m, se ramène à la construction de deux groupes résolubles partiels, dont l'un Δ permute les m indices entre eux, l'autre Γ_1 laissant tous les indices invariables, sauf le premier, x_1, que ses substitutions remplacent par des fonctions de x_1.*

7. La question de construire les deux groupes Δ et Γ_1 revient évidemment à résoudre le problème initial pour les degrés m et n. Réciproquement, ces groupes une fois construits d'une manière quelconque, on obtiendra évidemment, par leur combinaison, un groupe G résoluble et décomposable de degré n^m. Pour que G soit primitif, il faudra que Δ soit transitif, et Γ_1 primitif (*Traité*, n° **311**). Pour qu'il soit général, il faudra en outre que Δ et Γ_1 le soient également, chacun dans son espèce.

Si Γ_1 était décomposable, on ramènerait de nouveau sa construction à celle de deux groupes partiels Δ' et Γ'_1, et ainsi de suite. Supposons, pour fixer les idées, que Γ'_1 soit indécomposable. La question de construire les groupes Δ, Δ' revient au problème initial, mais avec un degré fort abaissé. La solution de ce problème serait donc complète si l'on savait construire, pour chaque degré, les groupes résolubles primitifs et indécomposables les plus généraux, tels que Γ'_1.

Cas des groupes primitifs et indécomposables.

8. THÉORÈME. — *Soient* G *un groupe quelconque;* G, H, I,..., K, 1 *une série de groupes tels, que chacun d'eux soit contenu dans le précédent et permutable aux substitutions de* G, *mais ne soit contenu dans aucun autre groupe plus général jouissant de cette double propriété. L'un quelconque de ces groupes, tel que* H, *résultera de la combinaison d'un ou plusieurs groupes partiels* $\mathfrak{H}_1, \mathfrak{H}_2, \ldots$ *ayant tous le même ordre, et jouissant des propriétés suivantes :*

1° *Les substitutions communes aux deux groupes*

$$\mathfrak{H}_\alpha \quad et \quad (\mathfrak{H}_1, \ldots, \mathfrak{H}_{\alpha-1}, \mathfrak{H}_{\alpha+1}, \ldots)$$

seront celles du groupe I, *qui succède à* H *dans la suite* G, H, I,..., K, 1;

2° *Les substitutions de* $\mathfrak{H}_\alpha$ *sont échangeables à celles de* $\mathfrak{H}_\beta$ *aux substitutions près de* I, *si* $\alpha \gtrless \beta$;

3° *Chacun des groupes* $\mathfrak{H}_1, \mathfrak{H}_2, \ldots$ *se réduit à* I *par la suppression d'un de ses facteurs de composition.*

Soit H_1 un groupe qui soit plus général que I, contenu dans H et permutable à ses substitutions, et qui ne contienne aucun autre groupe jouissant des mêmes propriétés. Soient $H_1, H_2, \ldots$ les groupes transformés de H_1 par les substitutions de G. Ces substitutions étant permutables à H, qui contient H_1, le groupe $(H_1, H_2, \ldots)$ sera contenu dans H. Il est d'ailleurs plus général que I; enfin il est permutable aux substitutions de G (car, si une substitution t de G transforme H_α en H', en la combinant avec la substitution s qui transforme H_1 en H_α, on obtient une substitution st, appartenant à G, et qui transforme H_1 en H'; donc H' est un des groupes de la suite $H_1, H_2 \ldots$). Or il n'existe, par hypothèse, aucun groupe intermédiaire entre H et I qui jouisse de ces propriétés. On aura donc $H = (H_1, H_2, \ldots)$.

Si quelques-uns des groupes $H_1, H_2, \ldots$ sont dérivés de la combinaison des autres, on pourra les effacer. Soient $H_\alpha, H_\beta, \ldots$ les groupes restants; on aura plus simplement $H = (H_\alpha, H_\beta, \ldots)$.

Le groupe H_1 contenant I, auquel les substitutions de G sont per-

mutables, ses transformés H_α, H_β,.. et par suite chacun des deux groupes H_α, $(H_\beta, \ldots)$ contiendront I, qui est son propre transformé. Mais ces deux groupes n'auront aucune autre substitution commune. En effet, soit g_α la substitution de G qui transforme H_1 en H_α; H_α sera permutable aux substitutions du groupe transformé de H par g_α, lequel n'est autre que H. On voit de même que les substitutions de H sont permutables à chacun des groupes $H_\beta, \ldots$; elles le seront donc au groupe J_α formé des substitutions communes à H_α et à $(H_\beta, \ldots)$. Mais H_α n'est pas contenu dans $(H_\beta, \ldots)$, sans quoi on l'aurait effacé; donc J_α sera moins général que H_α, quoique contenant I et permutable aux substitutions de H; son transformé J_1 par la substitution s^{-1} sera moins général que H_1, contiendra I qui est son propre transformé, et sera permutable aux substitutions de H. Mais il n'existe, par hypothèse, aucun groupe intermédiaire entre H_1 et I qui jouisse de ces propriétés; donc J_1, et par suite J_α, se réduit à I.

