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

CAMILLE JORDAN

Mémoire sur la résolution algébrique des équations; extrait. Définitions et notions préliminaires

Journal de mathématiques pures et appliquées 2^e série, tome 12 (1867), p. 109-157.
<http://www.numdam.org/item?id=JMPA_1867_2_12__109_0>

MÉMOIRE

SUR LA

RÉSOLUTION ALGÉBRIQUE DES ÉQUATIONS;

PAR M. CAMILLE JORDAN,
Ingénieur des Mines.

EXTRAIT.

DÉFINITIONS ET NOTIONS PRÉLIMINAIRES.

On nomme *substitution* l'opération qui consiste à intervertir l'ordre d'un certain nombre de choses $a, b, c, \ldots$.

On désigne par AB la substitution qui produit le même effet que les deux substitutions A et B, exécutées successivement : par 1 la substitution qui laisse chaque chose à sa place.

La suite des substitutions 1, A, $A^2, \ldots$ a tous ses termes différents jusqu'à un terme A^μ qui se réduit à 1 et à partir duquel les autres se reproduisent périodiquement. Le nombre μ est dit l'*ordre* de la substitution A.

Un système de substitutions A, B, C,... forme un *groupe* si le produit AB de deux quelconques d'entre elles fait lui-même partie du système.

Tout groupe contient la substitution 1 : car s'il contient A, il contiendra par définition celle des puissances de A qui se réduit à l'unité. Tout groupe qui contient des substitutions autres que 1 en contient une d'ordre premier; car soit A une des substitutions du groupe, μ son ordre, p un diviseur premier de μ : $A^{\frac{\mu}{p}}$ sera évidemment d'ordre p et appartiendra au groupe.

L'*ordre* d'un groupe est le nombre de ses substitutions.

Soient A, B, C,... un certain nombre de substitutions; formons tous les produits possibles que l'on peut faire avec les facteurs A, B, C,. .,

pris chacun un nombre quelconque de fois et dans un ordre quelconque : le groupe ainsi obtenu sera dit le groupe *dérivé* de A, B, C,..., et nous le représenterons par la notation (A, B, C,...).

La substitution $M^{-1}AM$ est dite la *transformée de* A *par* M [*]. Si $M^{-1}AM = A$, d'où $AM = MA$, les substitutions A et M sont dites *échangeables* entre elles.

On a identiquement $M^{-1}AM.M^{-1}BM = M^{-1}ABM$.

Donc le produit de deux substitutions a pour transformée le produit de leurs transformées.

On en conclut aisément :

1° Que les transformées des substitutions d'un groupe (A, B, C,...) par M forment un groupe qu'on peut appeler le groupe *transformé* de (A, B, C,...) par M. Si ce groupe se confond avec le groupe (A, B, C,...), ce groupe et la substitution M sont dits réciproquement *permutables* [**].

2° Que si deux substitutions sont échangeables, leurs transformées par une substitution quelconque le seront.

3° Que si une substitution est permutable à un groupe, leurs transformés par une substitution quelconque seront permutables.

Un groupe est dit *transitif* si ses substitutions permettent d'amener une des lettres *a*, *b*,... à la place de chacune des autres.

Un groupe transitif est dit *primitif* ou non, suivant qu'il sera ou non impossible d'y répartir les lettres en systèmes tels que chacune des substitutions du groupe remplace les diverses lettres de chaque système par les lettres d'un même système.

Ces définitions posées, les deux théorèmes de Galois qui nous serviront de point de départ peuvent être énoncés ainsi qu'il suit :

---

[*] On vérifie aisément que si A remplace une lettre *a* par une autre lettre *b*, et si M remplace respectivement *a* et *b* par *a'* et *b'*, $M^{-1}AM$ remplace *a'* par *b'*. Nous aurons à faire un fréquent usage de cette remarque.

[**] Si M est permutable au groupe (A, B, C,...), toute substitution du groupe (A, B, C,..., M) peut être mise à volonté sous l'une des deux formes $M^{\alpha}N$ ou $N'M^{\alpha}$, N et N' étant des substitutions du groupe (A, B, C,...). Car la substitution M^2AM par exemple est identique à $M^3.M^{-1}AM = M^3.N$ en remarquant que $M^{-1}AM$ fait partie du groupe. De même $M^2AM = M^2AM^{-2}.M^3 = N'.M^3$.

THÉORÈME I. — *Soit* $F(x) = 0$ *une équation algébrique quelconque à coefficients rationnels : il existe un certain groupe de substitutions entre ses racines tel, que toute fonction rationnelle des racines, invariable par les substitutions de ce groupe, ait une valeur rationnelle, et réciproquement.*

THÉORÈME II. — *Pour qu'une équation* $F(x) = 0$ *à coefficients rationnels soit soluble par radicaux, il faut et il suffit que son groupe puisse s'obtenir en combinant ensemble une suite de substitutions* 1, A, B, C,... *telles, que chacune d'elles soit permutable au groupe dérivé des précédentes.*

Nous nommerons, pour abréger, groupes *résolubles* ceux qui caractérisent des équations solubles par radicaux.

CHAPITRE PREMIER.

THÉORÈMES GÉNÉRAUX.

1. Soit 1, A, B, C,... l'échelle des substitutions qui forment le groupe d'une équation résoluble, et dont chacune est permutable au groupe dérivé des précédentes. Si l'on forme les puissances successives d'une de ces substitutions, telle que C, on arrivera à en trouver une C^{μ} égale à l'unité, ou à quelque autre des substitutions du groupe (1, A, B) dérivé des précédentes.

On peut supposer μ *premier :* car si $\mu = d\delta$, on pourrait remplacer l'échelle 1, A, B, C,... par la suivante 1, A, B, C^{δ}, C,... qui contient un échelon de plus, et jouit évidemment encore de la propriété fondamentale que chaque substitution est permutable au groupe dérivé des précédentes.

2. THÉORÈME I. — *Soit* L *un groupe résoluble. Si* λ, λ'... *sont des substitutions qui puissent être liées idéalement avec celles de* L *par une corrélation telle :* 1° *qu'à chaque substitution de* L *corresponde une seule substitution* λ; 2° *que le produit* ll' *de deux substitutions quelconques de* L, l *et* l', *ait pour corrélative le produit* $\lambda\lambda'$ *des substitutions*

λ et λ' respectivement corrélatives de l et l', le groupe dérivé de λ, λ',... sera résoluble.

Formons en effet l'échelle $1, l, l', l'', \ldots$ génératrice du groupe L. Les conditions nécessaires et suffisantes pour que ces substitutions forment l'échelle d'un groupe résoluble sont les suivantes :

$$\begin{aligned}
&l'^{-1} l\, l' = \text{une puissance de } l, \text{ soit } l^{\alpha};\\
&l''^{-1} l\, l'' = \\
&l''^{-1} l' l'' = \end{aligned} \Bigg\} \text{des substitutions dérivées de } l \text{ et } l', \text{ telles que } \begin{cases} l^{\alpha_1} l'^{\beta_1};\\ l^{\alpha'_1} l'^{\beta'_1};\end{cases}$$

. . . . . .

Si l'on prend les substitutions corrélatives de celles qui entrent dans les deux membres de ces égalités, on aura les relations suivantes :

$$\begin{aligned}
&\lambda'^{-1}\lambda\,\lambda' = \lambda^{\alpha},\\
&\lambda''^{-1}\lambda\,\lambda'' = \lambda^{\alpha_1}\lambda'^{\beta_1},\\
&\lambda''^{-1}\lambda'\lambda'' = \lambda^{\alpha'_1}\lambda'^{\beta'_1},\\
&\ldots\ldots\ldots
\end{aligned}$$

qui montrent que $1, \lambda, \lambda', \lambda'', \ldots$ forment l'échelle d'un groupe résoluble.

3. Théorème II. — *Si $\mathfrak{F}$ est un faisceau (ou groupe partiel) de substitutions contenu dans le groupe résoluble* L *et permutable à toutes ses substitutions, on pourra toujours choisir l'échelle des substitutions* 1, A, B, C,... *dont l'adjonction successive reproduit le groupe* L *de telle sorte que les substitutions $\mathfrak{F}$ soient les premières introduites.*

Supposons en effet que le groupe dérivé de 1, A, B ne contienne aucune substitution du faisceau (sauf l'unité qu'il contient nécessairement), mais que l'adjonction d'une nouvelle substitution C en introduise une. C étant permutable au groupe (1, A, B), cette substitution pourra être ramenée à la forme $C^{\gamma}M$, M étant une substitution du groupe (1, A, B).

1° *Aucune des substitutions introduites avec* C, *à l'exception de* $C^{\gamma}M$ *et de ses puissances, ne fera partie du faisceau $\mathfrak{F}$.* En effet, considérons l'une d'elles : on peut la mettre sous la forme $C^{\delta}M_1$, où M_1 désigne une substitution du groupe (1, A, B).

Or on a généralement

$$C^{\delta}M_1(C^{\gamma}M)^{a} = C^{a\gamma+\delta}M_2,$$

M_2 étant encore une substitution du groupe (1, A, B). On sait d'ailleurs qu'il existe une puissance C^{μ} de C qui fait également partie de ce groupe, et que l'exposant μ est premier. On pourra donc déterminer le paramètre a de telle sorte que

$$a\gamma + \delta \equiv 0 \pmod{\mu};$$

et la substitution $C^{\delta}M_1.(C^{\gamma}M)^{a}$ fera elle-même partie du groupe (1, A, B). D'ailleurs elle fera partie du faisceau $\mathfrak{F}$, si $C^{\delta}M$ en fait partie ainsi que $C^{\gamma}M$; et comme par hypothèse ce faisceau n'a aucune substitution commune avec le groupe (1, A, B), sauf l'unité, on aura

$$C^{\delta}M_1(C^{\gamma}M)^{a} = 1, \quad \text{d'où} \quad C^{\delta}M_1 = (C^{\gamma}M)^{-a}.$$

2° *Toutes les substitutions* (1, A, B, C) *sont permutables au faisceau f dérivé de* $C^{\gamma}M$ *et de ses puissances.* En effet, le faisceau f', transformé de f par l'une quelconque de ces substitutions, doit faire partie à la fois du faisceau $\mathfrak{F}$ auquel cette substitution est permutable et du groupe (1, A, B, C); il se confond donc avec f.

3° Il résulte de là que *le groupe dérivé de l'échelle de substitutions suivante*

$$1, C^{\gamma}M, A, B$$

est résoluble. D'ailleurs ce groupe est identique à celui dérivé de 1, A, B, C. En effet, d'une part la substitution $C^{\gamma}M$ dérive de la combinaison des substitutions A, B, C; d'autre part, C dérive de la combinaison de $C^{\gamma}M$, A, B. En effet, soit

$$b\gamma \equiv 1 \pmod{\mu},$$

on aura

$$(C^{\gamma}M)^{b} = C^{b\gamma}M = CM',$$

M′ étant une substitution dérivée de 1, A, B, d'où

$$C = (C^{\gamma}M)^{b}M'^{-1}.$$

Chacun des deux groupes contient donc toutes les substitutions d'où l'autre est dérivé.

Adjoignons maintenant au groupe partiel $(1, C^{\gamma}M, A, B)$ une nouvelle substitution D. Supposons, pour fixer les idées, que cette adjonction introduise de nouvelles substitutions de la forme $\mathfrak{F}$. Soit $D^{\delta}N$ l'une d'elles, N étant une substitution dérivée de $C^{\gamma}M$, A, B.

On démontrera exactement comme tout à l'heure :

1° Qu'aucune des substitutions introduites avec D, à l'exception de celles qui dérivent de la combinaison de $C^{\gamma}M$ et de $D^{\gamma}N$, ne fera partie du faisceau $\mathfrak{F}$.

2° Que toutes les substitutions $(1, C^{\gamma}M, A, B, C)$ sont permutables au faisceau dérivé de $C^{\gamma}M$ et $D^{\delta}N$.

3° Que les substitutions $1, C^{\gamma}M, D^{\delta}N, A, B$ forment l'échelle d'un groupe résoluble identique au groupe (1, A, B, C, D).

Continuant ainsi, on voit qu'on pourra modifier l'échelle génératrice du groupe L de manière à faire passer en avant toutes les substitutions de $\mathfrak{F}$ à mesure qu'elles seront introduites. Le théorème est donc démontré.

4. Théorème III. — *Si* L *est un groupe résoluble*, $\mathfrak{L}$ *un groupe contenu dans* L *et permutable à toutes ses substitutions* (*ce peut être* L *lui-même*), $\mathfrak{F}$ *un faisceau contenu dans le groupe* $\mathfrak{L}$ *et ne renfermant qu'une partie de ses substitutions, et qui, de plus, soit permutable à toutes les substitutions* L, *on pourra déterminer un faisceau* $\mathfrak{G}$ *jouissant des propriétés suivantes :* 1° *il contiendra toutes les substitutions de* $\mathfrak{F}$, *jointes à d'autres substitutions;* 2° *il sera contenu dans* $\mathfrak{L}$; 3° *il sera permutable à toutes les substitutions* L; 4° *deux quelconques de ses substitutions g et g′ satisfont à une relation de la forme*

$$gg' = g'gf,$$

f désignant une substitution du faisceau $\mathfrak{F}$.

