ANNALES SCIENTIFIQUES DE L'É.N.S.

ERNEST VESSIOT

Sur une théorie nouvelle de la réductibilité des équations algébriques

Annales scientifiques de l'É.N.S. 3^e série, tome 58 (1941), p. 1-36

<http://www.numdam.org/item?id=ASENS_1941_3_58__1_0>

ANNALES
SCIENTIFIQUES
DE
L'ÉCOLE NORMALE SUPÉRIEURE

SUR UNE

THÉORIE NOUVELLE DE LA RÉDUCTIBILITÉ

DES

ÉQUATIONS ALGÉBRIQUES

PAR M. ERNEST VESSIOT.

Introduction.

1. Je montre, dans ce travail, comment l'on est conduit à une théorie nouvelle de la réductibilité des équations algébriques par la considération des transformations rationnelles qui laissent ces équations invariantes.

Pour les équations de degré n, à racines simples,

$$(\mathcal{F}) \qquad 0 = F(x) = x^n + p_1 x^{n-1} + p_2 x^{n-2} + \ldots + p_{n-1} x + p_n,$$

il suffit d'introduire les transformations entières de degré $(n-1)$

$$(\mathcal{E}) \qquad y = \theta(x) = t_1 x^{n-1} + t_2 x^{n-2} + \ldots + t_{n-1} x + t_n,$$

que j'appelle, pour abréger, *canoniques*. Car, de toute transformation rationnelle

$$(\mathcal{R}) \qquad y = R(x) = \frac{a_1 x^p + a_2 x^{p-1} + \ldots + a_p}{b_1 x^q + b_2 x^{q-1} + \ldots + b_q},$$

on peut déduire, par des calculs rationnels, une transformation canonique qui change les racines d'une équation $\mathfrak{F}$ donnée, comme le fait cette transformation $\mathfrak{R}$.

Par ailleurs, l'introduction des transformations $\mathfrak{T}$ dans l'étude des équations $\mathfrak{F}$ se justifie, *a priori*, par le fait que ces équations $\mathfrak{F}$ forment une *classe*, vis-à-vis de la famille des transformations $\mathfrak{T}$.

D'une manière précise, il y a $n!$ transformations $\mathfrak{T}$ qui changent une équation $\mathfrak{F}$ donnée en une même autre. Il y en a donc aussi $n!$ qui laissent cette équation invariante.

Ces *auto-transformations canoniques* de $\mathfrak{F}$ ne forment pas un groupe, mais elles forment (*mod.* $\mathfrak{F}$), un *pseudo-groupe*, que j'appelle le *pseudo-groupe d'invariance* de $\mathfrak{F}$. Voici ce que j'entends par ce terme de *pseudo-groupe*.

Soient $\mathfrak{T}_1$ et $\mathfrak{T}_2$ deux quelconques des transformations $\mathfrak{T}$, et $y=\theta_1(x)$, $y=\theta_2(x)$ leurs équations. Si $\theta_3(x)$ est le reste de la division de $\theta_2[\theta_1(x)]$ par $F(x)$, $y=\theta_3(x)$ est une transformation $\mathfrak{T}$, soit $\mathfrak{T}_3$, qui transforme les racines de $\mathfrak{F}$ comme le fait la transformation produit $y=\theta_2[\theta_1(x)]$. Ce sera le *pseudo-produit* (*mod.* $\mathfrak{F}$) de $\mathfrak{T}_1$ par $\mathfrak{T}_2$. Si ce pseudo-produit est la transformation identique $y=x$ (qui est l'une des transformations $\mathfrak{T}$), $\mathfrak{T}_2$ sera dite *pseudo-inverse* de $\mathfrak{T}_1$ (*mod.* $\mathfrak{F}$).

Cela posé, tout ensemble de transformations $\mathfrak{T}$ auquel appartiendra le pseudo-produit (*mod.* $\mathfrak{F}$) de deux quelconques d'entre elles, et dont les transformations s'associeront en couples, dans lesquels chaque transformation du couple sera pseudo-inverse de l'autre (*mod.* $\mathfrak{F}$), sera dit un *pseudo-groupe* (*mod.* $\mathfrak{F}$).

2. Chaque auto-transformation de $\mathfrak{F}$ effectue sur ses racines, considérées comme des objets distincts, une certaine permutation ϖ. Le pseudo-groupe d'invariance de $\mathfrak{F}$ est ainsi en correspondance, holoédriquement isomorphique, avec le groupe des permutations de n objets. On passe, par suite, d'une solution quelconque du système en $(x_1, \ldots, x_n)$

$$(P) \qquad \Sigma x_\alpha = -p_1, \qquad \Sigma x_\alpha x_\beta = p_2, \qquad \ldots, \qquad x_1 x_2 \ldots x_n = (-1)^n p_n,$$

associé à $\mathfrak{F}$, à toute autre par une auto-transformation de $\mathfrak{F}$ et une

seule, étant entendu que chaque x_i est transformé comme x en cogrédience, par les diverses transformations canoniques $\mathfrak{C}$.

Si donc $x' = \Theta(x)$ est l'une quelconque des auto-transformations de $\mathfrak{F}$, les diverses transformations

$$x'_i = \Theta(x_i) \qquad (i = 1, 2, \ldots, n) \tag{1}$$

constituent pour P un *pseudo-groupe d'invariance* $\mathfrak{I}$. On sait, par ailleurs, que P est un *système automorphe* (1) et que son *groupe d'automorphie* se compose des diverses transformations

$$x'_i = x_{\rho_i} \qquad (i = 1, 2, \ldots, n), \tag{2}$$

$\rho_1, \ldots, \rho_n$ étant l'une quelconque des permutations des indices 1, 2, ..., n. Comme ce groupe d'automorphie $\mathfrak{A}$, le pseudo-groupe d'invariance $\mathfrak{I}$ échange les solutions de P suivant un mode *simplement transitif*. Considérés ensemble, $\mathfrak{A}$ et $\mathfrak{I}$ présentent cette propriété que chaque transformation de l'un est *permutable* avec chaque transformation de l'autre.

3. Vis-à-vis d'un *domaine de rationalité* donné Δ, une équation $\mathfrak{F}$ donnée, appartenant à ce domaine, est *générale*, ou *spéciale*, selon que le système P qui lui est *associé* est *irréductible*, ou *réductible* (respectivement), au sens général donné à ces mots par M. Drach (2). Il nous sera commode de parler de la *réductibilité* de $\mathfrak{F}$, si elle est spéciale, comme signifiant la réductibilité de P, ainsi que nous l'avons fait dans le titre de ce travail et dans les premières lignes de la présente Introduction.

---

(1) Étant donné un système S d'équations, finies ou différentielles, à n inconnues, je dis qu'il est *automorphe* s'il existe un groupe G de transformations de l'espace à n dimensions, pouvant se définir indépendamment de S, tel que toutes les solutions de S se déduisent de l'une quelconque d'entre elles par les diverses transformations de G, effectuées sur les inconnues; et je dis alors que G est *groupe d'automorphie* de S.

(2) Un système S, rationnel dans Δ, est dit *réductible* dans Δ si l'on peut lui adjoindre une équation, rationnelle dans Δ, qui ne soit pas une conséquence de S, et telle que le nouveau système ainsi obtenu soit compatible. Si S n'est pas réductible, il est dit *irréductible*.

Dire que P est réductible dans Δ équivaut à dire que l'un au moins de ses *sous-systèmes* (1) est rationnel dans Δ. Je me suis donc proposé de préciser le *mode de réductibilité* (au sens large que je viens d'indiquer) propre à chaque équation $\mathcal{F}$ spéciale donnée, en caractérisant, par une propriété commune relative à ses auto-transformations, l'ensemble des sous-systèmes de son système associé P qui se trouvent être rationnels dans Δ. J'ai trouvé que ce sont tous ceux qui admettent les auto-transformations de $\mathcal{F}$ constituant un certain pseudo-groupe (*mod.* $\mathcal{F}$). Ce pseudo-groupe définissant ainsi la manière particulière dont l'équation $\mathcal{F}$ considérée est spéciale, je l'appelle le *pseudo-groupe spécifique* de $\mathcal{F}$.

Les solutions de P se répartissent en *familles de solutions conjuguées*, deux solutions étant dites *conjuguées* si l'on passe de l'une des deux à l'autre par une transformation du pseudo-groupe spécifique K de $\mathcal{F}$; et les solutions de l'une quelconque de ces familles constituent l'ensemble des solutions d'un sous-système rationnel de P, irréductible dans Δ, que j'appelle *spécifique*, parce qu'il a ce pseudo-groupe spécifique K pour pseudo-groupe d'invariance. Ces sous-systèmes spécifiques sont, par ailleurs, automorphes et ont pour groupes d'automorphie des sous-groupes du groupe d'automorphie $\mathfrak{A}$ de P, homologues entre eux.

Chaque solution demeure inséparable de ses conjuguées tant qu'on n'emploie, pour la déterminer, que des équations rationnelles dans Δ.