Enfin, les substitutions de H_α sont échangeables aux I près à celles de chacun des groupes H_1, $H_2, \ldots$, $H_{\alpha-1}, \ldots$, $H_{\alpha+1}, \ldots$. Soient, en effet, h_α, h_β deux substitutions prises respectivement dans H_α et H_β; la substitution $h_\alpha^{-1}.h_\beta^{-1}h_\alpha h_\beta = h_\alpha^{-1}h_\beta^{-1}h_\alpha.h_\beta$ appartiendra à H_α, auquel h_β est permutable, et à H_β, auquel h_α est permutable. Elle appartiendra donc au groupe I, formé par les substitutions communes à ces deux groupes.

9. Les groupes H_α, $H_\beta, \ldots$ satisfont donc à deux des conditions imposées aux groupes $\mathfrak{H}_1$, $\mathfrak{H}_2, \ldots$. S'il n'existe aucun groupe plus général que I, contenu dans H_α et permutable à ses substitutions, le groupe H_α, et par suite ses transformés $H_\beta, \ldots$ satisferont également à la troisième condition.

Supposons, au contraire, qu'il existe un semblable groupe $H_{\alpha 1}$; on pourra le déterminer de telle sorte qu'il ne contienne aucun groupe plus général que I et jouissant des mêmes propriétés. Soient alors $H_{\alpha 1}$, $H_{\alpha 2}, \ldots$ les groupes transformés de $H_{\alpha 1}$ par les diverses substitutions de H. On verra, en répétant les raisonnements précédents, sauf à y remplacer G et H par H et H_α : 1° que H_α résulte de la combinaison des groupes partiels $H_{\alpha 1}$, $H_{\alpha 2}, \ldots$; 2° qu'en effaçant ceux de ces groupes qui dérivent de la combinaison des autres, les groupes restants $H_{\alpha a}$,

$H_{\alpha b}, \ldots$ contiennent les substitutions de I, mais qu'il n'existe aucune autre substitution commune aux deux groupes $H_{\alpha a}$ et $(H_{\alpha b}, \ldots)$; 3° que les substitutions de $H_{\alpha a}$ sont échangeables aux I près à celles de $H_{\alpha b}$.

Les groupes $H_{\alpha a}, H_{\alpha b}, \ldots$ et leurs transformés $H_{\beta a}, H_{\beta b}, \ldots; \ldots$ par les substitutions de G, qui transforment H_α en $H_\beta, \ldots$, formeront donc un système de groupes partiels dont H est dérivé, et qui satisfont à deux des conditions imposées aux groupes $\mathcal{S}_1$, $\mathcal{S}_2, \ldots$. Ils satisferont en outre à la troisième, s'il n'existe aucun groupe plus général que I contenu dans $H_{\alpha a}$ et permutable à ses substitutions.

S'il existait, au contraire, un semblable groupe $H_{\alpha a_1}$, on continuerait le raisonnement comme tout à l'heure, en y remplaçant G et H par H_α et $H_{\alpha a}$; et, comme les groupes décroissants H, H_α, $H_{\alpha a}, \ldots$ ne peuvent former une suite indéfinie, le théorème sera nécessairement vrai.

10. Le dernier groupe de la suite G, H, I,..., K, 1 ne contenant d'autre substitution que l'unité, l'énoncé du théorème précédent se simplifiera pour le groupe précédent K. On aura ainsi la proposition suivante :

Le groupe K (*contenu dans* G *et permutable à ses substitutions, mais ne contenant aucun groupe moindre qui jouisse des mêmes propriétés*) *résulte de la combinaison d'un ou plusieurs groupes simples* $K_1, K_2, \ldots, K_n$. *Si* $n > 1$, *les substitutions de ces groupes seront mutuellement échangeables. Ces groupes auront d'ailleurs le même ordre* q, *et chacun d'eux n'aura aucune substitution commune* (*sauf l'unité*) *avec le groupe qui résulte de la combinaison des autres groupes partiels.*

On en conclut immédiatement qu'en désignant les substitutions de K_α par $k_{\alpha 1} \ldots, k_{\alpha q}$, les substitutions de K seront en nombre q^n, et de la forme générale $k_{1a} k_{2b} \ldots$.

On remarquera enfin que q est l'un des facteurs de composition de l'équation X, qui a pour groupe G. Cette équation est résoluble, par hypothèse, à l'aide d'équations auxiliaires E, E',... appartenant aux types T, T',.... Pour cela, il faudra que l'une de ces équations auxiliaires ait un facteur de composition égal à q.