Nous exprimerons d'une manière abrégée cette dernière propriété, en disant que les substitutions g et g' sont *échangeables, aux substitutions $\mathfrak{F}$ près.*

Démonstration. — D'après le théorème précédent, nous pouvons former l'échelle

$$1, A, B, C, D, E, \ldots,$$

génératrice de L, de telle sorte que les premières substitutions introduites soient celles du groupe $\mathfrak{L}$, et, parmi ces dernières, celles du faisceau $\mathfrak{F}$. Supposons donc, pour fixer les idées, que le faisceau $\mathfrak{F}$ soit dérivé des trois premières substitutions de la série 1, A, B; le groupe $\mathfrak{L}$, contenant par hypothèse des substitutions qui ne font pas partie de $\mathfrak{F}$, la substitution suivante C fera partie de ce groupe.

Adjoignons maintenant à 1, A, B la suite des substitutions C, D, E,..., et formons la série des groupes partiels successifs

$$(1, A, B, C), \quad (1, A, B, C, D), \quad (1, A, B, C, D, E), \ldots.$$

Nous établirons d'abord la proposition suivante :

I. *Si dans l'un de ces groupes partiels,* (1, A, B, C, D) *par exemple, on peut déterminer un faisceau* Γ *jouissant des propriétés suivantes :* 1° *de contenir toutes les substitutions de* $\mathfrak{F}$*, jointes à d'autres substitutions;* 2° *d'être contenu dans* $\mathfrak{L}$*;* 3° *d'être permutable à toutes les substitutions du groupe partiel* (1, A, B, C, D); 4° *d'avoir toutes ses substitutions échangeables entre elles aux* $\mathfrak{F}$ *près, on pourra déterminer, dans le groupe partiel suivant* (1, A, B, C, D, E), *un faisceau* Γ_1 *jouissant, par rapport à ce nouveau groupe, des mêmes propriétés, et l'on pourra s'élever ainsi progressivement d'un groupe partiel à l'autre, jusqu'à ce qu'on ait reproduit le groupe* L *et le faisceau correspondant* $\mathfrak{G}$*, dont l'existence se trouvera ainsi démontrée.*

Si le faisceau Γ correspondant au groupe partiel (1, A, B, C, D) peut être choisi de diverses manières, tout en satisfaisant aux quatre conditions fondamentales, nous choisirons pour notre démonstration une des manières pour lesquelles le nombre de ses substitutions est *minimum.*

Adjoignons la substitution suivante E; supposons-la non permutable à Γ, car, si elle l'était, la proposition serait immédiatement démontrée pour le groupe (1, A, B, C, D, E). Soient $E^{-1}\Gamma E = \Gamma'$ le faisceau transformé de Γ par E; $E^{-2}\Gamma E^2 = \Gamma''$ le faisceau transformé de Γ′, etc. La série de ces faisceaux sera nécessairement limitée, car si E^{μ} est égale à l'une des substitutions (1, A, B, C, D), elle sera, par hypothèse, permutable à Γ. Donc $\Gamma^{\mu} = \Gamma$.

Cela posé : 1° le faisceau dérivé de l'ensemble des substitutions $\Gamma, \Gamma' \ldots \Gamma^{\mu-1}$ contient toutes les substitutions $\mathcal{S}$, jointes à d'autres substitutions : cela est évident, puisqu'il contient toutes les substitutions de Γ.

2° Il est contenu dans le groupe $\mathcal{L}$, car les substitutions Γ sont comprises dans ce groupe, et leurs transformées Γ′, Γ″ par les substitutions E, $E^2 \ldots$, permutables à $\mathcal{L}$, y seront également comprises.

3° Il est permutable aux substitutions (1, A, B, C, D, E). En effet, Γ est permutable aux substitutions (1, A, B, C, D); Γ′, transformé de Γ par E, le sera à celles du groupe transformé de (1, A, B, C, D) par E : mais ce groupe transformé est identique au groupe (1, A, B, C, D) : donc Γ′ et de même Γ″... seront permutables aux substitutions (1, A, B, C, D). D'ailleurs E transforme Γ en Γ′, Γ′ en Γ″, ... Le faisceau résultant (Γ, Γ′, Γ″) est donc permutable à toutes les substitutions (1, A, B, C, D, E).

4° Enfin toutes ces substitutions sont échangeables entre elles aux $\mathcal{S}$ près.

En effet, soient, en premier lieu, deux substitutions γ', δ^{ν}, appartenant à un même faisceau partiel, Γ′ par exemple. Posons

$$\gamma'\delta^{\nu} = \delta^{\nu}\gamma'\varphi,$$

φ étant une substitution inconnue à déterminer : cette équation, transformée par $E^{\mu-1}$, donnera

$$(E^{\mu-1})^{-1}\gamma' E^{\mu-1}(E^{\mu-1})^{-1}\delta^{\nu}E^{\mu-1}$$
$$= (E^{\mu-1})^{-1}\delta^{\nu}E^{\mu-1}(E^{\mu-1})^{-1}\gamma' E^{\mu-1}(E^{\mu-1})^{-1}\varphi E^{\mu-1}.$$

Les deux substitutions $(E^{\mu-1})^{-1}\gamma' E^{\mu-1}$, $(E^{\mu-1})^{-1}\delta^{\nu}E^{\mu-1}$ font partie

du faisceau Γ : elles sont donc échangeables entre elles aux $\mathcal{F}$ près. $(E^{\mu-1})^{-1}\varphi E^{\mu-1}$ fera donc partie du faisceau $\mathcal{F}$. Sa transformée φ par $(E^{\mu-1})^{-1}$, qui est permutable à $\mathcal{F}$, fera également partie de ce faisceau.

Soient maintenant deux substitutions γ, γ' appartenant à des faisceaux partiels différents Γ et Γ'. La substitution γ' faisant partie du groupe (1, A, B, C, D) sera permutable au faisceau Γ. On a donc

$$\gamma'^{-1}\gamma\gamma' = \delta,$$

δ étant une substitution du faisceau Γ.

On déduit de là

$$\gamma'\delta\gamma'^{-1} = \gamma\gamma'\gamma'^{-1} = (\gamma^{-1})^{-1}\gamma'\gamma^{-1}.$$

Or la substitution γ^{-1} fait partie du groupe (1, A, B, C, D), dont les substitutions sont permutables au faisceau Γ'. La transformée de γ' par γ^{-1}, $\gamma'\delta\gamma^{-1}$ fera donc partie de ce faisceau, et, comme γ' en fait partie de son côté, $\delta\gamma^{-1}$ en fera partie également. D'ailleurs δ et γ font partie du faisceau Γ. La substitution $\delta\gamma^{-1}$ sera donc commune aux deux faisceaux Γ et Γ'.

Mais les substitutions communes à ces deux faisceaux ne sont autres que les $\mathcal{F}$. En effet, d'une part les substitutions $\mathcal{F}$ faisant partie de Γ et la substitution E les transformant les unes dans les autres, elles feront toutes partie de Γ'. D'autre part, Γ et Γ' n'ont aucune autre substitution commune; car ces substitutions communes, faisant partie de Γ, seraient évidemment échangeables entre elles aux $\mathcal{F}$ près, et seraient toutes contenues dans $\mathfrak{L}$: elles formeraient un faisceau Γ_1 contenant toutes les substitutions $\mathcal{F}$, jointes à d'autres substitutions; enfin Γ_1 serait permutable à toutes les substitutions (1, A, B, C, D), car chacune de ces dernières substitutions étant permutable à la fois à Γ et à Γ', transformerait les substitutions de Γ_1 communes à ces deux groupes en substitutions également communes à ces deux groupes, et qui, par suite, reproduiraient à l'ordre près celles de Γ_1. Le faisceau Γ_1, qui contient moins de substitutions que Γ, jouirait donc des mêmes propriétés fondamentales, ce qui est contraire à notre point de départ.

On aura donc

$$\delta\gamma^{-1} = f \quad \text{ou} \quad \delta = f\gamma, \quad \text{d'où} \quad \gamma\gamma' = \gamma' f \gamma = \gamma'\gamma f_1,$$

f, f_1 désignant des substitutions convenablement choisies dans le faisceau $\mathfrak{F}$.

II. Mais le premier groupe partiel (1, A, B, C) contient toutes les substitutions de $\mathfrak{F}$ jointes à C : il est contenu dans $\mathfrak{L}$; il est permutable à ses propres substitutions; enfin celles-ci sont échangeables entre elles aux $\mathfrak{F}$ près. Car ces substitutions sont toutes de la forme $C^{\lambda} f$, où f désigne une des substitutions de $\mathfrak{F}$, et C étant permutable aux $\mathfrak{F}$, si l'on pose en général

$$C^{\lambda} f . C^{\lambda'} f' = C^{\lambda'} f' . C^{\lambda} f . \varphi,$$

la substitution

$$\varphi = (C^{\lambda'} f' . C^{\lambda} f)^{-1} . C^{\lambda} f . C^{\lambda'} f' = C^{-\lambda-\lambda'+\lambda+\lambda'} f_1 = f_1$$

se réduit à une substitution de $\mathfrak{F}$.

Le faisceau Γ correspondant à ce groupe partiel sera donc ce groupe lui-même : en s'élevant ensuite de proche en proche par la méthode que nous venons d'exposer, on démontrera le théorème.

5. Théorème IV. — *Tout groupe résoluble* L *peut être considéré comme le dernier terme d'une série de groupes partiels* 1, F, G, H, ... *jouissant des propriétés suivantes :* 1° *chacun de ces groupes est contenu dans le suivant;* 2° *il est permutable à toutes les substitutions* L; 3° *deux quelconques de ses substitutions sont échangeables entre elles, aux substitutions près du groupe précédent.*

Ce théorème capital résulte immédiatement de l'application réitérée du précédent.

Posons, en effet, dans le théorème précédent, $\mathfrak{L} = L$ et prenons, pour le faisceau $\mathfrak{F}$, la substitution unique 1. Nous en conclurons l'existence d'un faisceau plus général F, également permutable aux substitutions L.

Prenant ensuite $\mathfrak{F} = F$, nous en conclurons l'existence du faisceau G, etc.

Le nombre des substitutions des groupes partiels F, G, H,... croissant à chaque opération, on finira par arriver au groupe total L, qui clora la série.

6. Théorème V. — *Réciproquement, tout groupe jouissant de la propriété ci-dessus énoncée est résoluble.*

En effet, on pourra former une échelle de substitutions satisfaisant aux conditions exigées par le théorème de Galois en prenant d'abord les substitutions de F dans un ordre quelconque, puisqu'elles sont échangeables entre elles : en leur adjoignant ensuite les autres substitutions de G, également dans un ordre quelconque, puisqu'elles sont permutables à F et échangeables entre elles aux substitutions F près, qui ont déjà été introduites : en leur adjoignant ensuite les autres substitutions de H, etc.

7. Théorème VI. — *Si* L *est un groupe résoluble, tout groupe* Λ *contenu dans* L *le sera également.*

Formons en effet la série des groupes partiels 1, F, G, H,..., L, dont le dernier terme est L. Désignons le système des substitutions communes à Λ et à chacun de ces divers groupes pris successivement par $1, \mathcal{F}, \mathcal{G}, \mathcal{H}, \ldots, \Lambda$.

1° Chacun des groupes de cette nouvelle série, $\mathcal{G}$ par exemple, sera permutable aux substitutions Λ. Car les substitutions Λ faisant partie du groupe des substitutions L permutables à G transformeront les $\mathcal{G}$, qui font partie de G, en substitutions faisant également partie de G; d'autre part, ces transformées appartiennent au groupe Λ. Ce sont donc, à l'ordre près, les substitutions $\mathcal{G}$ elles-mêmes.

2° Les substitutions de chacun des groupes $1, \mathcal{F}, \mathcal{G}, \mathcal{H}, \ldots, \Lambda$ sont échangeables entre elles aux substitutions près du groupe précédent. Car soient g et g' deux substitutions de $\mathcal{G}$: étant comprises dans le groupe G, elles devront satisfaire à une relation de la forme $gg' = g'g\varphi$, φ étant l'une des substitutions de F. On en déduit $\varphi = g^{-1}g'^{-1}gg'$. Les substitutions g et g' faisant partie du groupe Λ, φ en fera partie également. Ce sera donc une des substitutions $\mathcal{F}$.

Le groupe Λ sera donc résoluble (théorème V).

8. Théorème VII. — *Toute équation irréductible a son groupe transitif et réciproquement.*

Car si le groupe G d'une équation $f(x) = 0$ n'est pas transitif, soient x_1 une des racines de l'équation, x_2, x_3,... celles des racines de $f(x) = 0$, auxquelles les substitutions G font succéder x_1 : ces substitutions permuteront exclusivement entre elles les racines x_1, x_2, x_3,...; car si l'une d'elles, A, fait succéder x_2 à une autre racine x_μ, cette substitution, combinée à la substitution B du groupe G qui fait succéder x_1 à x_2, donnera une substitution AB qui fera également partie de G et qui fera succéder x_1 à x_μ. Donc x_μ fera partie de la suite x_1, x_2, x_3,....

Cela posé, le polynôme $(x - x_1)(x - x_2)(x - x_3)\ldots$ étant symétrique en x_1, x_2, x_3,... et ne contenant pas les autres racines, sera invariable par les substitutions G, et par suite rationnel : donc $f(x)$ aura un diviseur rationnel et $f(x) = 0$ ne sera pas irréductible.

Réciproquement, si $f(x)$ a un diviseur rationnel

$$(x - x_1)(x - x_2)(x - x_3)\ldots,$$

ce facteur devra rester inaltéré par toutes les substitutions de G : donc ces substitutions permuteront exclusivement entre elles les racines x_1, x_2, x_3,...; car s'il en était autrement, elles altéreraient évidemment la valeur de l'expression $(x - x_1)$, $(x - x_2)$,..., tant que x restera indéterminé.