4. *Le groupe de Galois* de $\mathcal{F}$, dont on retrouve facilement, par cette voie, la notion et les propriétés fondamentales, n'est pas autre chose que le groupe des permutations ϖ (des racines de $\mathcal{F}$) produites par les diverses transformations de son pseudo-groupe spécifique K. Il se présente ainsi comme un groupe concret, entièrement défini, indépendamment de sa représentation par des groupes de substitutions

(1) J'appelle *sous-système* d'un système S quelconque d'équations, finies ou différentielles, un système S', aux mêmes inconnues que S, dont toute solution est une solution de S, mais qui n'admet pas toutes les solutions de S. On ne considère ici que des sous-systèmes rationnels en $x_1, \ldots, x_n$.

homologues entre eux : ce qui me paraît conforme à la conception originale de Galois (1).

1. Sur la transformation des équations algébriques.

Soit $\mathcal{F}$ une équation algébrique en x, de degré n,

$$(1) \qquad 0 = F(x) = x^n + p_1 x^{n-1} + p_2 x^{n-2} + \ldots + p_{n-1} x + p_n,$$

dont les racines $\xi_1, \ldots, \xi_n$ seront supposées inégales. Appliquons-lui une transformation rationnelle $\mathcal{R}$ quelconque,

$$(2) \qquad y = R(x) = \frac{A(x)}{B(x)} = \frac{a_0 + a_1 x + \ldots + a_p x^p}{b_0 + b_1 x + \ldots + b_q x^q},$$

le dénominateur B étant supposé premier avec F. Cela se fera, par définition, en éliminant x entre les équations (1) et (2), ce qui donnera pour transformée de $\mathcal{F}$, d'après la théorie classique de la transformation des équations algébriques, l'équation $\mathcal{G}$ en y,

$$(3) \qquad 0 = G(y) = y^n + q_1 y^{n-1} + q_2 y^{n-2} + \ldots + q_{n-1} y + q_n,$$

qui a pour racines $\eta_1, \ldots, \eta_n$ les transformées

$$(4) \qquad \eta_i = R(\xi_i) \qquad (i = 1, 2, \ldots, n)$$

des racines $\xi_1, \ldots, \xi_n$ de $\mathcal{F}$.

Soit alors P le système en $x_1, \ldots, x_n$

$$(5) \qquad \Sigma x_\alpha = -p_1, \qquad \Sigma x_\alpha x_\beta = p_2, \qquad \ldots, \qquad x_1 x_2 \ldots x_n = (-1)^n p_n,$$

que nous dirons *associé* à $\mathcal{F}$, et soit, de même, Q le système en $y_1, \ldots, y_n$,

$$(6) \qquad \Sigma y_\alpha = -q_1, \qquad \Sigma y_\alpha y_\beta = q_2, \qquad \ldots, \qquad y_1 y_2 \ldots y_n = (-1)^n q_n,$$

associé à $\mathcal{G}$.

---

(1) Les résultats de ce Mémoire ont été résumés dans une Note des *Comptes rendus de l'Académie des Sciences*, portant le même titre (Séance du 29 janvier 1940, 210, p. 159).

Appliquons à P la transformation $\mathcal{R}$, c'est-à-dire, plus explicitement, la transformation $\overline{\mathcal{R}}$

$$y_i = \mathrm{R}(x_i) \qquad (i = 1, 2, \ldots, n), \tag{7}$$

qui opère, par cogrédience, sur chacune des variables x_i, comme $\mathcal{R}$ opère sur x.

Nous aurons à éliminer les x_i entre les équations (5) et (7), c'est-à-dire à exprimer que $(y_1, \ldots, y_n)$ résulte de la transformation par $\mathcal{R}$ d'une solution $(x_1, \ldots, x_n)$ de P. Or, les diverses solutions de P sont données par les formules

$$x_i = \xi_{\rho_i} \qquad (i = 1, 2, \ldots, n), \tag{8}$$

$\rho_1, \ldots, \rho_n$ étant l'une quelconque des permutations des indices 1, 2, ..., n; de sorte que leurs transformées respectives sont données, avec les mêmes ρ_i, par les formules

$$y_i = \mathrm{R}(\xi_{\rho_i}) = \eta_{\rho_i} \qquad (i = 1, 2, \ldots, n), \tag{9}$$

et sont, par conséquent, les diverses solutions de Q. Le résultat de l'élimination en question devra, par suite, exprimer que $(y_1, \ldots, y_n)$ est une solution de $\mathcal{R}$, et sera, dès lors, le système Q lui-même.

Nous concluons donc que, $\mathcal{F}$ et $\mathcal{G}$ étant deux équations algébriques quelconques de degré n, sans racines multiples, et P et Q étant leurs systèmes associés respectifs, toute transformation rationnelle qui change $\mathcal{F}$ en $\mathcal{G}$, change aussi P en Q.

2. Transformations canoniques.

Le but de ce travail est d'utiliser systématiquement les transformations rationnelles $\mathcal{R}$ pour l'étude des équations algébriques de degré n, à racines simples, et, en particulier, pour l'analyse de leur réductibilité. Il suffira, en fait, d'y employer les transformations entières de degré $(n-1)$,

$$y = \mathrm{E}(x) = e_1 + e_2 x + \ldots + e_n x^{n-1}, \tag{10}$$

que nous appellerons, pour un degré n donné, *canoniques*. On sait, en

effet, qu'étant données une transformation rationnelle quelconque $\mathcal{R}$ et une équation algébrique $\mathcal{F}$ de degré n, à racines simples, il existe une transformation entière et de degré $(n-1)$, $\mathcal{E}$, et une seule, que l'on pourra appeler *réduite* de $\mathcal{R}$ par rapport à $\mathcal{F}$, qui donne aux racines de $\mathcal{F}$ les mêmes transformées que $\mathcal{R}$; et que cette réduite peut s'obtenir par des calculs rationnels.

Elle est donnée, par exemple, avec les notations du n° 1, par la formule d'interpolation de Lagrange (1)

$$y = \mathrm{R}(\xi_\alpha)\Phi(x, \xi_\alpha) \qquad (\alpha = 1, 2, \ldots, n), \tag{11}$$

$\Phi(x, a)$ étant le quotient

$$\Phi(x, a) = \frac{\mathrm{F}(x) - \mathrm{F}(a)}{(x-a)\mathrm{F}'(a)}. \tag{12}$$

Le second membre de (11), étant une fonction symétrique des ξ_i, pourra s'exprimer rationnellement en fonction des coefficients de $\mathcal{F}$ et de $\mathcal{R}$.

Sous leur forme générale (10), les transformations canoniques relatives à la famille N des équations algébriques de degré n, à racines simples, dépendent de n paramètres arbitraires $e_1, \ldots, e_n$. Quand il s'agira d'étudier les transformées d'une équation particulière $\mathcal{F}$ de cette famille N, on pourra les prendre sous la forme

$$y = \eta_\alpha \Phi(x, \xi_\alpha) \qquad (\alpha = 1, 2, \ldots, n), \tag{13}$$

qui met en évidence les transformées

$$\eta_i = \mathrm{E}(\xi_i) \qquad (i = 1, 2, \ldots, n), \tag{14}$$

des racines ξ_i de $\mathcal{F}$. Et ces transformées $\eta_1, \ldots, \eta_n$ y seront alors des paramètres arbitraires. On passera des paramètres e_i aux paramètres η_i et inversement, par la transformation linéaire (14) et par son inverse.

La transformée de $\mathcal{F}$ par l'une quelconque de ces transformations (13) sera l'équation $\mathcal{G}$ qui a pour racines $\eta_1, \ldots, \eta_n$. On pourra

---

(1) La notation $a_\alpha b_\alpha (\alpha = 1, 2, \ldots, n)$ désigne la somme $\sum_{\alpha=1}^{n} a_\alpha b_\alpha$.

donc passer, par une transformation canonique, de toute équation $\mathcal{F}$ de la famille, à toute équation $\mathcal{G}$ de la famille.

On peut donc dire que la famille N des équations de degré n à racines simples est une *classe*, vis-à-vis des transformations canoniques relatives au degré n; mais il faut observer que celles-ci ne forment pas un groupe, tant parce qu'elles ne sont pas inverses deux à deux que parce que le produit de deux d'entre elles est une transformation entière dont le degré est, en général, supérieur à $(n-1)$.

Les transformations canoniques qui font passer d'une même équation $\mathcal{F}$ à une même équation $\mathcal{G}$, dans la classe N, sont au nombre de $n!$ Car, pour que la transformation

$$y = \zeta_\alpha \Phi(x, \xi_\alpha) \qquad (\alpha = 1, 2, \ldots, n), \tag{15}$$

du type (13), change l'équation $\mathcal{F}$, qui a pour racines $\xi_1, \ldots, \xi_n$, en une équation $\mathcal{G}$ donnée, il faut et il suffit que $\zeta_1, \ldots, \zeta_n$ soient les racines de celle-ci, prises dans un ordre quelconque : c'est-à-dire, si l'on a désigné par $\eta_1, \ldots, \eta_n$ les racines de $\mathcal{G}$, prises dans un ordre déterminé, arbitraire du reste, que l'on ait

$$\zeta_i = \eta_{\rho_i} \qquad (i = 1, 2, \ldots, n), \tag{16}$$

$\rho_1, \ldots, \rho_n$ étant l'une quelconque des permutations des indices 1, 2, ..., n.