11. Deux cas seront ici à distinguer :

PREMIER CAS. — *Les substitutions de* K_1 *sont échangeables entre elles.*

Soit k_1 une substitution d'ordre premier p, contenue dans K_1. Les puissances de k_1 forment un groupe contenu dans K_1 et permutable aux substitutions de K. Mais il n'existe, par hypothèse, aucun groupe moindre que K_1 et jouissant de ces propriétés; donc K_1 se réduit aux puissances de k_1, et son ordre q se réduit à p. Les groupes $K_1, K_2, \ldots$, transformés de K_1 par les substitutions de G, se réduiront aux puissances des substitutions $k_1, k_2, \ldots$ transformées de k_1. Ces substitutions étant échangeables entre elles, les substitutions de K seront toutes d'ordre p, et échangeables entre elles.

Les substitutions de K permutent transitivement les racines, sans quoi G ne serait pas primitif (*Traité*, n° 53). On en conclut que chaque substitution de K (sauf l'unité) déplace toutes les racines. En effet, si l'une d'elles s laisse immobile une racine a, soient b une autre racine quelconque, t une substitution de K qui remplace a par b; $s = t^{-1}st$ laissera b immobile, et par suite se réduira à l'unité.

Le groupe K ne contient qu'une substitution t qui remplace a par b; car, s'il en contenait une autre, u, il contiendrait tu^{-1}, qui laisse a immobile, sans se réduire à l'unité. L'ordre p^n de K sera donc précisément égal au nombre des racines $a, b, \ldots$.

Désignons ces racines par n indices $x, y, \ldots$ variables de 0 à $p-1$. Choisissons arbitrairement la racine à laquelle nous donnerons les indices 0, 0, ..., et désignons par $(xy\ldots)$ celle que la substitution $k_1^x k_2^y \ldots$ lui fait succéder. L'égalité évidente

$$k_1^x k_2^y \ldots k_1^\alpha k_2^\beta \ldots = k_1^{x+\alpha} k_2^{y+\beta} \ldots$$

montre que la substitution $k_1^\alpha k_2^\beta \ldots$ remplacera $(xy\ldots)$ par

$$(x+\alpha,\ y+\beta, \ldots).$$

Donc les substitutions de K seront de la forme

$$\left| x, y, \ldots \quad x+\alpha,\ y+\beta, \ldots \right|,$$

et celles de G, qui lui sont permutables, seront de la forme linéaire

$$| x, y, \ldots \quad ax + a'y + \ldots + \alpha, \; bx + b'y + \ldots + \beta, \ldots | .$$

12 SECOND CAS. — *Les substitutions de* K_1 *ne sont pas échangeables entre elles.*

Chacune des substitutions de G *transformera les groupes* $K_1, K_2, \ldots$ *les uns dans les autres.* — Soit, en effet, g une de ces substitutions; et supposons que le groupe L, transformé de K_1 par g, ne soit pas l'un des groupes $K_1, K_2, \ldots$. Le groupe K étant son propre transformé par g, ses substitutions seront permutables à L, ainsi qu'à $K_1, K_2, \ldots$. Elles seront donc permutables au groupe J_α formé par les substitutions communes à L et à K_α; elles le seront donc au groupe J_1, transformé de J_α par la substitution de G qui transforme K, K_α en K, K_1. Mais, par hypothèse, K_1 ne contient aucun groupe moindre permutable aux substitutions de K (sauf celui qui se réduit à la substitution 1); donc J_1, et par suite J_α, se réduit à cette substitution.

Cela posé, soient l et k_α deux substitutions prises respectivement dans L et dans K_α. La substitution $l^{-1}.k_\alpha^{-1}lk_\alpha = l^{-1}k_\alpha^{-1}l.k_\alpha$, étant commune à L et à K_α, se réduira à l'unité; donc l est échangeable à k_α.

Ainsi les substitutions de L sont échangeables à toutes celles de K_1, $K_2, \ldots$, dont K est dérivé. Celles des substitutions de K qui jouissent de cette propriété forment évidemment un groupe M. Le groupe M', transformé de M par une substitution quelconque de G, aura ses substitutions échangeables à celles de K, qui est son propre transformé; donc $M' = M$. Mais il n'existe, par hypothèse, aucun groupe moindre que K et permutable aux substitutions de G; donc $M = K$. Donc les substitutions de K, et *à fortiori* celles de K_1, seraient échangeables entre elles, contre l'hypothèse.

13. Cela posé, admettons en premier lieu que K_1 soit transitif. Son ordre q sera un multiple du nombre μ des racines (*Traité*, n° **44**). On aura d'ailleurs $\mu = q$, si le nombre n des groupes $K_1, K_2, \ldots$ surpasse l'unité, et, dans aucun cas, n ne pourra surpasser 2.