9. Supposons que nous ayons formé le tableau de tous les groupes résolubles et transitifs pour un degré donné; si nous effaçons tous ceux de ces groupes qui sont contenus dans quelque autre, il en restera quelques-uns, en nombre relativement restreint, auxquels nous donnerons le nom de groupes résolubles *généraux*. D'après ce qui précède, la condition nécessaire et suffisante pour qu'un groupe soit résoluble est qu'il soit contenu dans quelqu'un de ces groupes généraux L, L', L'',....

Ces derniers sont les seuls dont la détermination présente de l'intérêt. Chacun d'eux caractérise un type spécial d'équations irréductibles et résolubles par radicaux, et ils donnent à eux seuls les conditions nécessaires et suffisantes de résolubilité.

Considérons en effet une équation dont le groupe A soit contenu dans L. Toute fonction des racines invariable par les substitutions A

sera exprimable rationnellement. A plus forte raison une fonction des racines, invariable par toutes les substitutions L, sera exprimable rationnellement. L'équation proposée satisfera donc à toutes les conditions qui caractérisent les équations dont le groupe est L. Pour que son groupe se réduise à A, elle devra satisfaire en outre à d'autres conditions accessoires et étrangères à la question de résolubilité.

Nous bornerons donc notre recherche à celle des groupes résolubles, transitifs et généraux.

Notre méthode consistera à nous élever progressivement à la connaissance des groupes que nous cherchons, par la détermination successive des divers groupes partiels F, G, H,..., etc. Cette marche présente les avantages suivants : d'une part, les propriétés particulières à chacun de ces groupes facilitent sa construction; d'autre part, les substitutions de L étant assujetties à la condition d'être permutables à chacun de ces groupes, le champ des recherches se limitera progressivement, à mesure que l'on aura déterminé un plus grand nombre de ces groupes partiels successifs. Cette simplification n'aurait pas lieu, si l'on voulait prendre pour point de départ le théorème de Galois dans sa forme primitive, et former directement l'échelle des substitutions 1, A, B, C,..., assujetties à la seule condition que chacune d'elles soit permutable au groupe dérivé des précédentes.

CHAPITRE II.

RÉDUCTION DU PROBLÈME DANS LE CAS DES GROUPES PRIMITIFS.

1. Soit L un groupe résoluble et primitif. Nous avons vu qu'on peut toujours déterminer un groupe partiel F permutable aux substitutions L et tel que ses substitutions soient échangeables entre elles (chap. I[er], théorème IV). Si cette détermination peut se faire de plusieurs manières, nous serons toujours maîtres de choisir parmi ces diverses manières l'une de celles pour lesquelles le nombre des substitutions de F est *minimum*.

Soit f une substitution d'ordre premier p, choisie parmi celles du

faisceau F. Soient $f, f', f'', \ldots$ les transformées de f par les diverses substitutions du groupe L.

1° Le faisceau dérivé de $f, f', f'', \ldots$ a toutes ses substitutions échangeables entre elles, puisque toutes sont comprises dans le faisceau F : il est évidemment permutable à toutes les substitutions L. *Il contient donc toutes les substitutions de* F, puisque par hypothèse on ne peut déterminer aucun faisceau moindre que F et jouissant des deux propriétés fondamentales ci-dessus.

2° *Ce faisceau est transitif.* Supposons en effet qu'il ne le soit pas. Soient a une lettre donnée, $a, a', a'', \ldots$ les diverses lettres que les substitutions F permettent de lui faire succéder; toutes ces substitutions les permuteront exclusivement entre elles. En effet, si l'une de ces substitutions f' fait succéder à a' une lettre telle que α, on pourra faire succéder α à a en combinant cette substitution f' avec la substitution f'' qui fait succéder a' à a. La lettre α fera donc partie de la série $a, a', a'', \ldots$.

Soit b une autre lettre quelconque. Il existe dans le groupe L, supposé primitif et par suite transitif, une substitution au moins, A, qui la fera succéder à a. Soient $b', b'', \ldots$ les lettres que A fait succéder à $a', a'', \ldots$. Les lettres $b, b', b'', \ldots$ jouiront de la propriété d'être permutées exclusivement entre elles, et transitivement dans le faisceau transformé de F par A, lequel est identique à F. D'ailleurs, les deux systèmes $a, a', a'', \ldots$ et $b, b', b'', \ldots$ ne peuvent avoir aucune lettre commune : en effet, si l'on avait, par exemple $a'' = b'$, on pourrait, contre l'hypothèse, faire succéder b à a en combinant deux des substitutions F, la première remplaçant a par a'', la seconde remplaçant $a'' = b'$ par b.

Si c est une lettre qui ne fasse partie d'aucune des deux séries $a, a', a'', \ldots, b, b', b'', \ldots$, il existera dans L une substitution au moins qui la fera succéder à a; si $c, c', c'', \ldots$ sont les lettres que cette substitution fait succéder respectivement à $a, a', a'', \ldots$, elles jouissent de la propriété d'être permutées exclusivement entre elles et transitivement dans le faisceau F. D'ailleurs, les lettres du système $c, c', c'', \ldots$ sont essentiellement distinctes de celles des deux premiers systèmes $a, a', a'', \ldots$ et $b, b', b'', \ldots$.

Continuant ainsi, on voit que les lettres se partageront en systèmes

également nombreux, a, a', a'',..., b, b', b'',..., c, c', c'',..., les lettres de chaque système jouissant de la propriété d'être permutées exclusivement entre elles, et transitivement, dans les substitutions du faisceau F.

Considérons maintenant une substitution quelconque du groupe L. Les lettres qu'elle fait succéder à a, a', a'',... jouissent de la propriété d'être permutées exclusivement entre elles, et transitivement dans le faisceau transformé de F par la substitution considérée, lequel faisceau est identique à F. Si donc b', par exemple, est l'une de ces lettres, les autres sont celles que les F permutent avec b', à savoir celles du système b, b', b'',....

Ainsi, toutes les substitutions L feraient succéder à l'ensemble des lettres de chaque système, tel que a, a', a'',... l'ensemble des lettres d'un même système. Le groupe ne serait donc pas primitif, comme nous le supposons.

Il n'est donc pas permis d'admettre que le faisceau F ne soit pas transitif.

3° *Chacune des substitutions* F (*à l'exception de la substitution* 1) *déplace toutes les lettres*. Supposons en effet que l'une d'elles, A, laisse la lettre a immobile. Soit a' une autre lettre quelconque. Le faisceau F étant transitif, contiendra une substitution B qui remplace a par a'. La substitution $B^{-1}AB$ laissera a' immobile (p. 6, note). Mais A et B étant échangeables, $B^{-1}AB = A$. La substitution A ne déplacerait donc aucune lettre, et se réduirait à l'unité.

4° *Toutes les substitutions* F *sont d'ordre* p. Car elles dérivent toutes de la combinaison de f, f', f'',..., substitutions échangeables entre elles et d'ordre p. Soit $f^{\alpha}f'^{\beta}f''^{\gamma}\ldots$ l'une d'elles : on aura

$$(f^{\alpha}f'^{\beta}f''^{\gamma}\ldots)^p = f^{\alpha p}f'^{\beta p}f''^{\gamma p}\ldots = 1.$$

5° *L'ordre de* F *est une puissance exacte de* p, *telle que* p^n. En effet, la substitution f est d'ordre p. Si F renferme des substitutions différentes de f et de ses puissances, soit f_1 l'une d'elles; les substitutions f et f_1 étant échangeables entre elles et d'ordre p, celles qui dérivent de leur combinaison seront toutes de la forme $f^{\alpha}f_1^{\beta}$, α et β étant des entiers variables de 0 à $p-1$. D'ailleurs, les substitutions de cette

forme relatives aux p^2 systèmes de valeurs de α et de β sont toutes distinctes.

Supposons en effet

$$f^{\alpha} f_1^{\beta} = f^{\alpha'} f_1^{\beta'},$$

d'où

$$f_1^{\beta-\beta'} = f^{\alpha'-\alpha}.$$

Si $\beta = \beta'$, on devra avoir

$$\alpha = \alpha'.$$

Si $\beta - \beta' \gtrless 0$, en élevant l'égalité ci-dessus à la puissance x, on aura

$$f_1^{(\beta-\beta')x} = f^{(\alpha'-\alpha)x}.$$

L'entier arbitraire x peut être choisi de telle sorte que

$$(\beta - \beta')x \equiv 1 \pmod{p};$$

on aura alors

$$f_1 = f_1^{(\beta-\beta')x} = f^{(\alpha'-\alpha)x},$$

et f_1 serait, contrairement à l'hypothèse, une puissance de f.

Le nombre des substitutions distinctes dérivées de f et f_1 sera donc p^2.

Si F contient une substitution f_2 différente de celles-là, les substitutions dérivées de f, f_1, f_2 seront de la forme $f^{\alpha} f_1^{\beta} f_2^{\gamma}$, où α, β, γ sont des entiers variables de 0 à $p-1$.

Les substitutions de cette forme relatives aux p^3 systèmes de valeurs de α, β, γ sont toutes distinctes. En effet, de l'égalité

$$f^{\alpha} f_1^{\beta} f_2^{\gamma} = f^{\alpha'} f_1^{\beta'} f_2^{\gamma'},$$

on déduit, si $\gamma = \gamma'$,

$$f^{\alpha} f_1^{\beta} = f^{\alpha} f_1^{\beta'},$$

d'où

$$\alpha = \alpha', \quad \beta = \beta',$$

et si $\gamma \lessgtr \gamma'$, on en déduirait

$$f_2^{\gamma-\gamma'} = f^{\alpha'-\alpha} f_1^{\beta'-\beta},$$

ou, en posant $(\gamma - \gamma')\,x \equiv 1 \pmod{p}$,

$$f_2 = f_2^{(\gamma-\gamma')x} = f^{(\alpha'-\alpha)x}\, f_1^{(\beta'-\beta)x}.$$

La substitution f_2 serait donc dérivée des précédentes, contre l'hypothèse.

Le nombre des substitutions distinctes dérivées de f, f_1, f_2 sera donc p^3.

On continuera ainsi jusqu'à ce qu'on ait épuisé le faisceau F.

6° *Le nombre des lettres sera* p^n : en effet, le faisceau F étant transitif contiendra au moins une substitution qui permette de remplacer une lettre a par une autre lettre quelconque a'. D'ailleurs il n'en contiendra qu'une : car s'il y en avait deux différentes f et f', la substitution $f^{-1}f'$, différente de l'unité, laisserait a immobile, ce qui ne peut être (3°). Le nombre des lettres est donc précisément égal au nombre p^n des substitutions F.

On peut donc énoncer ce premier théorème :

THÉORÈME I. — *Dans tout groupe résoluble primitif, le nombre des lettres est une puissance, telle que* p^n, *d'un nombre premier* p.

2. Désignons les diverses lettres par le symbole général $a_{x,Y}$, les indices x et Y variant le premier de 0 à $p-1$, le second de 0 à $p^{n-1}-1$; on peut choisir arbitrairement parmi les systèmes de valeurs de ces deux indices, celui qu'on voudra faire correspondre à chaque lettre donnée; nous le ferons ainsi qu'il suit :

Soient $f, f_1, \ldots, f_{n-1}$, n substitutions dont aucune ne soit dérivée des précédentes, et qui reproduisent par leurs combinaisons toutes les substitutions de F (page 123, 5°). Choisissons à volonté celle des lettres que nous désignerons par $a_{0,0}$; les substitutions $f, f_1, \ldots, f_{n-2}$ et leurs dérivées sont en nombre p^{n-1}, et deux d'entre elles ne peuvent remplacer $a_{0,0}$ par une même lettre : elles permuteront donc $a_{0,0}$ avec p^{n-1} autres lettres, que nous désignerons respectivement par $a_{0,0}$, $a_{0,1}, \ldots$, $a_{0,Y}, \ldots$, les diverses valeurs de l'indice Y étant assignées à ces diverses lettres d'une manière arbitraire.

La substitution f_{n-1} remplacera $a_{0,0}, \ldots, a_{0,Y}, \ldots$ par une série d'autres

lettres, que nous représenterons respectivement par $a_{1,0},\ldots,\ a_{1,Y},\ldots$: à celles-ci elle fera succéder d'autres lettres $a_{2,0},\ldots,\ a_{2,Y},\ldots$. La substitution $(f_{n-1})^{\alpha}$ fera ainsi succéder en général aux lettres $a_{0,0},\ldots,\ a_{0,Y}$ les lettres correspondantes de la série $a_{\alpha,0},\ldots,\ a_{\alpha,Y}$. $(f_{n-1})^{p}$ étant égale à l'unité, la série $a_{p,0},\ldots,\ a_{p,Y}$ se réduira identiquement à $a_{0,0},\ldots,\ a_{0,Y}$ et les séries se reproduiront périodiquement à partir de celle-là. On n'aura donc en tout que p séries distinctes

$$\begin{array}{l} a_{0,0},\ldots,\quad a_{0,Y},\ldots, \\ \ldots\ldots\ldots \\ a_{x,0},\ldots,\quad a_{x,Y},\ldots, \\ \ldots\ldots\ldots \\ a_{p-1,0},\ldots,\quad a_{p-1,Y}\cdot\ldots \end{array}$$

D'ailleurs, tous les termes de ces séries représenteront des lettres essentiellement différentes.

En effet, les substitutions du faisceau partiel $(1, f, \ldots, f_{n-2})$ permutent exclusivement entre elles les lettres $a_{0,0},\ldots,\ a_{0,Y}$. Les lettres $a_{x,0},\ldots,$ $a_{x,Y}$ qui remplacent celles-ci par l'effet de la substitution $(f_{n-1})^{x}$ seront donc permutées exclusivement entre elles dans le faisceau transformé de $(1, f, f_1,\ldots, f_{n-2})$ par $(f_{n-1})^{x}$: mais les substitutions $1, f, f_1,\ldots,$ f_{n-1} étant toutes échangeables, ce faisceau transformé est identique à $(1, f, f_1,\ldots, f_{n-2})$.