La forme générale des transformations canoniques qui changent $\mathcal{F}$, de racines $\xi_1, \ldots, \xi_n$, en $\mathcal{G}$, de racines $\eta_1, \ldots, \eta_n$, est donc

$$y = \eta_{\rho_\alpha} \Phi(x, \xi_\alpha) \qquad (\alpha = 1, 2, \ldots, n), \tag{17}$$

$\rho_1, \ldots, \rho_n$ étant l'une quelconque des permutations des indices 1, 2, ..., n. Les $n!$ transformations ainsi définies diffèrent par la manière dont elles transforment le système des n racines de $\mathcal{F}$; et sont, par suite et *a fortiori*, analytiquement différentes.

3. Auto-transformations et pseudo-groupe d'invariance.

En appliquant les résultats qui précèdent au cas où $\mathcal{G}$ est identique à $\mathcal{F}$, on conclut qu'il y a $n!$ transformations canoniques différentes, et pas davantage, qui laissent invariante une équation donnée $\mathcal{F}$, de

degré n; et que, si $\xi_1, \ldots, \xi_n$ désignent les racines de cette équation, prises dans un ordre déterminé, arbitrairement choisi, leur équation générale est

$$y = \xi_{\rho_\alpha} \Phi(x, \xi_\alpha) \qquad (\alpha = 1, 2, \ldots, n), \tag{18}$$

$\rho_1, \ldots, \rho_n$ étant l'une quelconque des permutations des indices 1, 2, ..., n. Nous les appellerons les *auto-transformations* canoniques de $\mathcal{F}$.

Prises sous la forme générale (10), elles seraient fournies par les diverses solutions (au nombre de $n!$, d'après ce qui vient d'être dit), du système $\mathcal{D}$ d'équations en $e_1, \ldots, e_n$, qui exprime que la transformation (10) laisse $\mathcal{F}$ invariante : système que l'on appellera le système des *équations de définition* de ces auto-transformations.

Soient Θ une quelconque des auto-transformations canoniques de $\mathcal{F}$, $e_i = t_i$ $(i = 1, 2, \ldots, n)$, la solution du système $\mathcal{D}$ qui la donne, et

$$y = \theta(x) = t_1 + t_2 x + \ldots + t_n x^{n-1} \tag{19}$$

son équation. Laissant $\mathcal{F}$ invariante, elle change chaque racine de $\mathcal{F}$ en une racine de $\mathcal{F}$ et change l'ensemble des racines de $\mathcal{F}$ en lui-même : elle produit donc sur le système des racines de $\mathcal{F}$, considérées comme des objets différents, une certaine permutation ϖ, que nous dirons *induite* par elle.

Or, si l'on a désigné les racines de $\mathcal{F}$, prises dans un ordre déterminé arbitraire, par $\xi_1, \ldots, \xi_n$, cette auto-transformation Θ aura, pour un choix approprié des ρ_i, une équation de la forme (18), et la permutation concrète ϖ se traduira par la substitution abstraite σ qui change chaque indice i en ρ_i. Il en résulte qu'il y a correspondance biunivoque entre les auto-transformations canoniques Θ et les permutations concrètes ϖ qu'elles induisent, celles-ci étant, dans leur ensemble, toutes les $n!$ permutations des racines.

De plus, si ϖ_1 et ϖ_2 sont les permutations concrètes des racines induites, respectivement, par deux auto-transformations canoniques quelconques, $y = \theta_1(x)$ et $y = \theta_2(x)$, le produit $\varpi_1 \varpi_2 = \varpi_3$ sera induit par le produit $y = \theta_1[\theta_2(x)]$, et, par conséquent, par la

réduite $y = \theta_3(x)$ de ce produit (1), et cette réduite laissant, comme ce produit, $\mathcal{F}$ invariante, sera l'une des auto-transformations canoniques de $\mathcal{F}$.

Il est évident, par ailleurs, que la transformation identique $y = x$ est l'une des auto-transformations canoniques de $\mathcal{F}$, et a pour induite la permutation unité.

Enfin, comme à chaque permutation concrète ϖ en correspond une autre, ϖ_0, qui est son inverse, à chaque auto-transformation canonique $y = \theta(x)$ en correspondra une autre $y = \theta_0(x)$ qui aura pour induite la permutation ϖ_0, inverse de la permutation ϖ induite par la première; et la réduite du produit $y = \theta[\theta_0(x)]$, comme celle du produit $y = \theta_0[\theta(x)]$, ayant pour induite la permutation unité, sera la transformation identique $y = x$.

Les permutations concrètes ϖ forment un groupe Π, qui est le groupe général de toutes les permutations concrètes des racines de $\mathcal{F}$.

Les auto-transformations canoniques Θ, au contraire, pour les raisons données ci-dessus (n° 2) pour les transformations canoniques, ne forment pas un groupe. Mais, d'après l'analyse qui précède, elles se comportent comme si elles en formaient un, en ce qui concerne leurs effets sur les racines de $\mathcal{F}$, qui se traduisent par les permutations ϖ qu'elles induisent respectivement. Nous dirons, en conséquence, qu'elles forment, relativement à $\mathcal{F}$, un *pseudo-groupe*, et nous appellerons celui-ci le *pseudo-groupe d'invariance* de $\mathcal{F}$. La réduite du produit de deux transformations de ce pseudo-groupe (prise relativement à $\mathcal{F}$) sera dite leur *pseudo-produit;* et deux de ces transformations dont le pseudo-produit sera la transformation identique seront dites *pseudo-inverses* l'une de l'autre.

De sorte que ce *pseudo-groupe* contiendra la transformation identique, que le *pseudo-produit* de deux quelconques de ses transformations sera une de ses transformations, et que ses transformations seront, deux à deux, *pseudo-inverses* l'une de l'autre. Ainsi apparaissent, pour l'ensemble des auto-transformations canoniques d'une

---

(1) $\theta_3(x)$ est le reste de la division de $\theta_1[\theta_2(x)]$ par $F(x)$; ce qui revient à dire que l'on a

$$\theta_3(x) \equiv \theta_1[\theta_2(x)] \quad mod.\ F(x).$$

équation $\mathcal{F}$, $F(x)=0$, quand le calcul de ces transformations est traité *modulo* F, les propriétés caractéristiques des groupes.

Quant aux $n!$ substitutions σ, elles constituent le groupe général $\mathcal{S}$ des substitutions des indices $1, 2, \ldots, n$; et la manière dont elles ont été introduites établit une correspondance holoédriquement isomorphique entre ce groupe $\mathcal{S}$ d'une part, et le pseudo-groupe d'invariance $\mathcal{J}$, ou le groupe de permutations H d'autre part. Il faut entendre par là, en ce qui concerne $\mathcal{S}$ et $\mathcal{J}$, qu'au produit de deux substitutions de $\mathcal{S}$ correspond le pseudo-produit des deux transformations de $\mathcal{J}$ qui leur sont respectivement homologues.

Le groupe $\mathcal{S}$ donne ainsi une représentation du pseudo-groupe d'invariance $\mathcal{J}$; mais cette représentation change si l'on modifie le numérotage des racines de $\mathcal{F}$: chacune des substitutions σ se trouve alors remplacée par sa transformée par une certaine substitution des indices $1, 2, \ldots, n$, la même pour toutes.

4. Pseudo-groupe d'invariance du système associé.

L'introduction des auto-transformations canoniques permet de considérer toute équation algébrique $\mathcal{F}$ comme *automorphe* (1), ou mieux comme *pseudo-automorphe*, puisque ses diverses auto-transformations canoniques, qui forment le *pseudo-groupe* d'invariance $\mathcal{J}$, font passer de chaque racine de $\mathcal{F}$ à toute autre (2). Mais c'est dans la manière dont ces auto-transformations se comportent vis-à-vis du système P *associé* à $\mathcal{F}$ que réside leur importance.

Il résulte d'abord du n° 1 que toute auto-transformation canonique Θ de $\mathcal{F}$, $y=\theta(x,)$ ou, plus explicitement, la transformation $\overline{\Theta}$,

$$(20) \qquad y_i=\theta(x_i) \qquad (i=1, 2, \ldots, n),$$

(1) On sait qu'un système d'équations, finies ou différentielles, est dit *automorphe* si ses diverses solutions se déduisent de l'une quelconque d'entre elles par les transformations d'un *groupe*, effectuées sur les inconnues; et que ce groupe est dit groupe d'*automorphie* du système.

(2) Il y a $(n-1)!$ auto-transformations canoniques de $\mathcal{F}$ qui changent une racine donnée en une autre racine donnée.

qui en résulte par cogrédience, laisse P invariant. Nous dirons donc de ces transformations $\overline{\Theta}$ que ce sont les *auto-transformations canoniques* de P.

Chacune d'elles, changeant toute solution de P en une solution de P, et changeant en lui-même l'ensemble des $n!$ solutions (8) de P, produit sur le système de ces $n!$ solutions, considérées comme des objets distincts, une permutation $\overline{\omega}$, que l'on dira induite par cette auto-transformation $\overline{\Theta}$.