En effet, les groupes $K_1, \ldots, K_n$, transformés de K_1, seront transitifs comme lui; et chacune de leurs substitutions (l'unité exceptée) dé-

placera toutes les racines. Car soient s une substitution de K_1, qui laisse immobile une racine a, b une autre racine quelconque, t une substitution de K_2, qui remplace a par b, $t^{-1}st = s$ laissera b immobile; donc s, ne déplaçant aucune racine, se réduit à l'unité.

Il résulte de là que K_1 est l'un des groupes signalés dans notre *Traité* (**71-75**). Le groupe transitif K_2, dont les substitutions sont échangeables à celles de K_1, sera le *conjoint* de K_1 (*Ibid.*, **75**).

Enfin, $n < 3$; car, s'il en était autrement, K_1 et K_3 étant tous deux conjoints à K_2, d'après ce qui précède, seraient identiques. Mais les substitutions de K_1 sont échangeables à celles de K_3; elles le seraient donc entre elles, contrairement à l'hypothèse actuelle.

14. Supposons, au contraire, que K_1 ne soit pas transitif. Soient $L_1 = (K_a, \ldots)$, $L'_1 = (K_{a'}, \ldots), \ldots$ des groupes quelconques dérivés chacun de la combinaison de quelques-uns des groupes K_1, $K_2, \ldots$. On pourra grouper les racines en systèmes S_1, $S'_1 \ldots$ en réunissant ensemble celles qui sont permutées entre elles par les substitutions de chacun des groupes L_1, $L'_1, \ldots$. Les substitutions de K étant permutables à chacun des groupes $K_a, \ldots$, $K_{a'}, \ldots$, le seront à L_1, $L'_1, \ldots$; elles remplaceront donc les racines de chaque système par celles d'un même système. D'ailleurs, K étant transitif (**11**), ses substitutions permutent transitivement les systèmes S_1, $S'_1, \ldots$; donc ils contiendront tous un même nombre μ de racines.

Connaissant deux semblables groupements en systèmes S_1, $S'_1, \ldots$ et S_2, $S'_2, \ldots$ respectivement correspondants aux groupes L_1, $L'_1, \ldots$ et L_2, $L'_2, \ldots$, on en déduira immédiatement deux autres.

Le premier s'obtient en groupant ensemble les racines qui appartenaient à un même système dans chacun des deux groupements donnés, et qui, par suite, sont permutées entre elles par les substitutions de chacun des groupes L_1, $L'_1, \ldots, L_2$, $L'_2, \ldots$.

Pour obtenir le second, on groupera ensemble, en un seul système plus général, tous ceux des systèmes S_1, $S'_1, \ldots$ qui sont permutés ensemble par les substitutions de chacun des groupes L_2, $L'_2, \ldots$. Les substitutions de K, étant permutables à $L_2, \ldots$, remplaceront évidemment les racines de chacun de ces nouveaux systèmes par celles d'un même nouveau système. Il est clair d'ailleurs que ces nouveaux

systèmes seront caractérisés par la propriété que les racines de chacun d'eux soient permutées entre elles par les substitutions de chacun des groupes (L_1, L_2), (L_1, L'_2),..., (L'_1, L_2), (L'_1, L'_2),....

15. Cela posé, parmi les diverses manières de choisir les groupes $L_1, L'_1,\ldots$, prenons l'une de celles pour lesquelles μ est *minimum*, tout en restant supérieur à 1; μ sera inférieur au nombre total des racines, car il est au plus égal au nombre des racines que permutent ensemble les substitutions du groupe non transitif K_1. On aura donc plusieurs systèmes $S_1, S'_1,\ldots$.

Soient maintenant $g_1 = 1, g_2,\ldots, g_\rho,\ldots$ les diverses substitutions de G; $S_1, S'_1,\ldots$; $S_2, S'_2,\ldots$; ...; $S_\rho, S'_\rho,\ldots$; ... les divers systèmes de racines par lesquels elles remplacent respectivement les systèmes $S_1, S'_1,\ldots$. Le groupe K étant permutable à $g_1,\ldots, g_\rho,\ldots$, il est clair que ses substitutions remplacent les racines de chacun des systèmes $S_\rho, S'_\rho,\ldots$ par celles d'un même système, et que ce nouveau groupement des racines en systèmes correspondra aux groupes $L_\rho, L'_\rho,\ldots$ transformés de $L_1, L'_1,\ldots$ par g_ρ.