Ainsi les substitutions $(1, f, f_1,\ldots, f_{n-2})$ permutent exclusivement entre elles les lettres de chacune des séries : f_{n-1} permute les séries entre elles; toutes les substitutions F permuteront donc exclusivement entre elles les lettres comprises dans ces séries. Mais le nombre total des termes de ces séries est égal à p^n, nombre des lettres. Si donc plusieurs de ces termes représentaient la même lettre, on aurait un système de moins de p^n lettres se permutant exclusivement entre elles par les substitutions F. Le faisceau F ne serait donc pas transitif, ce que nous avons démontré impossible.

Ainsi, toutes les lettres représentées en général par le symbole $a_{x,Y}$ seront distinctes, et la substitution f_{n-1} remplacera en général la

lettre $a_{x,Y}$ par la lettre $a_{x+1 \,(\mathrm{mod.}\, p),\, Y}$, ce que nous pourrons exprimer par la notation suivante :

$$f_{n-1} = \begin{vmatrix} x & x+1 \,(\mathrm{mod.}\, p) \\ Y & Y \end{vmatrix}.$$

Chacune des substitutions $(1, f, \ldots, f_{n-2})$ remplace en général chaque lettre $a_{x,Y}$ par une lettre $a_{x,Y'}$ de la même série; l'indice Y′ peut dépendre de x et de Y; si l'on pose $Y' = \psi(x, Y)$, on pourra représenter la substitution considérée f' par la notation

$$f' = \begin{vmatrix} x & x \\ Y & \psi(x, Y) \end{vmatrix}.$$

Mais on doit avoir

$$f' f_{n-1} = f_{n-1} f'.$$

Or $f' f_{n-1}$ remplace la lettre $a_{x,Y}$ par celle-ci $a_{x+1 \,(\mathrm{mod.}\, p),\, \psi(x, Y)}$; $f_{n-1} f'$ la remplace par celle-ci $a_{x+1 \,(\mathrm{mod.}\, p),\, \psi[x+1 \,(\mathrm{mod.}\, p),\, Y]}$. Ces deux lettres devant être identiques, on aura

$$\psi(x, Y) = \psi[x + 1 \,(\mathrm{mod.}\, p), Y].$$

La fonction ψ est donc indépendante de x, et se réduit à $\psi(Y)$.

Considérons maintenant en particulier les lettres $a_{0,0}, \ldots, a_{0,Y}$ de la première série. Au lieu de les distinguer les unes des autres par l'indice unique Y, on pourra le faire à l'aide de deux indices y et Z, variant l'un de 0 à $p - 1$, l'autre de 0 à $p^{n-2} - 1$; et l'on verra, exactement comme tout à l'heure, que les valeurs de ces indices pour chacune des lettres que l'on considère peuvent être choisies de telle sorte, 1° que la substitution f_{n-2} remplace en général la lettre $a_{0,y,Z}$ par la lettre $a_{0,y+1 \,(\mathrm{mod.}\, p),\, Z}$; 2° que toute substitution f' du faisceau partiel $(1, f, \ldots, f_{n-3})$ la remplace par une lettre $a_{0,y,Z'}$, l'indice Z′ étant indépendant de y. Désignons en général par $a_{x,y,Z}$ la lettre que la substitution $(f_{n-1})^x$ fait succéder à $a_{0,y,Z}$. La substitution f_{n-2} remplacera

la lettre générale $a_{x,y,\mathrm{Z}}$ par $a_{x,y+1\,(\mathrm{mod.}\,p),\mathrm{Z}}$, et la substitution f' la remplacera par $a_{x,y,\mathrm{Z}'}$. En effet, toutes ces substitutions étant échangeables entre elles, on aura

$$(f_{n-1})^{-x} f_{n-2} (f_{n-1})^{x} = f_{n-2},$$

et comme $(f_{n-1})^{-x}$ remplace $a_{x,y,\mathrm{Z}}$ par $a_{0,y,\mathrm{Z}}$, que f_{n-2} remplace par $a_{0,y+1\,(\mathrm{mod.}\,p),\mathrm{Z}}$, que $(f_{n-1})^{x}$ remplace enfin par $a_{x,y+1\,(\mathrm{mod.}\,p),\mathrm{Z}}$, on voit que f_{n-2} remplacera $a_{x,y,\mathrm{Z}}$ par $a_{x,y+1\,(\mathrm{mod.}\,p),\mathrm{Z}}$. On aura de même

$$(f_{n-1})^{-x} f' (f_{n-1})^{x} = f';$$

et f' remplaçant $a_{0,y,\mathrm{Z}}$ par $a_{0,y,\mathrm{Z}'}$, $(f_{n-1})^{-x} f' (f_{n-1})^{x} = f'$ remplacera $a_{x,y,\mathrm{Z}}$ par $a_{x,y,\mathrm{Z}'}$.

On aura ainsi

$$f_{n-1} = \begin{vmatrix} x & x+1\,(\mathrm{mod.}\,p) \\ y & y \\ \mathrm{Z} & \mathrm{Z} \end{vmatrix}, \quad f_{n-2} = \begin{vmatrix} x & x \\ y & y+1\,(\mathrm{mod.}\,p) \\ \mathrm{Z} & \mathrm{Z} \end{vmatrix},$$

les substitutions $(1, f, \ldots, f_{n-3})$ étant toutes de la forme

$$\begin{vmatrix} x & x \\ y & y \\ \mathrm{Z} & \psi_1(\mathrm{Z}) \end{vmatrix}.$$

On pourra de même remplacer l'indice Z par deux autres, z et U,...; en continuant ces opérations on arrivera en dernière analyse au théorème suivant.

THÉORÈME II. — *Soit* L *un groupe résoluble primitif entre* p^n *lettres,* p *étant premier. Si l'on désigne les lettres par le symbole général* $a_{x,y,z,\ldots}$, *où* x, y, z *sont des indices en nombre* n, *variables chacun de* 0 *à* $p-1$, *on pourra choisir les valeurs de* x, y, z,... *qui correspondent à chaque lettre, de telle sorte que les substitutions du premier groupe partiel* F *dérivent des suivantes :*

$$f_{n-1} = \begin{vmatrix} x & x+1\,(\mathrm{mod.}\,p) \\ y & y \\ z & z \\ \cdots & \cdots \end{vmatrix}, \quad f_{n-2} = \begin{vmatrix} x & x \\ y & y+1\,(\mathrm{mod.}\,p) \\ z & z \\ \cdots & \cdots \end{vmatrix}, \ldots.$$

Les substitutions de F *seront donc toutes de la forme*

$$f^{\alpha}_{n-1} f^{\alpha'}_{n-2} f^{\alpha''}_{n-3} \cdots = \begin{vmatrix} x & x+\alpha \pmod p \\ y & y+\alpha' \pmod p \\ z & z+\alpha'' \pmod p \\ \cdots & \cdots \end{vmatrix},$$

ou plus simplement

$$f^{\alpha}_{n-1} f^{\alpha'}_{n-2} f^{\alpha''}_{n-3} \cdots = \begin{vmatrix} x & x+\alpha \\ y & y+\alpha' \\ z & z+\alpha'' \\ \cdots & \cdots \end{vmatrix},$$

en sous-entendant la condition de prendre à la place des indices $x+\alpha$, $y+\alpha'$, $z+\alpha''$,..., lorsqu'ils dépassent p, le reste qu'ils donnent étant divisés par ce nombre.

3. Le groupe partiel F est ainsi déterminé : les substitutions L lui sont toutes permutables, ce qui jette déjà un grand jour sur la nature de ces substitutions.

Soit en effet

$$\Lambda = \begin{vmatrix} x & \varphi(x,y,z\ldots) \\ y & \varphi'(x,y,z\ldots) \\ z & \varphi''(x,y,z\ldots) \\ \cdots & \cdots \end{vmatrix}$$

l'une d'elles; la transformée de $\begin{vmatrix} x & x+1 \\ y & y \\ z & z \\ \cdots & \cdots \end{vmatrix}$ par Λ sera

$$\begin{vmatrix} \varphi(x,y,z\ldots) & \varphi(x+1,y,z\ldots) \\ \varphi'(x,y,z\ldots) & \varphi'(x+1,y,z\ldots) \\ \varphi''(x,y,z\ldots) & \varphi''(x+1,y,z\ldots) \\ \cdots & \cdots \end{vmatrix}.$$

Pour que cette substitution se réduise à l'une de celles de F,

telle que

$$\begin{vmatrix} x & x+a \\ y & y+a' \\ z & z+a'' \\ \cdots & \cdots \end{vmatrix},$$

il faudra que l'on ait les relations

$$\begin{aligned} \varphi(x+1, y, z\ldots) &= \varphi(x, y, z\ldots) + a, \\ \varphi'(x+1, y, z\ldots) &= \varphi'(x, y, z\ldots) + a', \\ \varphi''(x+1, y, z\ldots) &= \varphi''(x, y, z\ldots) + a''. \\ &\cdots\cdots\cdots\cdots\cdots\cdots \end{aligned}$$

On aura de même, si

$$\begin{vmatrix} x & x+b \\ y & y+b' \\ z & z+b'' \\ \cdots & \cdots \end{vmatrix}$$

est la transformée de $\begin{vmatrix} x & x \\ y & y+1 \\ z & z \\ \cdots & \cdots \end{vmatrix}$ par A,

$$\begin{aligned} \varphi(x, y+1\ldots) &= \varphi(x, y, z\ldots) + b, \\ \varphi'(x, y+1\ldots) &= \varphi'(x, y, z\ldots) + b', \\ \varphi''(x, y+1\ldots) &= \varphi''(x, y, z\ldots) + b''. \\ &\cdots\cdots\cdots\cdots\cdots\cdots \end{aligned}$$

On aura de même

$$\begin{aligned} &\varphi(x, y, z+1\ldots) = \varphi(x, y, z\ldots) + c\ldots. \\ &\cdots\cdots\cdots\cdots\cdots\cdots \end{aligned}$$

On déduit de là, en posant $\varphi(0, 0, 0, \ldots) = \alpha$, $\varphi'(0, 0, 0, \ldots) = \alpha'$,

$\varphi''(0, 0, 0, ..) = \alpha''. ..,$

$$\begin{aligned}
\varphi\,(x, y, z, \ldots) &= a\,x + b\,y + c\,z + \ldots + \alpha,\\
\varphi'(x, y, z, ..) &= a'x + b'y + c'z + \ldots + \alpha',\\
\varphi''(x, y, z, \ldots) &= a''x + b''y + c''z + \ldots + \alpha'',\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

d'où le théorème suivant :

THÉORÈME III. — *Les substitutions du groupe primitif* L *sont toutes de la forme linéaire.*

$$\left|\begin{array}{ll}
x & a\,x + b\,y + c\,z + \ldots + \alpha,\\
y & a'x + b'y + c'z + \ldots + \alpha',\\
z & a''x + b''y + c''z + \ldots + \alpha'',\\
& \ldots\ldots\ldots\ldots\ldots
\end{array}\right|$$

a, b, c,. ., α, α', α'',... étant des entiers constants.

4. Tous les systèmes de valeurs entières de ces coefficients ne sont pas admissibles. En effet, dans toute substitution, une lettre quelconque, dont les indices sont respectivement x_1, y_1, z_1,..., doit remplacer une lettre unique et bien déterminée. Soient x, y, z,... les indices de cette lettre, ils sont liés à x_1, y_1, z_1,... par les relations

$$\begin{aligned}
a\,x + b\,y + c\,z + \ldots + \alpha &\equiv x_1 \pmod{p},\\
a'x + b'y + c'z + \ldots + \alpha' &\equiv y_1 \pmod{p},\\
a''x + b''y + c''z + \ldots + \alpha'' &\equiv z_1 \pmod{p},\\
&\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

Pour que ces relations déterminent x, y, z sans ambiguïté ni impossibilité, il sera nécessaire et suffisant que le déterminant

$$\left|\begin{array}{lll}
a & b & c\ldots\\
a' & b' & c'\ldots\\
a'' & b'' & c''\ldots\\
\ldots & \ldots & \ldots
\end{array}\right| \quad \text{soit} \gtrless 0 \pmod{p}.$$

5. Soit

$$\begin{vmatrix} x & a\,x+b\,y+c\,z+\ldots+\alpha \\ y & a'x+b'y+c'z+\ldots+\alpha' \\ z & a''x+b''y+c''z+\ldots+\alpha'' \\ \cdot & \cdot\cdot\cdot\cdot \quad \cdot\cdot\cdot\cdot\cdot\cdot \quad \cdot\cdot\cdot\cdot \end{vmatrix}$$

une des substitutions du groupe : en la combinant avec la substitution

$$\begin{vmatrix} x & x-\alpha \\ y & y-\alpha' \\ z & z-\alpha'' \\ \cdot & \cdot\cdot\cdot\cdot\cdot\cdot \end{vmatrix},$$

qui est de la forme des F et fait, à ce titre, partie du groupe L, on obtiendra la substitution linéaire sans termes constants

$$\begin{vmatrix} x & a\,x+b\,y+c\,z+\ldots \\ y & a'x+b'y+c'z+\ldots \\ z & a''x+b''y+c''z+\ldots \\ \cdot & \cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot \end{vmatrix}.$$

Les substitutions de cette espèce contenues dans L forment évidemment un groupe $\mathfrak{L}$; car la combinaison de deux substitutions linéaires sans termes constants donne une substitution linéaire également sans termes constants. Ce groupe étant contenu dans L, sera résoluble. D'autre part, il suffit que $\mathfrak{L}$ soit résoluble pour que L le soit; car toutes les substitutions de L s'obtiennent en combinant les substitutions $\mathfrak{L}$ avec celles du faisceau F, qui leur est permutable.