Si l'on prend Θ sous la forme (18), $\overline{\Theta}$ sera

$$(21) \qquad y_i = \xi_{\rho_\alpha} \Phi(x_i, \xi_\alpha) \qquad (\alpha = 1, 2, \ldots, n;\ i = 1, 2, \ldots, n),$$

et elle changera la solution $x_i = \xi_i$ $(i = 1, 2, \ldots, n)$, qui a été, par hypothèse, arbitrairement choisie, en

$$(22) \qquad y_i = \xi_{\rho_i} \qquad (i = 1, 2, \ldots, n),$$

d'où il résulte qu'il y a une transformation $\overline{\Theta}$, et une seule, qui change une solution donnée de P en une autre solution de P donnée.

On sait que le système P, en vertu de la symétrie de ses équations, est *automorphe*, son *groupe d'automorphie* $\mathfrak{A}$ étant le groupe des $n!$ permutations des variables $x_1, \ldots, x_n$, qui sont représentées par les transformations Ω

$$(23) \qquad x'_i = x_{\sigma_i} \qquad (i = 1, 2, \ldots, n)$$

($\sigma_1, \ldots, \sigma_n$ étant les diverses permutations des indices $1, 2, \ldots, n$). La transformation générale (23) change la solution

$$x_i = \xi_i \qquad (i = 1, 2, \ldots, n)$$

en

$$(24) \qquad x'_i = \xi_{\sigma_i} \qquad (i = 1, 2, \ldots, n);$$

elle effectue donc une permutation de ces solutions, et l'on peut y choisir $\sigma_1, \ldots, \sigma_n$ de manière que cette permutation ω change la solution arbitraire $\xi_1, \ldots, \xi_n$, supposée donnée, en une solution quelconque $x_i = \xi_{\sigma_i}$ $(i = 1, 2, \ldots, n)$, également donnée à l'avance. Le groupe des permutations ω, qui est holoédriquement isomorphe au groupe $\mathfrak{S}$ des substitutions des n indices, est donc *simplement transitif*.

Il résulte de ce qui précède qu'il en est de même pour le groupe des permutations $\overline{\varpi}$, induites par les auto-transformations canoniques $\overline{\Theta}$ de P.

Ces auto-transformations ne forment pas un groupe, mais, comme les auto-transformations Θ de $\mathfrak{F}$, elles forment un *pseudo-groupe*, si l'on convient que le *pseudo-produit* de deux transformations $\overline{\Theta_1}$ et $\overline{\Theta_2}$,

$$(25) \qquad y_i = \theta_1(x_i), \qquad y_i = \theta_2(x_i) \qquad (i = 1, 2, \ldots, n),$$

sera

$$(26) \qquad y_i = \theta_3(x_i) \qquad (i = 1, 2, \ldots, n),$$

où $\theta_3(x)$ est le reste de la division de $\theta_1[\theta_2(x)]$ par $F(x)$: ce qui entraîne la définition de deux transformations *pseudo-inverses*.

Ce pseudo-groupe sera dit le *pseudo-groupe d'invariance* $\overline{\mathfrak{I}}$ de P (1). On voit qu'il joue, vis-à-vis de P, le rôle d'un second groupe d'automorphie.

Il convient d'observer cependant que les permutations concrètes $\overline{\varpi}$, induites par les transformations du pseudo-groupe $\overline{\mathfrak{I}}$, sont entièrement déterminées par elles; tandis que les permutations ω, résultant des transformations Ω du groupe d'automorphie $\mathfrak{A}$, ne le sont que lorsqu'on a numéroté les racines : ce qui peut se faire de $n!$ manières. En ce qui concerne le pseudo-groupe d'invariance $\overline{\mathfrak{I}}$, ce numérotage intervient seulement quand on veut donner à ses équations générales la forme explicite (21).

Il est bien remarquable, par ailleurs, que chaque transformation $\overline{\Theta}$ du pseudo-groupe d'invariance est *permutatable* à chaque transformation Ω du groupe d'automorphie. Il suffit, pour le vérifier, de chercher la transformée de la transformation (21) de $\overline{\mathfrak{I}}$ par la transformation (23) de $\mathfrak{A}$. Il vient, pour $i = 1, 2, \ldots, n$,

$$(27) \qquad y'_i = y_{\sigma_i} = \xi_{\rho_\alpha} \Phi(x_{\sigma_i}, \xi_\alpha) = \xi_{\rho_\alpha} \Phi(x'_i, \xi_\alpha) \qquad (\alpha = 1, 2, \ldots, n),$$

(1) Nous dirons aussi, de $\mathfrak{I}$ lui-même, qu'il est le *pseudo-groupe d'invariance* de P. Car appliquer à P, par cogrédience, une auto-transformation canonique θ de $\mathfrak{F}$, $y = \theta(x)$, c'est lui appliquer l'auto-transformation $\overline{\theta}$ de P, $y_i = \theta(x_i)$ $(i = 1, 2, \ldots, n)$, qui lui correspond. Et cela facilitera souvent le langage.

c'est-à-dire

$$(28) \qquad y'_i = \xi_{\rho_\alpha} \Phi(x'_i, \xi_\alpha) \qquad (\alpha = 1, 2, \ldots, n;\ i = 1, 2, \ldots, n),$$

ce qui est, écrite avec les x'_i, y'_i au lieu des x_i, y_i, la transformation (21) elle-même. Celle-ci est donc invariante par la transformation (23), ce qui prouve la permutabilité annoncée (1).

5. Des sous-systèmes du système associé.

J'appelle *sous-système* d'un système quelconque S d'équations, tout système Σ d'équations, aux mêmes inconnues, dont toute solution est une solution de S, mais qui n'admet pas toutes les solutions de S.

Considérons les sous-systèmes du système P, en $x_1, \ldots, x_n$, associé à une équation algébrique $\mathcal{F}$ quelconque de degré n (*voir* n° 1). Chacun d'eux s'obtiendra en adjoignant aux équations (5) de P une ou plusieurs *équations complémentaires*, en $x_1, \ldots, x_n$, compatibles avec P, sans en être des conséquences.

Je dis qu'on peut le faire de manière à avoir un sous-système Σ dont les solutions soient les divers éléments d'un ensemble E de solutions de P, arbitrairement donné.

Introduisons, en effet, une *résolvante de Galois* de $\mathcal{F}$. Soit

$$(29) \qquad V = m_1 x_1 + m_2 x_2 + \ldots + m_n x_n$$

l'inconnue auxiliaire choisie, et

$$(30) \qquad \varphi(V) = 0$$

---

(1) Par cette propriété de permutabilité, le pseudo-groupe d'invariance $\mathfrak{I}$ se présente, vis-à-vis du groupe d'automorphie $\mathfrak{A}$, comme l'analogue du groupe simplement transitif $\mathfrak{H}$ *réciproque* d'un groupe simplement transitif $\mathcal{G}$ donné, dans la théorie des groupes continus finis de S. Lie. C'est un premier exemple du parallélisme qui existe entre la présente théorie et celle que j'ai exposée, pour la réductibilité des systèmes différentiels automorphes dont les groupes d'automorphie sont des groupes continus simplement transitifs, dans un autre travail, qui doit paraître dans les *Annales Scientifiques de l'École Normale supérieure*. Si $\mathcal{G}$ est le groupe d'automorphie d'un tel système, son réciproque $\mathfrak{H}$ donne naissance à un *groupe d'invariance* K, qui joue le rôle d'un second groupe d'automorphie, et les transformations de $\mathcal{G}$ sont permutables à celles de K, comme à celles de $\mathfrak{H}$.

la résolvante, de degré égal à $n!$, dont elle dépend. Soient, de plus,

$$x_i = \varphi_i(V) \qquad (i = 1, 2, \ldots, n), \tag{31}$$

les formules rationnelles, donnant la solution $(x_1, \ldots, x_n)$ de P qui correspond à une racine quelconque V de cette résolvante. Aux éléments, solutions de P, de l'ensemble E donné correspondront autant de racines de (30), qui seront les diverses racines d'une certaine équation

$$\psi(V) = 0, \tag{32}$$

où $\psi(V)$ sera un diviseur de $\varphi(V)$. Cet ensemble sera donc défini par le système surabondant, obtenu en ajoutant aux équations (5) de P les équations (29), (30), (31), (32), où V est une inconnue auxiliaire. Et comme le système formé de P et de (29) équivaut au système formé de (30) et (31), on pourra ne garder que les équations (5) de P, avec (29) et (32); ou encore, adjoindre simplement à P l'équation (32) et l'équation

$$\psi(m_1 x_1 + \ldots + m_n x_n) = 0. \tag{33}$$

Mais (29) ne servira plus alors qu'à calculer l'inconnue auxiliaire V, et l'on pourra faire abstraction de celle-ci. De sorte qu'en définitive le système Σ annoncé s'obtiendra, sous une *forme type*, en adjoignant à P la seule équation complémentaire (33). On remarquera qu'elle est rationnelle en $x_1, \ldots, x_n$.