Le groupe G étant primitif, l'une au moins de ses substitutions g_2 ne remplacera pas les systèmes $S_1, S'_1,\ldots$ les uns par les autres. Cela étant, les μ racines de chacun des systèmes $S_2, S'_2,\ldots$ appartiendront à μ systèmes différents de la suite $S_1, S'_1,\ldots$. Supposons en effet que ν racines de S_2 appartinssent à S_1, par exemple. Des deux groupements en systèmes $S_1, S'_1,\ldots$ et $S_2, S'_2,\ldots$ on en déduirait un troisième où l'un des systèmes serait exclusivement formé de ces ν racines communes (**14**); μ ne serait donc pas le minimum supposé, à moins que l'on n'eût $\nu = \mu$, d'où $S_1 = S_2$. Mais alors les systèmes $S_1, S'_1,\ldots$ se confondraient, à l'ordre près, avec $S_2, S'_2,\ldots$ (résultat inadmissible). En effet, soit k une substitution de K qui remplace $S_1 = S_2$ par un autre système S'^r_1 de la suite $S_1, S'_1,\ldots$; elle doit le remplacer par un autre système S'^s_2 de la suite $S_2, S'_2,\ldots$; donc $S'^r_1 = S'^s_2$.

Cela posé, en combinant les deux groupements $S_1, S'_1,\ldots$ et $S_2, S'_2,\ldots$, on obtiendra un nouveau groupement en systèmes $S_{12}, S'_{12},\ldots$ contenant chacun μ^2 racines (**14**). Considérons maintenant l'un des systèmes $S_3, S'_3,\ldots$. S'il n'est pas contenu en entier dans l'un des systèmes $S_{12}, S'_{12},\ldots$, ses μ racines appartiendront à μ systèmes différents. Car si ν d'entre les racines de S_3 appartiennent à S_{12}, on obtiendra (**14**)

un nouveau groupement en systèmes formés de ν racines; et si ν était $< \mu$ mais > 1, μ ne serait pas le minimum supposé.

Supposons, pour fixer les idées, que les racines de S_3 appartiennent à μ systèmes différents de la suite $S_{12}, S'_{12}, \ldots$ Le procédé du n° **14** permettra de trouver un nouveau groupement en systèmes S_{123}, S'_{123}, formés chacun de la réunion de μ des systèmes $S_{12}, S'_{12}, \ldots$ et contenant ainsi μ^3 racines.

On continuerait à raisonner de la même manière si, parmi les systèmes $S_4, S'_4, \ldots, \ldots; S_\rho, S'_\rho, \ldots; \ldots$, il en existait un dont les racines ne fussent pas contenues dans un seul des systèmes $S_{123}, S'_{123}, \ldots$. Adoptons donc, pour fixer les idées, l'hypothèse contraire. Chaque substitution g du groupe G permute les unes dans les autres les suites $S_1, S'_1, \ldots; \ldots; S_\rho, S'_\rho, \ldots; \ldots$. Elle remplacera donc chacun des systèmes $S_{123}, S'_{123}, \ldots$, dont les racines sont associées exclusivement entre elles dans les systèmes de chacune de ces suites, par un système qui jouira de la même propriété, et qui, en conséquence appartiendra à la suite $S_{123}, S'_{123}, \ldots$.

Mais G est primitif; donc les systèmes $S_{123}, S'_{123}, \ldots$ se réduiront à un seul, et le nombre total des racines sera ici égal à μ^3 (plus généralement à une puissance de μ, telle que μ^m).

16. Cela posé, on pourra distinguer les μ systèmes $S_{12}, S'_{12}, \ldots$ les uns des autres par un indice x, variable de 0 à $\mu - 1$. De même, en combinant les deux groupements $S_2, S'_2, \ldots$ et $S_3, S'_3, \ldots$, on obtiendra un nouveau groupement en μ systèmes $S_{23}, S'_{23}, \ldots$, (contenant chacun μ^2 racines), que l'on pourra distinguer par un second indice y. Enfin, on obtiendra d'une manière analogue un nouveau groupement en μ systèmes $S_{31}, S'_{31}, \ldots$, que l'on distinguera par un dernier indice z.

On pourrait, d'après le n° **14**, obtenir un nouveau groupement de racines en systèmes, en réunissant celles qui appartiennent au même système dans chacun des trois groupements $S_{12}, S'_{12}, \ldots; S_{23}, S'_{23}, \ldots; S_{31}, S'_{31}, \ldots$, et qui, par suite, ont les mêmes indices x, y, z. Mais il est aisé de voir que ces nouveaux systèmes ne contiennent chacun qu'une racine. En effet, les racines de S_3, et, *a fortiori*, les μ^2 racines de S_{23}, appartiennent au moins à μ systèmes différents de la suite $S_{12}, S'_{12}, \ldots$. Donc, chacun des systèmes de cette suite, tel que S_{12}, aura tout au plus μ racines communes avec S_{23}. Mais ces deux systèmes ont préci-

sément en commun les μ racines de S_2. Ces racines appartiendront à μ systèmes différents de la suite S_{31}, S'_{31},... ; car, s'il en était autrement, le nombre des racines se réduirait à μ^2, au lieu d'être égal à μ^3 (**15**). Donc chacun des systèmes S_{31}, S'_{31},... ne contient qu'une racine qui soit en même temps contenue dans S_{12} et dans S_{23}.