Le groupe $\mathfrak{L}$ est l'un des groupes résolubles les plus généraux parmi ceux dont les substitutions sont linéaires; car si A était un groupe résoluble de cette espèce, plus général que $\mathfrak{L}$, le groupe dérivé de A et de F serait plus général que L, dérivé de $\mathfrak{L}$ et de F, ce qui ne peut être par hypothèse.

THÉORÈME IV. — *Le problème se réduit donc à déterminer les groupes résolubles $\mathfrak{L}$ les plus généraux que possible parmi ceux dont les substi-*

tutions ont la forme linéaire sans termes constants

$$\begin{vmatrix} x & ax+by+cz+\dots \\ y & a'x+b'y+c'z+\dots \\ z & a''x+b''y+c''z+\dots \\ \dots & \dots\dots\dots\dots \end{vmatrix}$$

avec la condition

$$\begin{vmatrix} a & b & c\dots \\ a' & b' & c'\dots \\ a'' & b'' & c''\dots \\ \dots & \dots & \dots \end{vmatrix} \gtrless 0 \pmod{p},$$

et qui, combinés avec les substitutions

$$\mathrm{F} = \begin{vmatrix} x & x+\alpha \\ y & y+\alpha' \\ z & z+\alpha'' \\ \dots & \dots\dots \end{vmatrix},$$

reproduisent un groupe primitif.

CHAPITRE III.

RÉDUCTION DU PROBLÈME AU CAS PRÉCÉDENT.

1. La détermination des groupes résolubles transitifs, mais non primitifs les plus généraux, se ramène au cas des groupes primitifs. Cette réduction fait l'objet des pages suivantes :

2. Soit L un groupe transitif et général, mais non primitif. S'il existe plusieurs manières de répartir les lettres en systèmes tels, que dans toutes les substitutions L les lettres de chaque système soient remplacées par les lettres d'un même système, nous choisirons parmi ces modes de répartition un de ceux où le nombre q des systèmes est *minimum* : soit r le nombre de lettres de chacun d'eux

Les lettres pourront être distinguées les unes des autres par deux indices u et v, l'indice u, variable de 0 à $q-1$, caractérisant les divers systèmes; tandis que l'indice v, variable de 0 à $r-1$, servira à distinguer entre elles les lettres d'un même système.

Chacune des substitutions L sera de la forme

$$l = \begin{vmatrix} u & \varphi(u) \\ v & \psi(u, v) \end{vmatrix}.$$

1° Écrivons en regard de chacune de ces substitutions la substitution suivante

$$\lambda = | u, \varphi(u) |$$

entre q lettres auxiliaires caractérisées par un seul indice u variable de 0 à $q-1$, de telle sorte que chaque lettre auxiliaire corresponde à l'un des systèmes de lettres du groupe L. Le produit ll' de deux substitutions l, l' aura évidemment pour corrélative le produit $\lambda\lambda'$ de λ et λ', corrélatives de l et l'. Les substitutions λ forment donc un groupe résoluble Λ (chap. I^er^, théor. I^er^).

Ce groupe devra être transitif; car le groupe L, permutant transitivement toutes les lettres, devra *à fortiori* permuter transitivement les systèmes. De plus, il sera primitif; en effet, s'il ne l'était pas, on pourrait, en remplaçant l'indice unique u par deux indices u_1 et u_2 convenablement choisis, mettre toutes les substitutions Λ sous la forme

$$\begin{vmatrix} u_1 & \varphi_1(u_1) \\ u_2 & \varphi_2(u_1, u_2) \end{vmatrix},$$

et par suite les substitutions L sous la forme

$$\begin{vmatrix} u_1 & \varphi_1(u_1) \\ u_2 & \varphi_2(u_1, u_2) \\ v & \psi_1(u_1, u_2, v) \end{vmatrix};$$

d'où l'on voit qu'en réunissant ensemble toutes les lettres pour lesquelles l'indice u_1 est le même, on aurait, contrairement à notre

supposition, une répartition en systèmes dont le nombre serait inférieur à q.

2° Le groupe A étant primitif, il résulte du chapitre II : 1° que q égale une puissance p^n d'un nombre premier p ; 2° qu'on peut remplacer l'indice unique u par n indices $x, y, z, \ldots$, variant chacun de 0 à $p-1$, et choisis de telle sorte que les substitutions de A soient toutes de la forme linéaire

$$\left|\begin{array}{ll} x & a\,x + b\,y + c\,z + \ldots + \alpha \\ y & a'x + b'y + c'z + \ldots + \alpha' \\ z & a''x + b''y + c''z + \ldots + \alpha'' \\ \cdots & \cdots\cdots\cdots\cdots\cdots \end{array}\right| ;$$

en outre, ce groupe A contiendra toutes les substitutions du faisceau

$$\left|\begin{array}{ll} x & x + \alpha \\ y & y + \alpha' \\ z & z + \alpha'' \\ \cdots & \cdots\cdots \end{array}\right| .$$

Les substitutions L prendront la forme :

$$\left|\begin{array}{ll} x & ax + by + cz + \ldots + \alpha \\ y & a'x + b'y + c'z + \ldots + \alpha' \\ z & a''x + b''y + c''z + \ldots + \alpha'' \\ \cdots & \cdots\cdots\cdots\cdots\cdots \\ v & \text{fonct. de } (x, y, z, \ldots, v) \end{array}\right| .$$

3° Considérons en particulier parmi ces substitutions celles de la forme

$$\left|\begin{array}{ll} x & x + \alpha \\ y & y + \alpha' \\ z & z + \alpha'' \\ \cdots & \cdots\cdots \\ v & \text{fonct. de } (x, y, z, \ldots, v) \end{array}\right| .$$

Elles forment évidemment un groupe E auxquelles toutes les autres

sont permutables. On pourra donc les faire passer en avant lorsque l'on construira l'échelle génératrice de L.

4° Considérons plus spécialement encore les substitutions, s'il en existe, qui ne déplacent pas les systèmes : elles sont de la forme

$$\left|\begin{array}{ll} x & x \\ y & y \\ z & z \\ \cdots & \cdots \\ v & \text{fonct. de } (x, y, z, \ldots, v) \end{array}\right|,$$

et sont comprises parmi les E. Elles forment évidemment un groupe F auquel toutes les autres sont permutables. On pourra donc les faire passer en avant de toutes les autres.

3. LEMME I. — *S'il existe des substitutions* F *qui ne déplacent pas les systèmes, soit* F_1 *l'une d'elles, qui s'obtienne en exécutant simultanément certains déplacements* $f_1, f_1', f_1'', \ldots$ *dans l'intérieur des divers systèmes* S, S', S'', ... *entre les lettres qui les composent.*

Chacune des substitutions partielles $f_1, f_1', f_1'', \ldots$ *considérée isolément, devra faire partie de* F.

En effet, soit $F_2 = f_2 f_2' f_2'' \ldots$ une autre substitution de F; les déplacements que la substitution $F_1 F_2$ fait éprouver aux lettres des systèmes S, S', S'' seront respectivement $f_1 f_2$, $f_1' f_2'$, $f_1'' f_2'', \ldots$. Le groupe F, contenu dans L, étant résoluble, chacun des groupes partiels $(f_1, f_2, \ldots)$, $(f_1', f_2', \ldots)$, $(f_1'', f_2'', \ldots)$ sera donc résoluble (chap. I^er^, théor. I^er^); d'ailleurs ces groupes déplaçant chacun de son côté des lettres différentes sont échangeables entre eux : le groupe $\mathfrak{F} = (f_1, f_2, \ldots, f_1', f_2', \ldots, f_1'', f_2'', \ldots)$, dérivé de leur combinaison, est donc résoluble.

Toutes les substitutions L sont permutables à $\mathfrak{F}$ comme elles le sont à F. Soit en effet l une de ces substitutions : la transformée de F_1 par l, $l^{-1} F_1 l = l^{-1} f_1 l . l^{-1} f_1' l . l^{-1} f_1'' l, \ldots$, doit faire partie du groupe F. Donc les déplacements qu'elle fait subir aux lettres dans chacun des divers systèmes font partie du groupe $\mathfrak{F}$. Or les déplacements relatifs

aux systèmes auquels l fait succéder S, S′, S″,... sont respectivement $l^{-1}f_1 l$, $l^{-1}f_1' l$, $l^{-1}f_1'' l$,.... Chacune de ces substitutions fait donc partie du groupe $\mathfrak{F}$.

Le groupe dérivé de la combinaison de $\mathfrak{F}$ avec les substitutions de L sera donc résoluble. Il serait d'ailleurs, contre l'hypothèse, plus général que L, si toutes les substitutions $\mathfrak{F}$ n'étaient pas comprises dans L, et par suite dans F.

Le lemme est donc démontré.

4. Adjoignons maintenant successivement aux substitutions F les autres substitutions du groupe, en commençant par les E. La première sera de la forme

$$\mathrm{A} = \begin{vmatrix} x & x+1 \\ y & y \\ z & z \\ \cdots & \cdots \\ v & \varphi(x, y, z, \ldots, v) \end{vmatrix}.$$

On peut simplifier cette forme. En effet, les diverses valeurs de l'indice v peuvent être réparties d'une manière entièrement arbitraire entre les lettres de chaque système. On peut donc admettre : 1° qu'on laisse cette répartition arbitraire dans tous ceux des systèmes pour lesquels le premier indice x est égal à zéro; 2° qu'on donne à chaque lettre du système caractérisé par les indices 1, y, z,.. le même indice v qu'à celle des lettres du système caractérisé par les indices 0, y, z,..., à laquelle A la fait succéder; 3° qu'on donne de même à chaque lettre du système 2, y, z,... le même indice qu'à celle du système 1, y, z,..., à laquelle A la fait succéder, etc., jusqu'au système $p-1$, y, z. La fonction

$$\varphi(x, y, z, \ldots, v)$$

se réduira donc à v, quels que soient y, z,... pour toutes les valeurs de x à l'exception de $p-1$, auquel cas elle sera égale à une fonction

$$\psi(y, z, \ldots, v)$$

de y, z,... et v.

Cela posé, la substitution A est le produit de deux autres substi-

tutions

$$A_1 = \begin{vmatrix} x & x \\ y & y \\ z & z \\ \cdots & \\ v & \varphi(x, y, z, \ldots, v) \end{vmatrix} \quad \text{et} \quad \mathfrak{A} = \begin{vmatrix} x & x+1 \\ y & y \\ z & z \\ \cdots & \\ v & v \end{vmatrix},$$

A_1 fait partie du groupe F. En effet, on voit aisément que la substitution A^p est égale à

$$\begin{vmatrix} x & x \\ y & y \\ z & z \\ \cdots & \\ v & \psi(y, z, \ldots, v) \end{vmatrix},$$

elle fait partie de F : les déplacements qu'elle fait subir aux lettres des systèmes dont le premier indice x est $p-1$, considérées isolément, feront partie de F (lemme I); or A_1 représente précisément l'ensemble de ces déplacements.

Les substitutions du groupe à cette période de l'opération s'obtiendront donc en combinant les F avec

$$\mathfrak{A} = \begin{vmatrix} x & x+1 \\ y & y \\ z & z \\ \cdots & \\ v & v \end{vmatrix}.$$

5. Introduisons la substitution suivante :

$$B = \begin{vmatrix} x & x \\ y & y+1 \\ z & z \\ \cdots & \\ v & \varphi_1(x, y, z, \ldots, v) \end{vmatrix}.$$

Nous avons laissé arbitraire la valeur à assigner à l'indice v pour chacune des lettres des systèmes pour lesquels le premier indice x est nul : laissons encore ce choix arbitraire dans les systèmes pour lesquels $x = 0$, $y = 0$; mais donnons à chaque lettre du système caractérisé par les indices 0, 1, z,... le même indice v qu'à celle du système 0, 0, z à laquelle B la fait succéder : donnons de même à chaque lettre du système caractérisé par les indices 0, 2, z le même indice v qu'à celle du système 0, 1, z,... à laquelle B la fait succéder, etc. La fonction $\varphi_1(x, y, z, \ldots, v)$ se trouvera réduite à v lorsque $x = 0$ pour toutes les valeurs de y, excepté pour $y = p - 1$, auquel cas elle se réduira à une fonction de z et de v, $\psi_1(z, \ldots, v)$.

Cela posé, B sera le produit : 1° d'une substitution B_1 qui laisse toutes les lettres immobiles, à l'exception de celles $a_{0,p-1,z,\ldots,v}$, dont les deux premiers indices sont 0 et $p - 1$, qu'elle remplacera respectivement par $a_{0,p-1,z,\ldots,\psi_1(z,\ldots,v)}$; 2° d'une substitution

$$B' = \begin{vmatrix} x & x \\ y & y+1 \\ z & z \\ \cdots & \cdots \\ v & \varphi'_1(x, y, z, \ldots, v) \end{vmatrix},$$

la fonction φ'_1 se réduisant à v pour $x = 0$, quels que soient $y, z, \ldots, v$.

On voit aisément que B_1 n'est autre chose que l'ensemble des déplacements que la substitution B^p, qui fait partie du groupe F, fait éprouver aux lettres dont les deux premiers indices sont 0 et $p - 1$; donc B_1 fait partie de F (lemme I[er]). On obtiendra donc le même résultat en adjoignant au groupe (F, $\mathfrak{A}$) la substitution B_1, ou la substitution simplifiée $B' = B_1^{-1} B$. Cette dernière substitution devra, de même que B, être permutable au groupe (F, $\mathfrak{A}$), ce qui permettra de déterminer la fonction $\varphi'_1(x, y, z, \ldots, v)$ pour les valeurs de x autres que zéro.