6. Les transformations réductrices et les sous-systèmes.

En même temps que l'équation $\mathcal{F}$, supposée donnée, qui pourra être quelconque, nous allons considérer une *équation de référence* fixe, de degré n, dont nous nous donnerons arbitrairement les racines. Prenons, par exemple, pour ces racines les entiers 1, 2, ..., n. Nous désignerons cette équation de référence par $\mathcal{G}$, et nous conserverons les notations des numéros précédents. Nous poserons, de plus,

$$\Psi(y, b) = \frac{G(y) - G(b)}{(y - b)G'(b)}. \tag{34}$$

Alors, la transformation canonique

$$y = \alpha\,\Phi(x, u_\alpha) \qquad (\alpha = 1, 2, \ldots, n) \tag{35}$$

changera $\mathcal{F}$ en $\mathcal{G}$, et la transformation canonique

$$x = u_\alpha\,\Psi(y, \alpha) \qquad (\alpha = 1, 2, \ldots, n) \tag{36}$$

changera $\mathcal{G}$ en $\mathcal{F}$, pouvu que $(u_1, \ldots, u_n)$ y soit une solution de P (1). Nous dirons, s'il en est ainsi, que (35) est une *transformation réductrice* de $\mathcal{F}$, et que (36) est sa *pseudo-inverse*.

D'après le n° 1, toute transformation réductrice (35) change P, système associé à $\mathcal{F}$, en Q, système associé à $\mathcal{G}$, et sa pseudo-inverse (36) change Q en P; mais, de plus, le mode de raisonnement employé alors permet de montrer, tout aussi aisément, que (35) change en même temps tout sous-système Σ de P en le sous-système Σ_0 de Q qui a pour solutions $(y_1, \ldots, y_n)$ les transformées, par (35), des solutions $(x_1, \ldots, x_n)$ de Σ; et que (36) change, inversement, Σ_0 en Σ.

Les divers systèmes Σ_0 qui se déduisent ainsi de Σ par les diverses transformations réductrices de $\mathcal{F}$ seront dits les *réduits* de Σ.

Observons que les transformations réductrices, considérées ici, ne sont pas autre chose que les transformations considérées n° 2, *in fine*, dans le cas où l'équation quelconque $\mathcal{G}$, envisagée alors, est l'équation de référence choisie ici.

Notons que (35) et (36) établissent une correspondance biunivoque entre les solutions $(x_1, \ldots, x_n)$ de P et les solutions $(y_1, \ldots, y_n)$ de Q (étant sous-entendu qu'on opère par cogrédience sur les x_i et les y_i); et que, en particulier, la solution $(u_1, \ldots, u_n)$ de P et la solution $(1, 2, \ldots, n)$ de Q sont homologues dans cette correspondance.

Cela posé, cherchons à quelle condition la transformation réductrice (35), qui a $(u_1, \ldots, u_n)$ pour solution *génératrice*, et une autre transformation réductrice

$$y = \alpha\,\Phi(x, u'_\alpha) \qquad (\alpha = 1, 2, \ldots, n), \tag{37}$$

---

(1) D'une manière plus précise (35) change chaque racine $x = u_i$ de $\mathcal{F}$ en la racine $y = i$ de $\mathcal{G}$, et (36) change inversement chaque racine $y = i$ de $\mathcal{G}$ en la racine $x = u_i$ de $\mathcal{F}$.

ayant pour solution génératrice $(u'_1, \ldots, u'_n)$, pourront transformer un sous-système Σ en un même réduit Σ_0.

Désignons, à cet effet, par T la transformation (35), par T_0 sa pseudo-inverse (36); par T' la transformation (37) et par T'_0 sa pseudo-inverse

$$x = u'_\alpha \Psi(y, \alpha) \qquad (\alpha = 1, 2, \ldots, n). \tag{38}$$

Σ_0 étant défini par $\Sigma_0 = T(\Sigma)$, on devra avoir $\Sigma_0 = T'(\Sigma)$, ce qui équivaut à $\Sigma = T'_0(\Sigma_0)$; de sorte que la condition cherchée est que l'on ait

$$\Sigma = T'_0[T(\Sigma)] = \widehat{T'_0 T}(\Sigma),$$

c'est-à-dire que le produit $T'_0 T$ laisse Σ invariant.

Or T changeant $\mathcal{F}$ en $\mathcal{G}$ et T'_0 changeant $\mathcal{G}$ en $\mathcal{F}$, $T'_0 T$ laisse $\mathcal{F}$ invariant; et comme c'est la transformation entière

$$x' = u'_\alpha \Psi[\beta \Phi(x, u_\beta), \alpha] \qquad (\alpha, \beta = 1, 2, \ldots, n), \tag{39}$$

sa réduite, relative à $\mathcal{F}$, est l'une des auto-transformations canoniques Θ de $\mathcal{F}$. Celle-ci permutant les solutions de P comme $T'_0 T$, la condition cherchée est donc qu'elle laisse Σ invariant.

Par ailleurs T changeant la solution $(u_1, \ldots, u_n)$ de P en la solution $(1, 2, \ldots, n)$ de Q, et T'_0 changeant la solution $(1, 2, \ldots, n)$ de Q en la solution $(u'_1, \ldots, u'_n)$, $T'_0 T$ change la solution $(u_1, \ldots, u_n)$ de P en sa solution $(u'_1, \ldots, u'_n)$; et, dès lors, la réduite Θ de $T'_0 T$ est celle des auto-transformations canoniques de $\mathcal{F}$ qui change la solution $(u_1, \ldots, u_n)$ de P en sa solution $(u'_1, \ldots, u'_n)$ (1).

Nous arrivons donc à la conclusion suivante :

Pour que deux transformations réductrices de $\mathcal{F}$ changent un sous-système Σ de P *en le même réduit Σ_0, il faut et il suffit que Σ demeure invariant par la transformation du pseudo-groupe d'invariance de $\mathcal{F}$ qui change la solution $(u_1, \ldots, u_n)$ de* P, *génératrice de l'une de ces transformations réductrices, en la solution $(u'_1, \ldots, u'_n)$ de* P *qui est la solution génératrice de l'autre.*

(1) On a montré au n° 4 qu'il y a une auto-transformation canonique de $\mathcal{F}$, et une seule, qui change une solution donnée de P en une autre solution de P, arbitrairement donnée comme la première.

7. Systèmes adjoints à un sous-système.

Les auto-transformations canoniques de $\mathfrak{T}$ qu'un sous-système Σ de P admet constituent un *pseudo-groupe;* car le pseudo-produit de deux d'entre elles en est une, elles sont deux à deux pseudo-inverses, et la transformation identique en est une. Nous dirons que ce pseudo-groupe γ est un *pseudo-sous-groupe* du pseudo-groupe d'invariance $\mathfrak{I}$ de $\mathfrak{T}$. Il pourra, du reste, se réduire à la seule transformation identique.

Cela dit, considérons l'ensemble des solutions $(u_1, \ldots, u_n)$ de P qui sont génératrices de transformations réductrices de $\mathfrak{T}$ changeant Σ en un même réduit Σ_0. Ce seront les solutions d'un certain sous-système σ de P, que nous dirons *adjoint* à Σ. Chaque solution de P est solution de l'un de ces adjoints σ de Σ, et d'un seul. Car elle est génératrice d'une transformation réductrice, laquelle donne à Σ un réduit Σ_0 et un seul. Donc *les solutions de* P *se répartissent entre les divers adjoints* σ *de* Σ.

D'après la conclusion du numéro précédent, les solutions de chacun des adjoints σ de Σ se déduisent de l'une quelconque d'entre elles par les diverses transformations d'un même pseudo-groupe γ, qui est le plus grand pseudo-sous-groupe du groupe d'invariance $\mathfrak{I}$ de P qui laisse Σ invariant.

Remarquons qu'il en résulte que si l'une des solutions d'un adjoint particulier σ de Σ est une solution de Σ, il en est de même de toutes les autres solutions de cet adjoint; puisque toute transformation de γ, laissant Σ invariant, change toute solution de Σ en une solution de Σ.

De là résulte que *les solutions de* Σ *se répartissent entre certains de ses adjoints.*

Remarque I. — Appelons *ordre* d'un sous-système Σ de P le nombre ν de ses solutions. *Tous les adjoints* σ *de* Σ *ont le même ordre* qui est l'*ordre* du pseudo-groupe γ, c'est-à-dire le nombre des transformations de celui-ci. Si donc μ est l'ordre de γ et m le nombre des adjoints entre lesquels se répartissent les solutions de Σ, on a $\nu = m\mu$. Donc *l'ordre de* γ *est un diviseur de l'ordre de* Σ.

Remarque II. — Si N est le nombre total des adjoints σ de Σ, les $n!$ solutions de P se répartissant entre ces adjoints, on a $n! = N\mu$,

de sorte que μ, ordre de γ, et N, nombre des adjoints σ, sont des diviseurs de $n!$ Comme $n!$ est l'ordre du pseudo-groupe $\mathfrak{I}$, on retrouve ici, pour les pseudo-sous-groupes de $\mathfrak{I}$, un théorème bien connu de la théorie des groupes d'ordre fini.