Les racines pourront donc être caractérisées par les divers systèmes de valeurs des indices x, y, z. Cela posé, les substitutions de K, remplaçant les racines de chacun des systèmes S_{12}, S'_{12},... par celles d'un même système, remplaceront x par une fonction de x seul; de même pour chacun des autres indices : elles seront donc de la forme

$$(1) \qquad | x, y, z \quad f(x), \quad f_1(y), \quad f_2(z) |.$$

17. Soit en particulier K_ρ l'un quelconque des groupes K_1, K_2,... ; ses substitutions seront de la forme (1), et *si elles ne laissent pas invariable l'indice x, par exemple, elles permuteront transitivement entre elles les diverses valeurs de cet indice.* Supposons, en effet, qu'il en fût autrement, et que chacune des substitutions de K_ρ fît succéder aux racines dont le premier indice est o d'autres racines dans lesquelles le premier indice ne prît que n valeurs distinctes, telles que o, 1,..., $\nu - 1$, ν étant $< \mu$. Il est clair que K_ρ permuterait exclusivement ensemble les racines dont le premier indice est inférieur à ν. Cela posé, en réunissant ensemble les racines que K_ρ permute entre elles, on aura un groupement en systèmes σ, σ'_1.... En le combinant avec le groupement S_{12}, S'_{12},... déjà trouvé, on obtiendra un nouveau groupement Σ, Σ',... dont un système sera évidemment formé de toutes les racines dont le premier indice est inférieur à ν. Mais, d'autre part, nous avons un groupement S_3, S'_3,... dont les divers systèmes sont respectivement formés de racines qui ne diffèrent que par le premier indice x. Les racines qui appartiennent à un même système dans chacun des deux groupements Σ, Σ',... et S_3, S'_3,..., jointes ensemble, donneraient un nouveau groupement dont les systèmes contiendraient un nombre ν de racines inférieur à μ, ce qui est supposé impossible.

18. Les raisonnements que nous venons de faire, en supposant le nombre des racines égal à μ^3, s'appliquent évidemment au cas plus

général où ce nombre serait égal à μ^m, sauf qu'on aura m indices x, y, z,... au lieu de trois.

L'un au moins de ces indices est altéré par les substitutions de plusieurs des groupes K_1, K_2,... Supposons, en effet, qu'il en fût autrement. Remplaçons ceux des indices que K_1 altère par un seul indice x_1, ceux que K_2 altère par un indice x_2, etc., et groupons dans un même système les racines pour lesquelles un de ces indices, tel que x_r, a la même valeur. Les substitutions de K_r permuteront les systèmes, en remplaçant les unes par les autres les racines dont tous les indices, à l'exception de x_r, ont les mêmes valeurs. D'autre part, les substitutions du groupe $H_r = (K_1, \ldots, K_{r-1}, K_{r+1}, \ldots)$ permuteront exclusivement ensemble les racines d'un même système; elles les permuteront d'ailleurs transitivement, sans quoi K ne serait pas transitif, comme il doit l'être. Cela posé, soit g une substitution quelconque de G; elle permute les uns dans les autres les groupes K_1, K_2,... Soit $K_{f(r)}$ celui de ces groupes qu'elle transforme en K_r; elle transforme évidemment $H_{f(r)}$ en H_r. Donc elle remplacera les racines correspondantes à une même valeur de l'indice $x_{f(r)}$, lesquelles sont permutées ensemble par les substitutions de $H_{f(r)}$, par des racines qui soient permutées ensemble par les substitutions de H_r, et dans lesquelles, par suite, l'indice x_r aura une même valeur, laquelle ne dépendra que de la valeur particulière assignée à $x_{f(r)}$. Donc la substitution g sera de la forme

$$| x_r \quad \varphi_r[x_{f(r)}] |,$$

et G sera décomposable, résultat contraire à l'hypothèse actuelle.

19. Admettons donc que l'indice x, par exemple, soit altéré par deux groupes au moins, K_r et K_s de la suite K_1, K_2,.... Soient

$$| x, y, \ldots \quad f(x), f_1(y), \ldots |, \ldots$$

les substitutions de K_r,

$$| x, y, \ldots \quad \varphi(x), \varphi_1(y), \ldots |, \ldots$$

celles de K_s, lesquelles seront échangeables aux précédentes; *a fortiori*, les substitutions $|x \quad \varphi(x)|, \ldots$ seront échangeables aux substitu-

tions $|x \quad f(x)|$,.... Les deux groupes M_r et M_s, formés par ces substitutions, sont d'ailleurs transitifs (**17**). Donc leur ordre est égal à leur degré μ, et ils sont conjoints.