Soit, en effet, donnée la condition

$$B'^{-1} \mathfrak{A} B' = \mathfrak{A}^\alpha F_1 \ (*) \quad \text{ou} \quad \mathfrak{A} B' F_1^{-1} = B' \mathfrak{A}^\alpha,$$

(*) $\mathfrak{A}$ étant permutable à F, toutes les substitutions du groupe (F, $\mathfrak{A}$) sont de la forme $\mathfrak{A}^\alpha F_1$.

en désignant par F_1 l'une des substitutions F. Soit

$$F_1^{-1} = \begin{vmatrix} x & x \\ y & y \\ z & z \\ \cdots & \\ v & \chi(x, y, z, \ldots, v) \end{vmatrix};$$

on aura d'une part

$$\mathfrak{A}B'F_1^{-1} = \begin{vmatrix} x & x+1 \\ y & y+1 \\ z & z \\ \cdots & \\ v & \chi[x+1, y+1, z, \ldots, \varphi'_1(x+1, y, z, \ldots, v)] \end{vmatrix},$$

et d'autre part

$$B'\mathfrak{A}^{\alpha} = \begin{vmatrix} x & x+\alpha \\ y & y+1 \\ z & z \\ \cdots & \\ v & \varphi'_1(x, y, z, \ldots, v) \end{vmatrix}.$$

Pour que ces deux substitutions soient identiques, on devra avoir d'un côté $\alpha = 1$, et de l'autre

$$\varphi'_1(x, y, z, \ldots, v) = \chi[x+1, y+1, z, \ldots, \varphi'_1(x+1, y, z, \ldots, v)].$$

Cette équation peut servir à déterminer de proche en proche la valeur de la fonction φ'_1 pour $x = p-1$, $p-2$, etc., en partant de sa valeur initiale pour $x = 0$.

Pour $x = p-1$, on aura

$$\begin{aligned} \varphi'_1(p-1, y, z, \ldots, v) &= \chi[0, y+1, z, \ldots, \varphi'_1(0, y, z, \ldots, v)] \\ &= \chi(0, y+1, z, \ldots, v). \end{aligned}$$

B′ remplacera ainsi en général la lettre $a_{p-1, y, z, \ldots, v}$ par la lettre

$a_{p-1,y+1,z,\ldots,\chi(0,y+1,z,\ldots,\nu)}$. Soit B'_1 une substitution qui laisse toutes les lettres immobiles, sauf celles $a_{p-1,y+1,z,\ldots,\nu}$, dont le premier indice est $p-1$, et qui remplace celles-ci respectivement par $a_{p-1,y+1,z,\ldots,\chi(0,y+1,z,\ldots,\nu)}$. Posons $B' = B''B'_1$, B'' étant une nouvelle substitution : la substitution $B'' = B'B'^{-1}_1$ sera de la forme

$$B'' = \begin{vmatrix} x & x \\ y & y+1 \\ z & z \\ \cdots & \cdots \\ \nu & \varphi''_1(x,y,z,\ldots,\nu) \end{vmatrix},$$

la fonction φ''_1 se réduisant à ν pour $x = 0$ et $x = p-1$, quels que soient $y, z, \ldots, \nu$.

Cela posé, la substitution B'_1 fait partie du groupe F. En effet, $\mathfrak{A}$ étant permutable à F, la transformée

$$\mathfrak{A}^{-1}F_1^{-1}\mathfrak{A} = \begin{vmatrix} x-1 & x-1 \\ y & y \\ z & z \\ \cdots & \cdots \\ \nu & \chi(x,y,z,\ldots,\nu) \end{vmatrix} = \begin{vmatrix} x & x \\ y & y \\ z & z \\ \cdots & \cdots \\ \nu & \chi(x+1,y,z,\ldots,\nu) \end{vmatrix}$$

de F_1^{-1} par $\mathfrak{A}$ fera elle-même partie du groupe F. Les déplacements qu'elle fait subir aux lettres des systèmes dont le premier indice est $p-1$, considérées isolément, font partie de F (lemme I^{er}). Mais l'ensemble de ces déplacements est précisément B'_1.

On obtiendra donc le même résultat en adjoignant au groupe (F, $\mathfrak{A}$) la substitution B', ou la substitution simplifiée B''.

On voit exactement de même que l'on peut poser $B'' = B'''B''_1$, B''' étant une substitution de la forme

$$\begin{vmatrix} x & x \\ y & y+1 \\ z & z \\ \cdots & \cdots \\ \nu & \varphi'''_1(x,y,z,\ldots,\nu) \end{vmatrix},$$

dans laquelle la fonction φ''' se réduit à ν toutes les fois que $x = 0$ ou $= p - 1$ ou $= p - 2$; et B'''_1 étant une substitution de F.

On obtiendra encore le même résultat en adjoignant au groupe $(F, \mathfrak{A})$ la substitution B'' ou la substitution simplifiée B'''.

En poursuivant ainsi, on arrivera à une dernière substitution, où la fonction φ se réduit à ν pour toutes les valeurs de x.

Soit

$$\mathfrak{V} = \begin{vmatrix} x & x \\ y & y+1 \\ z & z \\ \cdots & \cdots \\ \nu & \nu \end{vmatrix}$$

cette dernière substitution. Le groupe dérivé de la combinaison de F, $\mathfrak{A}$, $\mathfrak{V}$ sera le même que celui dérivé de la combinaison de F, $\mathfrak{A}$, B.

6. On opérera de même sur la substitution suivante C, qu'on décomposera en une série de substitutions successives faisant toutes partie de F, à l'exception de la dernière,

$$\mathfrak{S} = \begin{vmatrix} x & x \\ y & y \\ z & z+1 \\ \cdots & \cdots \\ \nu & \nu \end{vmatrix}.$$

Poursuivant ainsi, on obtient en dernière analyse la proposition suivante :

LEMME II. — *Les substitutions* E *résultent toutes de la combinaison des substitutions* F *avec les suivantes :*

$$\mathfrak{A} = \begin{vmatrix} x & x+1 \\ y & y \\ z & z \\ \cdots & \cdots \\ \nu & \nu \end{vmatrix}, \quad \mathfrak{V} = \begin{vmatrix} x & x \\ y & y+1 \\ z & z \\ \cdots & \cdots \\ \nu & \nu \end{vmatrix}, \quad \mathfrak{S} = \begin{vmatrix} x & x \\ y & y \\ z & z+1 \\ \cdots & \cdots \\ \nu & \nu \end{vmatrix}, \ldots.$$

7. Soit maintenant

$$H = \begin{vmatrix} x & a\,x + b\,y + c\,z + \ldots + \delta \\ y & a'x + b'y + c'z + \ldots + \delta' \\ z & a''x + b''y + c''z + \ldots + \delta'' \\ \ldots & \ldots\ldots\ldots\ldots\ldots \\ v & \psi(x, y, z, \ldots, v) \end{vmatrix}$$

l'une quelconque des substitutions du groupe L; elle doit être permutable à E. On aura donc, entre autres relations, la suivante :

$$H^{-1}\mathfrak{A}H = \text{une substitution de E, telle que } F, \mathfrak{A}^{\alpha}\mathfrak{B}^{\beta}\mathfrak{C}^{\gamma}\ldots,$$

ou, en remarquant que H est permutable au groupe partiel F,

$$\mathfrak{A}H = HF_1\mathfrak{A}^{\alpha}\mathfrak{B}^{\beta}\mathfrak{C}^{\gamma}\ldots = F_2H\mathfrak{A}^{\alpha}\mathfrak{B}^{\beta}\mathfrak{C}^{\gamma},$$

$$F_2 = \begin{vmatrix} x & x \\ y & y \\ z & z \\ \ldots & \ldots\ldots\ldots \\ v & \chi(x, y, z, \ldots, v) \end{vmatrix}$$ étant une substitution de F.

Or on a, d'une part,

$$\mathfrak{A}H = \begin{vmatrix} x & a\,(x+1) + b\,y + c\,z + \ldots + \delta \\ y & a'(x+1) + b'y + c'z + \ldots + \delta' \\ z & a''(x+1) + b''y + c''z + \ldots + \delta'' \\ \ldots & \ldots\ldots\ldots\ldots\ldots \\ v & \psi\,(x+1, y, z, \ldots, v) \end{vmatrix},$$

et, d'autre part,

$$F_2H\mathfrak{A}^{\alpha}\mathfrak{B}^{\beta}\mathfrak{C}^{\gamma} = \begin{vmatrix} x & a\,x + b\,y + c\,z + \ldots + \delta + \alpha \\ y & a'x + b'y + c'z + \ldots + \delta' + \alpha' \\ z & a''x + b''y + c''z + \ldots + \delta'' + \alpha'' \\ \ldots & \ldots\ldots\ldots\ldots\ldots \\ v & \psi[x, y, z, \ldots, \chi(x, y, z, \ldots, v)] \end{vmatrix}.$$

Pour que ces deux substitutions soient identiques, on aura, entre autres équations de condition, celle-ci :

$$\psi(x+1, y, z, \ldots, v) = \psi[x, y, z, \ldots, \chi(x, y, z, \ldots, v)].$$

On trouverait de même

$$\psi(x, y+1, z, \ldots, v) = \psi[x, y, z, \ldots, \chi'(x, y, z, \ldots, v)],$$
$$\psi(x, y, z+1, \ldots, v) = \psi[x, y, z, \ldots, \chi''(x, y, z, \ldots, v)],$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$

$$F'_2 = \begin{vmatrix} x & x \\ y & y \\ z & z \\ \ldots & \ldots \\ v & \chi'(x, y, z, \ldots, v) \end{vmatrix}, \quad F''_2 = \begin{vmatrix} x & x \\ y & y \\ z & z \\ \ldots & \ldots \\ v & \chi''(x, y, z, \ldots, v) \end{vmatrix}, \ldots,$$

étant des substitutions du groupe F.

Ces équations de condition permettent de déterminer de proche en proche les valeurs de la fonction $\psi(x, y, z, \ldots, v)$, lorsqu'on connaît sa valeur initiale pour $x = 0$, $y = 0$, $z = 0, \ldots$.

On aura ainsi, en posant $x = 0$, $y = 0$, $z = 0, \ldots$,

$$\psi(1, 0, 0, \ldots, v) = \psi[0, 0, 0, \ldots, \chi(0, 0, 0, \ldots, v)].$$

D'où l'on voit que la substitution H est le produit de deux autres :

1° La première, G, laissant toutes les lettres immobiles, à l'exception des suivantes : $a_{1,0,0,\ldots,v}$, qu'elle remplace respectivement par $a_{1,0,0,\ldots,\chi(0,0,0,\ldots,v)}$;

2° La seconde,

$$H' = \begin{vmatrix} x & a\,x + b\,y + c\,z + \ldots + \delta \\ y & a'x + b'y + c'z + \ldots + \delta' \\ z & a''x + b''y + c''z + \ldots + \delta'' \\ \ldots & \ldots\ldots\ldots\ldots\ldots \\ v & \psi'(x, y, z, \ldots, v) \end{vmatrix},$$

où la fonction $\psi'(x, y, z, \ldots, v)$ est égale à $\psi(x, y, z, \ldots, v)$ pour toutes

les valeurs de x, y, z,..., v, excepté pour $x=1$, $y=0$, $z=0$,..., auquel cas on a

$$\psi'(1, 0, 0,\ldots, v) = \psi(0, 0, 0,\ldots, v);$$

ψ' satisfait ainsi à la condition

$$\psi'(1, 0, 0,\ldots, v) = \psi'(0, 0, 0,\ldots, v).$$

D'ailleurs G fait partie du groupe F. En effet, la transformée de F_2 par $\mathcal{A}$,

$$\mathcal{A}^{-1}F_2\mathcal{A} = \begin{vmatrix} x+1 & x+1 \\ y & y \\ z & z \\ \ldots & \ldots \\ v & \chi(x, y, z,\ldots, v) \end{vmatrix},$$

en fait partie; les déplacements qu'elle fait subir aux lettres du système 1, 0, 0,..., considérées isolément, en feront partie (lemme I) : or ce système de déplacements est précisément G.

On démontrera de même que la substitution H' est le produit de deux autres, dont l'une, G', fait partie de F, tandis que l'autre, H'', est égale à

$$\begin{vmatrix} x & ax+by+cz+\ldots+\delta \\ y & a'x+b'y+c'z+\ldots+\delta' \\ z & a''x+b''y+c''z+\ldots+\delta'' \\ \ldots & \ldots \\ v & \psi''(x, y, z,\ldots, v) \end{vmatrix},$$

la fonction ψ'' satisfaisant à la condition

$$\psi''(2, 0, 0,\ldots, v) = \psi''(1, 0, 0,\ldots, v) = \psi''(0, 0, 0,\ldots, v);$$

et, continuant ainsi, on arrivera enfin à décomposer H en une série de substitutions G, G',..., H_1, faisant toutes partie de F, à l'exception

de la dernière,

$$H_1 = \begin{vmatrix} x & ax + by + cz + \ldots + \delta \\ y & a'x + b'y + c'z + \ldots + \delta' \\ z & a''x + b''y + c''z + \ldots + \delta'' \\ \ldots & \ldots\ldots\ldots\ldots\ldots \\ \nu & \psi_1(y, z, \ldots, \nu) \end{vmatrix},$$

la fonction ψ_1 restant la même pour toutes les valeurs de x.