8. Propriétés des adjoints.

1° *Pseudo-groupe d'invariance.* — Comme on l'a vu au numéro précédent, le pseudo-groupe γ se comporte, vis-à-vis de chacun des adjoints σ considérés, comme le fait le pseudo-groupe $\mathfrak{I}$ (dont il est un pseudo-sous-groupe), vis-à-vis du système P : il en permute les solutions de telle manière qu'il y a une transformation et une seule de γ qui change une solution donnée de l'un quelconque σ de ces adjoints en une solution, arbitrairement donnée aussi, de cet adjoint (1). C'est ce que nous exprimerons en disant que γ, *plus grand pseudo-sous-groupe de* $\mathfrak{I}$ *laissant* Σ *invariant, est, pour chacun des adjoints* σ *de* Σ, *un pseudo-groupe d'invariance.*

2° *Passage d'un adjoint à un autre.* — Soient σ et σ' deux adjoints de Σ, $(u_1, \ldots, u_n)$ une solution de σ, et $(u'_1, \ldots, u'_n)$ une solution de σ'. Il existe une transformation a,

$$x'_i = x_{\rho_i} \qquad (i = 1, 2, \ldots, n), \tag{40}$$

qui fait passer de $(u_1, \ldots, u_n)$ à $(u'_1, \ldots, u'_n)$, puisque ce sont deux solutions de P. Or les solutions $(v_1, \ldots, v_n)$ de σ sont données par la formule

$$v_i = \theta(u_i) \qquad (i = 1, 2, \ldots, n), \tag{41}$$

(1) Il y a, en effet (n° 4), une transformation de $\mathfrak{I}$ et une seule qui change une solution donnée de P en une solution de P, arbitrairement donnée aussi. Si ces deux solutions appartiennent à un même adjoint σ, cette transformation appartient à γ, et réciproquement, d'après le numéro 6 et la définition des adjoints (n° 7); et elle est, *a fortiori*, la seule transformation de γ qui fasse passer de la première de ces solutions à la seconde. Il en résulte, de plus, que γ est le plus grand pseudo-sous-groupe de $\mathfrak{I}$ qui laisse un adjoint quelconque σ de Σ invariant, puisque toute transformation qui laisse cet adjoint σ invariant change chaque solution de cet adjoint en une solution de cet adjoint.

$x' = \theta(x)$ étant l'une quelconque des transformations de γ; et celles de σ', $(v'_1, \ldots, v'_n)$, sont données, sous la même condition, par

$$v'_i = \theta(u'_i) \qquad (i = 1, 2, \ldots, n). \tag{42}$$

Mais, d'autre part, chaque transformation de $\mathfrak{A}$ étant permutable avec chaque transformation de $\overline{\mathfrak{I}}$ (n° 4 *in fine*), le transformé de σ par a aura pour solution générale

$$u_i = \theta(u'_i) \qquad (i = 1, 2, \ldots, n), \tag{43}$$

les θ étant les mêmes que pour la formule (41), et, par conséquent, que pour la formule (42). C'est dire que σ' est le transformé de σ par a.

Donc, *on passe d'un adjoint σ d'un sous-système Σ quelconque à tout autre de ses adjoints, σ', par les transformations du groupe d'automorphie $\mathfrak{A}$ de* P *qui fait passer d'une solution de σ à une solution de σ'.*

3° *Automorphie des adjoints.* — Si σ' est, dans l'énoncé précédent, identique à σ, on en conclut qu'il y a μ transformations de $\mathfrak{A}$ qui laissent σ invariant, à savoir celles qui changent l'une quelconque, $(u_1, \ldots, u_n)$, de ses solutions en ses μ diverses solutions. Il n'y en a pas davantage; car toute autre, appliquée à $(u_1, \ldots, u_n)$, donnera une solution de P autre que ces μ solutions, et, par conséquent, ne laissera pas σ invariant. Ces μ transformations constituent donc le plus grand sous-groupe de $\mathfrak{A}$ qui laisse σ invariant. Soit α ce sous-groupe. On voit sans peine, que du fait que c'est un groupe, et que ses transformations changent l'une des solutions de σ en ses diverses solutions, il fait de même pour toute autre solution de σ.

Donc σ *est un système automorphe, son groupe d'automorphie étant le plus grand sous-groupe de $\mathfrak{A}$, α, qui laisse σ invariant.* Il résulte également de ce qui précède qu'il y a une transformation de ce groupe d'automorphie, et une seule, qui fait passer d'une solution de σ, arbitrairement choisie, à une autre solution, arbitrairement choisie également, de σ.

Remarque. — Si α et α' sont les groupes d'automorphie de deux adjoints du sous-système E, σ et σ', et si a est l'une des transformations de $\mathfrak{A}$ qui font passer de σ à σ', α' est le transformé de α par a. *Deux adjoints, σ et σ', d'un même sous-système ont donc même pseudo-*

groupe d'invariance; mais, en général, leurs groupes d'automorphie sont différents, et ce sont deux sous-groupes homologues du groupe d'automorphie $\mathfrak{A}$ *de* P.

L'analyse du numéro suivant éclairera, du reste, et précisera, sur certains points, les résultats de celui-ci en montrant la dépendance mutuelle des pseudo-groupes d'invariance et des groupes d'automorphie dont on vient de constater l'existence simultanée pour les systèmes adjoints.

9. Sous-systèmes principaux.

Soient Σ un sous-système de P, ν son ordre, et

$$x_i = u_i \qquad (i = 1, 2, \ldots, n) \tag{44}$$

une de ses solutions. Ses ν solutions sont données par la formule générale

$$x_i = u_{\rho_i} \qquad (i = 1, 2, \ldots, n), \tag{45}$$

$(\rho_1, \ldots, \rho_n)$ devant appartenir à un certain ensemble E de ν permutations des indices $(1, 2, \ldots, n)$, qui contiendra la permutation naturelle $(1, 2, \ldots, n)$.

On pourra passer de la solution (44) à chaque solution (45), soit par l'auto-transformation $\overline{\Theta}$ de P, qui a pour équation

$$x'_i = u_{\rho\alpha}\Phi(x_i, u_\alpha) \qquad (\alpha = 1, 2, \ldots, n;\ i = 1, 2, \ldots, n), \tag{46}$$

et, par conséquent, par l'auto-transformation Θ de $\mathfrak{F}$ qui a pour équation

$$x' = u_{\rho\alpha}\Phi(x, u_\alpha) \qquad (\alpha = 1, 2, \ldots, n) \tag{47}$$

(appliquée par cogrédience des x_i avec x); soit par la transformation a,

$$x'_j = x_{\rho_j} \qquad (j = 1, 2, \ldots, n), \tag{48}$$

du groupe d'automorphie $\mathfrak{A}$ de P.

L'auto-transformation Θ induit la permutation ϖ des racines de $\mathfrak{F}$ qui s'exprime par la substitution (i, ρ_i) $(i = 1, 2, \ldots, n)$, appliquée

aux indices i des u_i : je désignerai cette substitution par s. La transformation a revient, d'autre part, à effectuer sur les indices j des x_j la substitution (ρ_i, i) $(i = 1, 2, \ldots, n)$, c'est-à-dire la substitution s^{-1}, inverse de s.

Si les ν substitutions s forment un groupe g_0, les substitutions s^{-1} forment le même groupe, et réciproquement.

Or, dire que les substitutions s forment un groupe g_0, c'est dire que les permutations ϖ forment un groupe γ_0, qui se trouve rapporté, isomorphiquement et holoédriquement, à ce groupe g_0, et réciproquement. Et, pour que les permutations ϖ forment un groupe γ_0, il faut et il suffit que les auto-transformations Θ, qui les induisent, forment un *pseudo-groupe* γ, au sens qui a été donné à ce terme quand on a défini le pseudo-groupe d'invariance $\mathfrak{I}$ de P. Ce pseudo-groupe γ sera (comparer n° 7) un *pseudo-sous-groupe* de $\mathfrak{I}$; et il se trouvera rapporté (1) au groupe γ_0, et, par suite, au groupe g_0, isomorphiquement et holoédriquement. En même temps, les auto-transformations $\overline{\Theta}$ formeront aussi un pseudo-groupe $\overline{\gamma}$, qui sera un pseudo-sous-groupe de $\overline{\mathfrak{I}}$, et sera en correspondance isomorphique et holoédrique avec γ, γ_0 et g_0. Mais alors les ν transformations $\overline{\Theta}$, qui changent la solution (44) de Σ en ses diverses solutions, formant un pseudo-groupe, changeront aussi (on le démontrerait sans peine) toute solution de Σ en ses diverses solutions. De sorte que $\overline{\gamma}$ sera, pour Σ, un *pseudo-groupe d'invariance;* et il y aura une transformation de $\overline{\gamma}$, et une seule, changeant en une solution donnée de Σ une autre solution quelconque, donnée, de Σ.

Si, réciproquement, Σ a un pseudo-groupe d'invariance, il ne peut être constitué que par les ν transformations $\overline{\Theta}$ considérées, de sorte que celles-ci, et, par conséquent, les substitutions s, forment un groupe, et l'on a les correspondances isomorphiques indiquées.