L'ordre de K_r *se réduira lui-même à* μ. En effet, il est évidemment égal à l'ordre de M_r, multiplié par l'ordre du groupe N_r, formé par celles des substitutions de K_r qui n'altèrent pas l'indice x. Mais il est clair que N_r est permutable aux substitutions de K_r, et K_r est simple, par hypothèse; donc N_r se réduit à la seule substitution 1.

Les groupes K_1, K_2,..., transformés de K_r, auront aussi leur ordre égal à μ. Le nombre des racines que chacun d'eux permute entre elles est donc un diviseur de μ; mais, par hypothèse, il ne peut être moindre que μ; il lui est donc égal.

20. Cela posé, réunissons ensemble les racines que les substitutions de K_1 permutent entre elles; on aura ainsi un groupement en systèmes contenant chacun μ racines; et rien n'empêche d'admettre que ces systèmes sont précisément ceux que nous avons désignés par S_1, S'_1,.... Dans cette hypothèse, les groupements S_1, S'_1,...; S_2, S'_2,...; ..., qui se déduisent du premier groupement S_1, S'_1,... en y effectuant les substitutions g_1, g_2,... du groupe G (**15**), correspondront respectivement aux groupes transformés de K_1 par ces mêmes substitutions. En particulier, les m premiers groupements S_1, S'_1,...; ...; S_m, S'_m,..., étant essentiellement distincts, correspondront à m groupes distincts K_1,..., K_m.

Soient α, β,... des entiers quelconques différents et non supérieurs à m, le groupement $S_{\alpha\beta\ldots}$, $S'_{\alpha\beta\ldots}$, ... résultant de la combinaison des groupements S_α, S'_α,...; S_β, S'_β,...; ..., comme il est indiqué au n° **16**, correspondra au groupe $(K_\alpha, K_\beta, \ldots)$.

Nous continuerons de caractériser les racines par m indices x, y, z,... choisis de telle sorte que deux racines aient le même premier indice si elles appartiennent au même système dans le groupement $S_{12\ldots(m-1)}$, $S'_{12\ldots(m-1)}$,... [autrement dit, si elles sont permutées ensemble par les substitutions du groupe $(K_1, K_2, \ldots, K_{m-1})$ correspondant à ce groupement]; le même second indice, si elles sont permutées par les substitutions du groupe $(K_2, \ldots, K_m)$, etc. Cela posé, les substitutions de K_m, appartenant à chacun des groupes $(K_2, K_3, \ldots, K_m)$, (K_1, K_3, K_m),... laisseront invariable chacun des indices y, z,....

D'ailleurs, elles sont de la forme (1); donc, elles se réduiront à la forme

$$|x, y, z, \ldots \quad f(x), y, z, \ldots|.$$

De même, les substitutions de K_1 seront de la forme

$$|x, y, z, \ldots \quad x, f_1(y), z, \ldots|,$$

celles de K_2 de la forme

$$|x, y, z, \ldots \quad x, y, f_2(z), \ldots|,$$

etc,...

21. Cela posé, nous avons vu (**18**) que l'un au moins des indices x, y, z,..., par exemple x, est altéré par plusieurs groupes de la suite $K_1, \ldots, K_n$; or x est altéré par K_m et ne l'est pas par $K_1, \ldots, K_{m-1}$. Donc m sera $< n$, et x sera altéré par l'un au moins des groupes $K_{m+1}, \ldots, K_n$, tel que K_{m+1}. D'ailleurs, les substitutions de K_{m+1} sont de la forme (1).

Les substitutions de K_m et de K_{m+1} étant mutuellement échangeables, il en sera de même *a fortiori* des altérations

$$|x \quad f(x)|, \ldots \qquad \text{et} \qquad |x \quad \varphi(x)|, \ldots$$

que ces substitutions font subir à l'indice x. Or, soient respectivement H et I les deux groupes formés par ces altérations. Ils sont transitifs (**17**). Donc leur ordre q est égal à leur degré μ, et ce seront des groupes conjoints.

La suite $K_1, \ldots, K_n$ ne contient aucun autre groupe K_r dont les substitutions altèrent x. Car ces altérations formeraient un groupe J conjoint à I, et, par suite, identique à H; d'autre part, les substitutions de K_r étant échangeables à celles de K_1, celles de J le seraient *a fortiori* à celles de H; donc H, et par suite K_m, aurait toutes ses substitutions échangeables entre elles; son transformé K_1 jouirait de la même propriété, contrairement à l'hypothèse.