On décomposera de même H_1 en substitutions G_1, $G'_1, \ldots$, H_2, faisant toutes partie de F, excepté la dernière,

$$H_2 = \begin{vmatrix} x & ax + by + cz + \ldots + \delta \\ y & a'x + b'y + c'z + \ldots + \delta' \\ z & a''x + b''y + c''z + \ldots + \delta'' \\ \ldots & \ldots\ldots\ldots\ldots\ldots \\ \nu & \psi_2(z, \ldots, \nu) \end{vmatrix}.$$

Continuaut ainsi, on arrivera, en dernière analyse, à ramener H à des substitutions du groupe F combinées avec une substitution

$$S = \begin{vmatrix} x & ax + by + cz + \ldots + \delta \\ y & a'x + b'y + c'z + \ldots + \delta' \\ z & a''x + b''y + c''z + \ldots + \delta'' \\ \ldots & \ldots\ldots\ldots\ldots\ldots \\ \nu & \psi_n(\nu) \end{vmatrix},$$

la fonction ψ_n étant entièrement indépendante des valeurs de $x, y, z, \ldots$.

Cette dernière substitution se décompose elle-même en deux autres, échangeables entre elles :

$$I = \begin{vmatrix} x & x \\ y & y \\ z & z \\ \ldots & \ldots \\ \nu & \psi_n(\nu) \end{vmatrix} \quad \text{et} \quad J = \begin{vmatrix} x & ax + by + cz + \ldots + \delta \\ y & a'x + b'y + c'z + \ldots + \delta' \\ z & a''x + b''y + c''z + \ldots + \delta'' \\ \ldots & \ldots\ldots\ldots\ldots\ldots \\ \nu & \nu \end{vmatrix}.$$

Nous obtenons donc comme résultat le lemme suivant :

LEMME III. — *Les substitutions du groupe* L *s'obtiennent toutes par la combinaison des substitutions* F, $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$,..., *avec certaines substitutions de la forme*

$$IJ, \quad I'J',\ldots,$$

J, J',... *étant, ainsi que* $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$,..., *des substitutions qui permutent les systèmes entre eux, en remplaçant les unes par les autres les lettres affectées du même indice* ν : I, I',... *étant au contraire des substitutions qui laissent les systèmes immobiles, en permutant entre elles, simultanément et de la même manière, les lettres correspondantes de chacun d'eux.*

8. Soient IJ et I'J' deux substitutions de la forme ci-dessus contenues dans le groupe L; IJ.I'J' leur produit. Les déplacements d'ensemble que cette dernière substitution fait subir aux systèmes seront évidemment représentés par JJ', et les déplacements des lettres dans l'intérieur des systèmes le seront par II'; d'ailleurs le groupe dérivé de IJ, I'J',..., étant contenu dans L, est résoluble : chacun des deux groupes (I, I',...), (J, J',...), corrélatifs à celui-là, le sera donc également (chap. I^er^, théor. I^er^).

2° Les deux groupes (I, I',...), (J, J',...) ont leurs substitutions respectivement échangeables entre elles : le groupe (I, I',..., J, J',...), résultant de leur combinaison, sera donc résoluble.

3° Les substitutions J, J',... ayant la forme linéaire, sont permutables au groupe dérivé de $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$,...; les I, I',... sont échangeables à chacune de ces substitutions.

4° Enfin toutes les substitutions I, I',..., J, J',... sont permutables à F. Les substitutions IJ, I'J' l'étant, il suffira, pour établir cette proposition, de montrer que J, J',... le sont.

Or chacune des substitutions F résulte de la combinaison de substitutions partielles f, f', f'',... déplaçant chacune les lettres d'un seul système. Ces substitutions partielles, considérées isolément, font elles-mêmes partie du groupe F (lemme I^er^). Si nous prouvons que la transformée de chacune d'elles par J en fait également partie, J sera évidemment permutable à ce groupe.

Soit donc f une substitution qui laisse toutes les lettres immobiles, excepté les lettres $a_{x_0,y_0,z_0,\ldots,\nu}$ du système caractérisé par les indices $x_0, y_0, z_0, \ldots$, lettres qu'elle remplace respectivement par $a_{x_0,y_0,z_0,\ldots,\varphi(\nu)}$; soit

$$J^{-1} = \begin{vmatrix} x & ax+by+cz+\ldots+\delta \\ y & a'x+b'y+c'z+\ldots+\delta' \\ z & a''x+b''y+c''z+\ldots+\delta'' \\ \ldots & \ldots\ldots\ldots\ldots \\ \nu & \nu \end{vmatrix};$$

la transformée $J^{-1}fJ$ laisse toutes les lettres immobiles, à l'exception des suivantes :

$$a_{ax_0+by_0+cz_0+\ldots+\delta,\ a'x_0+b'y_0+c'z_0+\ldots+\delta',\ a''x_0+b''y_0+c''z_0+\ldots+\delta'',\ldots,\nu}$$

qu'elle remplace respectivement par les suivantes :

$$a_{ax_0+by_0+cz_0+\ldots+\delta,\ a'x_0+b'y_0+c'z_0+\ldots+\delta',\ a''x_0+b''y_0+c''z_0+\ldots+\delta'',\ldots,\varphi(\nu)}$$

et l'on voit aisément que cette substitution est identique à la transformée de f par

$$\mathfrak{A}^{-(ax_0+by_0+cz_0+\ldots+\delta)}\,\mathfrak{B}^{-(a'x_0+b'y_0+c'z_0+\ldots+\delta')}\,\mathfrak{C}^{-(a''x_0+b''y_0+c''z_0+\ldots+\delta'')},$$

laquelle fait partie de F.

5° Les observations précédentes montrent que le groupe dérivé des substitutions $(F, \mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \ldots, I, I', \ldots, J, J', \ldots)$ est résoluble : il contient toutes les substitutions de L; et comme nous admettons qu'il ne peut être plus général, il devra se confondre avec L.

Mais les substitutions de L qui ne déplacent pas les systèmes sont les F; dans le groupe $(F, \mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \ldots, I, I', \ldots, J, J', \ldots)$, ce sont les F combinées aux I, I', ... Pour que les deux groupes soient identiques, il faut donc que les substitutions I, I', ... rentrent toutes dans F.

Nous obtenons donc la proposition suivante :

LEMME IV. — *Toutes les substitutions de* L *résultent de la combinaison des substitutions* F, $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, ..., J, J', ..., etc.

9. Les substitutions $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$,..., J, J',... permutent les systèmes entre eux, en remplaçant les unes par les autres les lettres correspondantes : elles forment entre ces q systèmes, considérés chacun comme un tout d'une seule pièce, un groupe de substitutions Δ, qui sera résoluble et primitif comme nous l'avons vu plus haut.

Le groupe F est formé par la combinaison d'une série de substitutions qui ne déplacent chacune que les lettres d'un seul système. Soient respectivement $\Gamma_{0,0,0},\ldots$, $\Gamma_{x_0,y_0,z_0},\ldots$ les groupes formés en réunissant celles de ces substitutions qui déplacent les lettres des systèmes respectivement caractérisés par les indices o, o, o,..., $x_0, y_0, z_0,\ldots$, etc. Le groupe F résultera de la combinaison de ces groupes partiels.

Les divers groupes $\Gamma_{0,0,0},\ldots$, $\Gamma_{x_0,y_0,z_0},\ldots$ sont les transformés d'un seul d'entre eux, tel que $\Gamma_{0,0,0},\ldots$ par les substitutions $(\mathfrak{A}, \mathfrak{B}, \mathfrak{C},\ldots)$. En effet, la substitution $\mathfrak{A}^{-x_0}\mathfrak{B}^{-y_0}\mathfrak{C}^{-z_0}\ldots$ transforme les $\Gamma_{0,0,0},\ldots$ en d'autres substitutions, également comprises dans F et ne déplaçant que les lettres du seul système $x_0, y_0, z_0,\ldots$; ces transformées sont donc comprises dans le groupe $\Gamma_{x_0,y_0,z_0}\ldots$. Réciproquement, toute substitution dont la transformée ne déplacera que les lettres du système $x_0, y_0, z_0,\ldots$ ne devra elle-même déplacer que celles du système o, o, o,..., et sera comprise dans $\Gamma_{0,0,0},\ldots$. $\Gamma_{x_0,y_0,z_0},\ldots$ sera donc précisément le groupe transformé de $\Gamma_{0,0,0},\ldots$ par $\mathfrak{A}^{-x_0}\mathfrak{B}^{-y_0}\mathfrak{C}^{-z_0}\ldots$.

LEMME V. — Ainsi *les substitutions* L *résulteront toutes de la combinaison d'un groupe résoluble et primitif* Δ *qui permute les* p^n *systèmes tout d'une pièce, en remplaçant les unes par les autres les lettres correspondantes, avec un groupe résoluble* $\Gamma_{0,0,0},\ldots$ *qui laisse toutes les lettres immobiles, excepté les* r *lettres du premier système, qu'il permute entre elles.*

10. *Soient réciproquement* Δ et $\Gamma_{0,0,0},\ldots$ *deux groupes quelconques satisfaisant à ces conditions : le groupe résultant de leur combinaison sera résoluble.*

En effet, les premières substitutions de Δ, $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, etc.,..., transformeront respectivement $\Gamma_{0,0,0},\ldots$ en une suite de groupes pareils $\Gamma_{0,0,0},\ldots$, $\Gamma_{x_0,y_0,z_0},\ldots$ déplaçant chacun les lettres de l'un des systèmes.

Ces groupes déplaçant des lettres différentes sont échangeables entre eux, et formeront par suite, par leur réunion, un groupe résoluble F auquel les $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$,... seront permutables. Les autres substitutions de Δ le seront également (n° 8, 4°). Le groupe L, dérivé de F et de Δ, ou, ce qui revient au même, de $\Gamma_{0,0,0},\ldots$ et de Δ, sera donc résoluble.

Pour que le groupe L soit aussi général que possible, il faudra évidemment que les deux groupes Δ et $\Gamma_{0,0,0},\ldots$ aient été chacun de son côté choisis aussi généraux que possible. Enfin, *le groupe* $\Gamma_{0,0,0},\ldots$ *doit être transitif*. Car si ses substitutions ne permettaient de faire succéder à une lettre donnée qu'une partie des lettres du premier système, ces substitutions, combinées aux Δ, ne permettraient de lui faire succéder que ces mêmes lettres, jointes aux lettres correspondantes des autres systèmes. Le groupe L ne serait donc pas transitif.

Remarque. — Si Δ et $\Gamma_{0,0,0},\ldots$ contiennent respectivement N et N' substitutions, F en contiendra évidemment N'^{p^n} et L en contiendra NN'^{p^n}.

En récapitulant tout ce qui précède, nous obtenons donc le théorème suivant :

THÉORÈME I. — *Soit* L *un des groupes résolubles transitifs, mais non primitifs, les plus généraux entre m lettres : soit q le nombre des systèmes de lettres dans celle des répartitions, s'il en existe plusieurs, pour laquelle ce nombre est minimum; soit r le nombre des lettres de chaque système.*

Le groupe L *s'obtiendra en réunissant les substitutions résultant de la combinaison des deux groupes partiels suivants :*

1° *Un groupe résoluble* Δ, *dont les substitutions déplacent les systèmes d'un mouvement d'ensemble, sans altérer l'ordre des lettres dans leur intérieur : les déplacements des q systèmes entre eux formant d'ailleurs un groupe transitif, primitif et général.*

2° *Un groupe* Γ, *laissant toutes les lettres immobiles, à l'exception des r lettres de l'un des systèmes, le premier, par exemple, qu'il permute entre elles et à l'égard desquelles il est résoluble, transitif et général.*

11. Si ce dernier groupe Γ n'est pas primitif, que q' y soit le nombre des systèmes, $r' = \frac{r}{q'}$ celui des lettres de chacun d'eux, le groupe Γ peut à son tour se décomposer en deux autres Δ' et Γ', dont le premier permutera les q' systèmes entre eux d'une manière primitive; l'autre permutera entre elles les r' lettres d'un même système; si ce dernier n'est pas primitif, on pourra poursuivre la réduction, etc.

On obtient ainsi le théorème suivant :

THÉORÈME II. — *La détermination des groupes résolubles, généraux et transitifs, mais non primitifs, relatifs à une décomposition quelconque du nombre m en facteurs successifs q, q', q'',..., se ramène à celle des groupes primitifs* Δ, Δ', Δ'',... *entre q lettres, entre q' lettres, etc.*

Remarque I. — Pour que cette détermination soit possible, il faut que chacun des facteurs q, q',... soit une puissance de nombre premier (chap. II).

Remarque II. — Soient respectivement N, N', N'',... les nombres de substitutions des groupes Δ, Δ', Δ'',... : celui des substitutions du groupe non primitif, formé au moyen de ceux-là, sera évidemment $NN'^{q}N''^{qq'}\ldots$.

CHAPITRE IV.

CLASSIFICATION DES GROUPES RÉSOLUBLES.

Les résultats précédents suggèrent tout naturellement l'idée de répartir les types d'équations irréductibles et résolubles par radicaux d'un degré donné m en classes, suivant celle des décompositions de la forme $m = p^n p'^{n'}\ldots$, à laquelle appartiennent respectivement les groupes de ces équations.

Mais, pour que cette classification soit juste, il faut être certain que les groupes construits par notre méthode sont généraux et distincts les uns des autres, ce qui n'a pas été suffisamment établi jusqu'à présent. En effet, étant donnée une décomposition quelconque $m = p^n p'^{n'}\ldots$,

nous avons appris à former les groupes résolubles les plus généraux parmi ceux qui sont relatifs à cette décomposition ; mais il pourrait se faire que ces groupes fussent identiques, à la notation près, à certains groupes relatifs à d'autres décompositions ou à d'autres groupes non généraux contenus dans ceux-là. Nous allons prouver qu'il existe effectivement un cas, et *un seul,* où cette circonstance se présente.