D'autre part, dire que les substitutions s^{-1} forment un groupe g_0,

---

(1) Il faut entendre par là qu'au produit de deux permutations de γ_0, et des deux substitutions homologues de g_0, correspond le pseudo-produit des transformations de γ qui sont respectivement homologues à ces permutations, comme à ces substitutions. L'isomorphie de deux pseudo-groupes se définirait d'une manière analogue.

c'est dire que les transformations a forment un groupe, g, qui se trouve alors rapporté isomorphiquement (et holoédriquement) à ce groupe g_0. C'est un sous-groupe du groupe d'automorphie $\mathfrak{A}$ de P; et de son existence on conclura, comme on l'a fait au n° 8 pour les adjoints σ, que Σ est alors automorphe et que son groupe d'automorphie est ce sous-groupe g de A.

Si, réciproquement, Σ est automorphe et a pour groupe d'automorphie un sous-groupe de $\mathfrak{A}$, ce groupe d'automorphie ne peut être constitué que par les transformations a considérées; et, par conséquent, celles-ci formant un groupe, g, les substitutions s^{-1} forment un groupe g_0, et l'on a les correspondances d'isomorphie indiquées.

On conclut, en définitive, que *si un sous-système* Σ *de* P *a un pseudo-groupe d'invariance* γ (qui sera nécessairement un pseudo-sous-groupe du pseudo-groupe d'invariance $\mathfrak{I}$ de P), *il est aussi automorphe, avec pour groupe d'automorphie, un sous-groupe g du groupe d'automorphie* $\mathfrak{A}$ *de* P; *et* RÉCIPROQUEMENT. *Le pseudo-groupe d'invariance* γ *et le groupe d'automorphie g* se trouvent, par ce qui précède, rapportés l'un et l'autre, en isomorphie holoédrique, à un même groupe de substitutions g_0 : ils *sont* donc *holoédriquement isomorphes* entre eux.

L'ordre ν de Σ est, du reste, dans ce cas égal à l'ordre du pseudo-groupe d'invariance et du groupe d'automorphie de Σ.

Remarque I. — Ainsi se trouve mise en évidence une catégorie remarquable de sous-systèmes Σ, que nous appellerons les *sous-systèmes principaux* de P.

A cette catégorie appartiennent, d'après les propriétés trouvées au n° 8, les *adjoints* de tout sous-système Σ.

Mais on démontrerait, comme on l'a fait pour ces adjoints, que le pseudo-groupe d'invariance d'un sous-système principal est le plus grand pseudo-sous-groupe de $\mathfrak{I}$ qui le laisse invariant. Et il résulte, d'autre part, de l'étude des adjoints d'un sous-système quelconque Σ de P, que ce sont les divers sous-systèmes de P dont toutes les solutions se déduisent d'une solution de P par les diverses transformations du plus grand pseudo-sous-groupe de $\mathfrak{I}$ qui laisse Σ invariant.

On en conclut que *tout sous-système principal de* P *est l'un de ses propres adjoints.*

L'ensemble des sous-systèmes principaux de P *ne diffère donc pas de l'ensemble des adjoints de tous les sous-systèmes de* P.

Remarque II. — Les adjoints σ d'un sous-système Σ de P ont été définis au n° 7 au moyen d'un *réduit* particulier, Σ_0, de Σ; et ce mode de définition nous sera utile dans la suite. Mais il résulte de ce qui vient d'être dit qu'ils sont, en fait, entièrement déterminés par une de leurs solutions et par le plus grand pseudo-sous-groupe de $\mathfrak{I}$ qui laisse Σ invariant. On obtiendrait donc le même système d'adjoints, pour Σ, si l'on remplaçait, dans la définition initiale, le réduit Σ_0 par un autre, c'est-à-dire l'*équation de référence* $\mathcal{G}$ du n° 6 par une autre quelconque.

Remarque III. — Si l'on tient compte de la permutabilité des transformations du groupe $\mathfrak{A}$ avec celles du pseudo-groupe $\mathfrak{I}$, comme on l'a fait au n° 8 dans l'étude des adjoints d'un même sous-système, on arrive facilement aux conclusions suivantes :

1° Pour chaque pseudo-sous-groupe γ du pseudo-groupe d'invariance $\mathfrak{I}$ du système P, il y a des sous-systèmes principaux de P qui ont ce pseudo-groupe γ pour pseudo-groupe d'invariance, et les solutions de P se répartissent entre eux. Ils forment une *classe* vis-à-vis du groupe d'automorphie $\mathfrak{A}$ de P : leurs groupes d'automorphie respectifs sont, par suite, transformés les uns des autres par des transformations de $\mathfrak{A}$.

2° Pour chaque sous-groupe g du groupe d'automorphie $\mathfrak{A}$ du système P, il y a des sous-systèmes principaux de P qui ont ce groupe g pour groupe d'automorphie, et les solutions de P se répartissent entre eux. Ils forment une *classe* vis-à-vis du pseudo-groupe d'invariance $\mathfrak{I}$ de P : leurs pseudo-groupes d'invariance sont, par suite, *pseudo-transformés* (1) les uns des autres par des transformations de $\mathfrak{I}$.

---

(1) Soient S un des sous-systèmes principaux de la classe, $(u_1, \ldots, u_n)$, $(u'_1, \ldots, u'_n)$ deux quelconques de ses solutions, et $x' = \theta(x)$ la transformation Θ de $\mathfrak{I}$ qui change la première en la seconde. Soit ensuite S' le transformé de S par une transformation quelconque Λ de $\mathfrak{I}$, $y = \lambda(x)$, et $x = \lambda^{-1}(y)$ les équations de cette transformation et de sa pseudo-inverse Λ^{-1}. Aux solutions $(u_1, \ldots, u_n)$ et $(u'_1, \ldots, u'_n)$ de S correspondront, pour S', leurs transformées par Λ,

$$v_i = \lambda(u_i) \quad (i = 1, 2, \ldots, n); \qquad v'_i = \lambda(u'_i) \qquad (i = 1, 2, \ldots, n),$$

10. Remarques préliminaires sur la réductibilité du système associé à une équation algébrique.

On supposera, dans ce qui suit, que l'on donne, en même temps qu'une équation algébrique $\mathcal{F}$ de degré n, un certain *domaine de rationalité* Δ. Par définition, toute opération rationnelle (addition, multiplication, division) appliquée à des éléments du domaine donne comme résultat un élément du domaine. On suppose, d'autre part, que les nombres entiers, positifs ou négatifs, font toujours partie du domaine Δ. Il en est donc de même pour les nombres que l'on appelle rationnels dans l'algèbre élémentaire, et qui constituent le domaine de rationalité *naturel*. En d'autres termes, tout domaine de rationalité Δ contient le domaine de rationalité naturel, mais il peut contenir des éléments qui ne font pas partie de celui-ci.

Il sera entendu que le domaine de rationalité Δ contiendra toutes les variables ou indéterminées que l'on sera amené à introduire. Si donc, on est conduit à en considérer de nouvelles, au cours de l'étude de l'équation $\mathcal{F}$ donnée, on devra les *adjoindre* au domaine Δ primitivement donné : de sorte que celui-ci se trouvera automatiquement remplacé par le nouveau domaine de rationalité résultant de cette adjonction.

Le mot *rationnel* s'entendra, sauf avis contraire, de tout nombre ou expression appartenant au domaine Δ considéré. Une *fonction rationnelle de* $x_1, \ldots, x_n$ (variables figurant dans le système P associé à $\mathcal{F}$) sera donc une fonction rationnelle de ces variables, au sens élémentaire du mot, dont les coefficients appartiendront au domaine Δ.

---

et l'on aura

$$\varphi'_i = \lambda[\theta(u_i)] = \lambda\{\theta[\lambda^{-1}(\varphi_i)]\} \qquad (i = 1, 2, \ldots, n).$$

On passera donc de $(\varphi_1, \ldots, \varphi_n)$ à $(\varphi'_1, \ldots, \varphi'_n)$ en lui appliquant la transformation de $\mathcal{J}$ qui est la *réduite* [*mod.* $F(x)$] de $\Lambda\Theta\Lambda^{-1}$, et que nous appellerons la *pseudo-transformée* de Θ par Λ. Le pseudo-groupe d'invariance γ' de S′ sera l'ensemble de ces pseudo-transformées par Λ des diverses transformations Θ du pseudo-groupe d'invariance γ de S; et il est naturel de l'appeler, en conséquence, comme nous l'avons fait dans le texte, le *pseudo-transformé* de γ par Λ.

Une équation sera dite rationnelle si ses deux membres sont rationnels.

On supposera toujours que les coefficients $p_1, \ldots, p_n$ de l'équation $\mathcal{F}$ considérée appartiennent au domaine de rationalité Δ donné : de sorte que $\mathcal{F}$ sera toujours rationnelle, ainsi que son système associé P.

Cela posé, l'équation $\mathcal{F}$ sera dite *générale* dans le domaine Δ, si le système associé P est *irréductible* dans ce domaine : ce qui signifie qu'il n'existe aucune équation en $x_1, \ldots, x_n$ rationnelle qui soit compatible avec P, sans en être une conséquence (1). Cela revient à dire que P ***n'a pas de sous-système rationnel.*** Dans le cas contraire, P sera dit *réductible*, et $\mathcal{F}$ sera dite *spéciale*.

L'analyse qui suit aura pour but de préciser la manière dont une équation $\mathcal{F}$ donnée est spéciale, c'est-à-dire le mode de réductibilité du système associé P.