22. *La suite* $K_{m+1}, \ldots, K_n$ *se réduit à un seul groupe* K_{m+1}, *dont les substitutions altèrent tous les indices* x, y, z,.... Admettons, en effet, pour fixer les idées, qu'elle contînt deux groupes, dont le premier,

K_{m+1}, altérât les indices x, y seulement. Le groupe suivant, K_{m+2}, ne pourra altérer ces indices, comme on vient de le voir. Admettons qu'il altère les deux indices z, u. Les trois groupes K_1, K_m, K_{m+1} jouissent de la propriété de permuter chaque racine avec μ^2 racines, que deux quelconques de ces groupes suffiraient d'ailleurs pour permuter avec elle. Leurs transformés par une substitution quelconque de G, jouiront évidemment de la même propriété. Mais, d'autre part, il est clair que, parmi les systèmes de trois groupes à prendre dans la suite $K_1, \ldots, K_{m+2}$ les systèmes $C_1 = (K_1, K_m, K_{m+1})$ et $C_2 = (K_2, K_3, K_{m+2})$ sont les seuls qui jouissent de cette propriété. Or les substitutions de C_1 et de C_2 permutent exclusivement ensemble, et transitivement, les racines qui ne se distinguent que par les indices x, y, z, u. S'il existait d'autres indices $v, \ldots$, il faudrait, pour que les substitutions de G fussent permutables au groupe (C_1, C_2), qu'elles fissent succéder à $v, \ldots$ des fonctions de $v, \ldots$ seulement. Donc G ne serait pas primitif, résultat inadmissible.

Il n'y aura donc que quatre indices x, y, z, u. On pourra remplacer x et y par un seul indice x_1, z et u par un autre indice x_2. Les substitutions de C_1 n'altéreront que l'indice x_1, celles de C_2 que l'indice x_2. Les substitutions de G transformant exclusivement les uns dans les autres les groupes C_1 et C_2, on voit, comme au n° **18**, que l'une quelconque d'entre elles sera de la forme

$$| x_r \quad \varphi[x_{f(r)}] |;$$

G sera donc décomposable, résultat inadmissible.

Notre proposition est donc établie.

23. Les groupes $K_1, \ldots, K_m$, transformés de K_1 par des substitutions de G, sont isomorphes entre eux. Les altérations que leurs substitutions font respectivement subir aux indices x, y, z formeront des groupes isomorphes. Mais ils ont leur ordre égal à leur degré, et des groupes transitifs, jouissant de cette propriété, ne peuvent être isomorphes, à moins d'être identiques à la notation près (*Traité des substitutions*, **71-72**). On pourra donc, par un choix convenable dans la notation, faire en sorte que les substitutions de $K_1, \ldots, K_{m-1}$ altèrent respectivement $y, \ldots$ de la même manière que celles de K_m altèrent x.

24. Les substitutions de G permutant les uns dans les autres les groupes $K_1, \ldots, K_n$, ces groupes dépendront d'une équation de degré $n = m + 1$. Celle-ci résolue, le groupe de l'équation proposée se réduit à celles de ses substitutions qui sont permutables à chacun des groupes $K_1, \ldots, K_n$, lesquelles seront de la forme

$$| x, y, z, \ldots \quad \varphi(x), \varphi_1(y), \varphi_2(z), \ldots |.$$

Mais alors les μ^m racines de l'équation peuvent être groupées de m manières en systèmes, en réunissant ensemble celles qui ne diffèrent que par un seul indice. Dans chacun de ces groupements, les systèmes dépendront d'une équation du degré μ. La proposée se résoudra donc par une équation de degré $m + 1$ et m équations de degré μ.

25. Les principaux résultats des recherches précédentes peuvent être énoncés comme il suit :

THÉORÈME I. — *La recherche des groupes résolubles les plus généraux se ramène immédiatement à celle des groupes résolubles primitifs et indécomposables les plus généraux.*

THÉORÈME II. — *Ces derniers groupes ont pour degré μ^m, m étant entier, et μ un diviseur de l'un des facteurs de composition q de l'une des équations auxiliaires dont les conditions du problème font dépendre les équations cherchées.*

Si μ est un nombre premier, les groupes cherchés ont toutes leurs substitutions de la forme linéaire

$$\left| \begin{array}{ll} x_1 & a_1 x_1 + \ldots + a_m x_m + \alpha_1 \\ \ldots & \ldots\ldots\ldots\ldots\ldots\ldots \\ x_m & c_1 x_1 + \ldots + c_m x_m + \alpha_m \end{array} \right|$$

Si μ n'étant pas premier, m est > 1, on aura $\mu = q$, et les équations cherchées pourront se résoudre à l'aide d'une équation résoluble de degré $m + 1$, et de m équations résolubles de degré μ.