THÉORÈME I. — *Aucun groupe relatif à une décomposition de m où deux facteurs successifs soient égaux à 2 ne peut être général.*

Soient, en effet,

$$m = p^n \cdot 2 \cdot 2 \cdot p'^{n'} \dots$$

la décomposition considérée, Δ, Δ', Δ'', Δ'''... les groupes successifs qui, combinés ensemble, reproduisent le groupe considéré G : les lettres peuvent être groupées en systèmes et en hypersystèmes choisis de telle sorte, 1° que le groupe $(\Delta'''\dots)$ permute entre elles des lettres du premier système sans déplacer les autres ; 2° que le groupe (Δ', Δ'') permute entre eux les systèmes du premier hypersystème, en remplaçant les unes par les autres les lettres correspondantes, sans déplacer les lettres des autres hypersystèmes ; 3° enfin le groupe Δ permute entre eux les hypersystèmes.

Le nombre des systèmes que contient le premier hypersystème est égal à $2 \cdot 2 = 4$. Désignons-les par $S_{0,0}$, $S_{0,1}$, $S_{1,0}$, $S_{1,1}$: Δ'' se compose de la substitution 1, jointe à une autre substitution qui permute $S_{0,0}$ et $S_{0,1}$, sans déplacer les deux autres systèmes ; Δ' se compose de la substitution 1, jointe à une autre substitution qui remplace $S_{0,0}$ et $S_{0,1}$ par $S_{1,0}$ et $S_{1,1}$, et réciproquement. Ces substitutions, combinées entre elles, forment un groupe qui contient évidemment huit substitutions distinctes, toutes comprises parmi les vingt-quatre substitutions que l'on obtient en permutant de toutes les manières possibles les quatre systèmes ci-dessus. Ces dernières substitutions forment un groupe k résoluble (car on sait que l'équation générale du quatrième degré est résoluble), et plus général que (Δ', Δ''). Cela posé, le groupe dérivé de Δ, k, Δ''',... est évidemment résoluble, et plus général que G.

THÉORÈME II. — *Soit* G *un groupe résoluble, correspondant à une*

décomposition $m = p^{n} p'^{n'} p''^{n''} \ldots$ *et formé de groupes partiels* $\Delta, \Delta', \Delta'', \ldots$. *En réunissant, dans un premier système, d'abord toutes les lettres que déplace le groupe partiel* $(\Delta', \Delta'', \ldots)$, *puis celles-là seulement que déplace* $(\Delta'' \ldots)$, *etc., on obtient évidemment une suite de groupements des lettres en* p^{n} *hypersystèmes* H, $H_1, \ldots$, *contenant* $p'^{n'} p''^{n''} \ldots$ *lettres, puis en* $p^{n} p'^{n'}$ *systèmes ne contenant plus que* $p''^{n''} \ldots$ *lettres, etc. Mais il sera impossible de trouver aucun autre groupement des lettres en systèmes tels, que chaque substitution de* G *remplace les lettres d'un système par celles d'un même système.*

Supposons, en effet, un semblable groupement effectué. Soient $\Sigma, \Sigma', \ldots$ les nouveaux systèmes; admettons, pour fixer les idées, que toutes les lettres de Σ appartiennent au même hypersystème H, mais que deux d'entre elles, a et a_1, appartiennent à deux systèmes différents S et S_1. Les substitutions $(\Delta'' \ldots)$, n'altérant que le système S, ne déplacent pas a_1 : donc elles remplacent les lettres de Σ les unes par les autres, mais elles font succéder à a les diverses lettres de S; donc toutes les lettres de S font partie de Σ. De même, le groupe transformé de $(\Delta'' \ldots)$ par celle des substitutions Δ' qui remplace S par S_1 ne déplace pas a et fait succéder à a_1 les diverses lettres de S_1 : donc ces lettres font partie de Σ. De même, si Σ contient une lettre d'un autre système S_2, il les contiendra toutes. Σ contient toutes les lettres de H, car, s'il n'en était pas ainsi, H contiendrait un système S' dont les lettres ne feraient pas partie de Σ; mais Δ' contient une substitution qui remplace S par S', elle remplacerait les systèmes $S, S_1, S_2, \ldots$, qui forment Σ, par d'autres systèmes $S', S'_1, S'_2, \ldots$ dont la réunion formerait un des nouveaux systèmes, Σ'. De même, si S'' était un autre système contenu dans H, H contiendrait une nouvelle suite de systèmes $S'', S''_1, S''_2, \ldots$ constituant un des nouveaux systèmes, Σ'', etc. Chacune des substitutions Δ' devant remplacer les lettres de chacun des systèmes $\Sigma, \Sigma', \Sigma'', \ldots$, par les lettres d'un même système, remplacerait les systèmes de chacune des suites $S, S_1, S_2, \ldots, S', S'_1, S'_2, \ldots$, etc., par les systèmes d'une même suite : elles ne permuteraient donc pas ces systèmes primitivement, comme cela doit être.

Σ contenant ainsi toutes les lettres de H, et n'en contenant, par hypothèse, aucune autre, se confond avec H; et les autres systèmes Σ', etc.,

se confondront avec H,..., etc., que les Δ font succéder à H. On se trouve ainsi retomber sur un des anciens groupements.

THÉORÈME III. — *Un groupe résoluble non primitif* G, *formé par notre méthode entre* p^n *lettres* (p *étant premier*), *ne peut être contenu dans un groupe primitif* (*sauf le cas où* $p=2$, $n=2$).

En effet, soient p^α le nombre des systèmes de G, choisis de manière à contenir chacun le moins possible de lettres; $p^{n-\alpha}$ le nombre de lettres de chacun d'eux.

Soient ε, u, u',..., $u^{n-\alpha-1}$ les indices variables, le premier de o à $p^\alpha - 1$, les autres de o à $p-1$, qui servent à caractériser les diverses lettres. Le groupe G contient un groupe partiel Γ dont les substitutions déplacent les lettres du premier système, en laissant les autres immobiles : chacune d'elles déplacera donc au maximum $p^{n-\alpha}$ lettres. On doit même remarquer que Γ contient, outre les substitutions

$$\begin{vmatrix} o & o \\ u & u+\beta \\ u' & u'+\beta' \\ \cdots & \cdots \end{vmatrix},$$

qui forment un premier faisceau, d'autres substitutions autres que l'unité et de la forme linéaire

$$\begin{vmatrix} o & o \\ u & au+bu'\ldots \\ u' & a'u+b'u'\ldots \\ \cdots & \cdots \end{vmatrix};$$

ces dernières substitutions, laissant immobile la lettre dont les indices sont o, o, o,..., déplaceront moins de $p^{n-\alpha}$ lettres. Cette remarque ne se trouverait en défaut que si l'on avait à la fois $p=2$ et $n-\alpha=1$, cas où il n'existerait qu'une seule substitution linéaire

$$\begin{vmatrix} o & o \\ u & u \end{vmatrix}$$

se réduisant à l'unité.

D'autre part, soit $\mathcal{G}$ un groupe résoluble primitif : les lettres étant caractérisées par n indices, $x, y, \ldots$, ses substitutions seront de la forme

$$\begin{vmatrix} x & cx + dy + \ldots + \gamma \\ y & c'x + d'y + \ldots + \delta \\ \ldots & \ldots\ldots\ldots \end{vmatrix}.$$

Pour qu'une substitution S de cette forme laisse immobile la lettre dont les indices sont $x, y, \ldots$, il faut qu'on ait à la fois

$$\left.\begin{array}{llll} x \equiv cx + dy + \ldots + \gamma, & \text{d'où} & (c-1)x + dy + \ldots + \gamma \equiv 0 \\ y \equiv c'x + d'y + \ldots + \delta, & \text{d'où} & c'x + (d'-1)y + \ldots + \delta \equiv 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & & \end{array}\right\} (\text{mod. } p)$$

Ces congruences se réduisent à des identités si $c = 1$, $d = 0$, $\gamma = 0$, $c' = 0, \ldots$, auquel cas S se réduit à l'unité. Dans le cas contraire, l'une au moins de ces relations ne sera pas identique : supposons, par exemple, que la première ne le soit pas : si elle se réduit à $\gamma \equiv 0 \,(\text{mod. } p)$, elle devient impossible à satisfaire : donc S déplace toutes les lettres : dans le cas contraire, l'un des coefficients des variables, $c - 1$ par exemple, sera $\gtrless 0 \,(\text{mod. } p)$. On pourra alors prendre arbitrairement $y, \ldots$, et pour chaque système de valeurs de ces indices, dont le nombre est p^{n-1}, l'indice x sera déterminé par la relation

$$(c-1)x + dy + \ldots + \gamma \equiv 0 \,(\text{mod. } p).$$

On a donc p^{n-1} lettres seulement satisfaisant à cette dernière relation, et par suite p^{n-1} lettres au plus restant immobiles : donc $p^n - p^{n-1}$ lettres au moins sont déplacées.

Mais si $\mathcal{G}$ contenait G, l'une de ses substitutions déplacerait moins de $p^{n-\alpha}$ lettres (ou $p^{n-\alpha}$ lettres, si $p^{n-\alpha} = 2$) : d'où l'inégalité impossible

$$p^{n-\alpha} > p^n - p^{n-1} > p^{n-1}(p-1).$$

Si $p^{n-\alpha}$ se réduit à 2, on aurait à la place de cette inégalité l'égalité

$$2 = p^{n-\alpha} = p^n - p^{n-1} = p^{n-1}(p-1), \quad \text{d'où} \quad p^{n-1} = 2 \quad \text{et} \quad p^n = 4.$$

C'est le cas d'exception déjà trouvé.

THÉORÈME IV. — *Deux groupes* G, G_1, *construits d'après notre méthode, ne peuvent être contenus l'un dans l'autre si les deux décompositions du nombre m,* $p^n p'^{n'} p''^{n''}, \ldots$ *et* $\pi^\nu \pi'^{\nu'} \pi''^{\nu''} \ldots$ *auxquelles ils correspondent respectivement, ne sont pas identiques. (On suppose que dans aucune des deux décompositions on n'a deux facteurs successifs égaux à* 2.)

En effet, les lettres peuvent être groupées dans G_1 en π^ν systèmes contenant chacun $\pi'^{\nu'} \pi''^{\nu''} \ldots$ lettres, et tels, que chaque substitution de G_1 remplace les lettres d'un système par celles d'un même système : si G est contenu dans G_1, ses substitutions jouiront *à fortiori* de la même propriété : mais nous avons vu (théorème II) que les lettres de G ne peuvent être groupées en π^ν systèmes que si π^ν est égal à l'un des nombres p^n, $p^n p'^{n'}, \ldots$.

Soit, pour fixer les idées,

$$\pi^\nu = p^n p'^{n'}.$$

Le groupe G résulte de la combinaison de deux autres : l'un $(\Delta'' \ldots)$ déplaçant les lettres du premier système seulement, l'autre (Δ, Δ') déplaçant les systèmes d'un mouvement d'ensemble. De même G_1 résultera de deux groupes, dont l'un $(\Delta'_1, \Delta''_1, \ldots)$ déplace les lettres du premier système seulement, l'autre Δ_1 déplaçant les systèmes d'un mouvement d'ensemble. G étant contenu dans G_1, il est clair que $(\Delta'' \ldots)$ et (Δ, Δ') devraient être respectivement contenus dans $(\Delta'_1, \Delta''_1, \ldots)$ et Δ_1. Cela est impossible : car (Δ, Δ'), étant non primitif, ne peut être contenu dans Δ_1, qui est primitif (théor. III).

On voit donc qu'on aura nécessairement

$$\pi^\nu = p^n, \quad \text{d'où} \quad \pi'^{\nu'} \pi''^{\nu''} \ldots = p'^{n'} p''^{n''}, \ldots :$$

et, que pour que G soit contenu dans G_1, il sera nécessaire et suffisant que Δ soit contenu dans Δ_1 et $(\Delta', \Delta'' \ldots)$ dans $(\Delta'_1, \Delta''_1, \ldots)$. Mais notre construction suppose que Δ est un groupe primitif aussi général que possible : donc Δ étant contenu dans Δ_1 se confond avec lui. On verra de même que pour que $(\Delta', \Delta'', \ldots)$ soit contenu dans $(\Delta'_1, \Delta''_1, \ldots)$, il faut que $p'^{n'} = \pi'^{\nu'}$, et que $\Delta', (\Delta'' \ldots)$ soient respectivement contenus dans Δ'_1, $(\Delta''_1 \ldots), \ldots$. Le théorème se trouve ainsi démontré.

Les résultats obtenus dans ce chapitre peuvent donc se résumer ainsi qu'il suit :

THÉORÈME. — *Les décompositions* $m = p^n p'^{n'} \ldots$, *dans lesquelles deux facteurs successifs sont à la fois égaux à* 2, *ne fournissent aucun groupe général.*

Ces décompositions étant exclues, il existera autant de classes distinctes d'équations irréductibles et solubles par radicaux du degré m *qu'il reste d'autres décompositions.*

Le nombre des types distincts d'équations irréductibles et solubles par radicaux de la classe correspondante à la décomposition $m = p^n p'^{n'} \ldots$ *est égal à* $qq' \ldots$, q, $q', \ldots$, *désignant respectivement les nombres de types distincts de groupes résolubles et primitifs pour les degrés* p^n, $p'^{n'} \ldots$.