Nous remarquerons d'abord, à cet effet, que si un sous-système Σ de P est rationnel sous une forme quelconque donnée, sa *forme type*, définie au n° 5, est aussi rationnelle. Soit, en effet,

$$(49) \qquad A_k(x_1, \ldots, x_n) = 0 \qquad (k = 1, 2, \ldots, r),$$

les équations de ce sous-système Σ, telles qu'elles sont données, qui sont rationnelles par hypothèse. On supposera, ce qui est loisible, que les coefficients m_i de l'inconnue auxiliaire

$$(50) \qquad V = m_1 x_1 + \ldots + m_n x_n$$

sont rationnels (ils le seront, par définition, si on les laisse indéterminés). Alors la résolvante de Galois qui la fournit

$$(51) \qquad \varphi(V) = 0,$$

est rationnelle, ainsi que les formules annexes

$$(52) \qquad x_i = \varphi_i(V) \qquad (i = 1, 2, \ldots, n),$$

(1) C'est le point de vue introduit, comme l'on sait, par M. Drach. Il équivaut, bien entendu, à celui de Galois, plus arithmétique, d'après lequel aucune fonction rationnelle des racines de $\mathcal{F}$, non symétrique, n'a une valeur rationnelle. Mais il se prête mieux à l'intervention des transformations dans l'analyse que nous nous proposons de faire de la réductibilité de P.

qui donnent la solution qui correspond à une racine quelconque de cette résolvante.

Or, pour obtenir la forme type de Σ, on aura à exprimer que V satisfait aux équations rationnelles

$$(53) \qquad 0 = B_k(V) = A_k[\varphi_1(V), \ldots, \varphi_n(V)] \qquad (k = 1, 2, \ldots, r),$$

en même temps qu'à la résolvante (51). Donc V devra satisfaire à l'équation

$$(54) \qquad \psi(V) = 0,$$

où $\psi(V)$ sera le plus grand commun diviseur de φ et des B_k, et sera, par conséquent, rationnel. L'équation

$$(55) \qquad \psi(m_1x_1 + \ldots + m_nx_n) = 0,$$

qui constituera dès lors, avec P, la forme type de Σ, sera donc bien rationnelle.

Si, en particulier, Σ n'a qu'une solution, l'équation (54) sera du premier degré, la valeur V qu'elle donnera sera donc rationnelle, et il en sera de même pour la solution de Σ, qui sera donnée par les formules (52). Toutes les racines de $\mathcal{F}$ seront donc rationnelles. On peut ajouter que toutes les solutions de P, et, par conséquent, toutes les racines de la résolvante de Galois (51), seront rationnelles. Il en sera donc de même pour tous les diviseurs de $\varphi(V)$, de sorte que tous les sous-systèmes de P seront rationnels.

Remarque. — Si Σ_1 et Σ_2 sont deux sous-systèmes de Σ rationnels, le sous-système Σ_0, qui a pour solutions les solutions de P qui leur sont communes, s'il y en a, et le sous-système Σ_3, qui a pour solutions l'ensemble des solutions de Σ_1 et Σ_2, sont rationnels l'un et l'autre.

En effet, Σ_0 s'obtient en réunissant les équations de Σ_1 et de Σ_2.

Quant à Σ_3, on l'obtiendra en ramenant d'abord Σ_1 et Σ_2 à leurs formes types. Si leurs équations complémentaires respectives sont alors

$$\psi_1(m_1x_1 + \ldots + m_nx_n) = 0, \qquad \psi_2(m_1x_1 + \ldots + m_nx_n) = 0,$$

celle de Σ_3, ramenée aussi à sa forme type, sera

$$\psi_3(m_1x_1 + \ldots + m_nx_n) = 0,$$

$\psi_3(V)$ étant le plus petit commun multiple de $\psi_1(V)$ et de $\psi_2(V)$. Comme ψ_1 et ψ_2 sont rationnels par hypothèse, il en sera de même pour ψ_3. Donc Σ_3 sera bien rationnel.

11. Le pseudo-groupe spécifique.

Soit $\mathcal{F}$ une équation donnée de degré n, que nous supposons spéciale, sans, toutefois, que toutes ses racines soient rationnelles. Soit Σ un sous-système rationnel du système associé P. L'équation de référence $\mathcal{G}$, introduite au n° 6, ayant ses racines rationnelles, tous les sous-systèmes de son système associé Q sont rationnels. Donc tout réduit Σ_1 de Σ est rationnel. Par suite, les équations de condition, en $u_1, \ldots, u_n$, qui expriment que la transformation (35), à savoir

$$y = \alpha\Phi(x, u_\alpha) \qquad (\alpha = 1, 2, \ldots, n) \tag{56}$$

(laquelle est rationnelle, puisque les u_i sont indéterminées), change Σ en Σ_0, seront rationnelles. Donc l'adjoint σ de Σ dont les solutions sont génératrices de transformations (58) réduisant Σ à Σ_0 est rationnel, Car on l'obtient en adjoignant ces équations de conditions rationnelles aux équations de P (écrites avec les lettres u_i au lieu des lettres x_i).

Par conséquent, *les adjoints de tout sous-système rationnel de* P *sont aussi rationnels.*

Il en résulte que tout sous-système rationnel Σ de P admet des auto-transformations canoniques de $\mathcal{F}$ autres que la transformation identique; sans quoi les adjoints σ de Σ n'auraient chacun qu'une solution, et, puisqu'ils sont rationnels, toutes les racines de $\mathcal{F}$ seraient rationnelles (n° 10), ce qui est exclu. Soit γ le pseudo-sous-groupe du pseudo-groupe d'invariance $\mathcal{J}$ de $\mathcal{F}$ formé de ces auto-transformations. C'est (n° 8) le pseudo-groupe d'invariance commun à tous les adjoints σ de Σ; et ceux-ci ne sont pas autre chose (n° 9) que les sous-systèmes principaux de P, qui ont γ pour pseudo-groupe d'invariance.

Par conséquent, *si* $\mathcal{F}$ *est spéciale, sans que toutes ses racines soient rationnelles, le pseudo-groupe* γ *formé de toutes les auto-transformations canoniques de* $\mathcal{F}$ *qui laissent invariant un sous-système rationnel quelconque* Σ *de* P, *ne se réduit pas à la seule transformation identique, et*

tous les sous-systèmes principaux de P *qui ont pour pseudo-groupe d'invariance ce pseudo-sous-groupe* γ *du pseudo-groupe d'invariance* $\mathfrak{I}$ *de* P *sont rationnels*. Nous dirons que *la classe de ces sous-systèmes principaux* (relative au groupe d'automorphie $\mathfrak{A}$ de P, ainsi qu'il a été expliqué au n° 9, *Remarque III*) *est rationnelle*.

Il convient d'ajouter que tout sous-système principal étant l'un de ses propres adjoints, sa classe sera rationnelle, d'après ce qui précède, si lui-même est rationnel (1).

Désignons alors par $C_1, C_2, \ldots, C_m$ les classes rationnelles de sous-systèmes principaux de P, et par $\gamma_1, \gamma_2, \ldots, \gamma_m$ leurs pseudo-groupes d'invariance respectifs. Si $(u_1, \ldots, u_n)$ est une solution quelconque de P, il existera dans chaque classe C_k un sous-système S_k admettant cette solution. En réunissant les équations de ces m sous-systèmes S_k on aura un sous-système $\mathfrak{S}$ de P, rationnel, dont les diverses solutions se déduiront de $(u_1, \ldots, u_n)$ par les auto-transformations canoniques de $\mathfrak{F}$ communes aux divers pseudo-groupes γ_k. Celles-ci formant un certain pseudo-sous-groupe K de $\mathfrak{I}$, ce sous-système $\mathfrak{S}$ sera l'un des sous-systèmes principaux de P ayant ce pseudo-groupe K pour pseudo-groupe d'invariance. Sa classe $\mathfrak{C}$ sera donc rationnelle. Ce sera, par suite, l'une des classes C_k, et K sera l'un des pseudo-groupes γ_k.

Donc, *parmi les classes de sous-systèmes principaux de* P *rationnelles, il y en a une dont le pseudo-groupe d'invariance est contenu dans les pseudo-groupes d'invariance de toutes ces classes. Ce pseudo-groupe d'invariance* K *sera dit le* PSEUDO-GROUPE SPÉCIFIQUE *de* $\mathfrak{F}$; *et les sous-systèmes principaux dont il est le pseudo-groupe d'invariance seront dits* SOUS-SYSTÈMES SPÉCIFIQUES *de* $\mathfrak{F}$.

Le pseudo-groupe K ainsi défini caractérise, en effet, entièrement le mode de réductibilité de P. Car il résulte de ce qui précède que tout sous-système de P rationnel demeure invariant par ses transformations; et, réciproquement, tout sous-système de P qui admet les transformations de K est rationnel, parce que ses solutions se répartissent entre des sous-systèmes spécifiques, et que, ceux-ci étant

(1) Cela résulte aussi de ce que les transformations du groupe d'automorphie, qui font passer de ce sous-système à tous ceux de sa classe, sont rationnelles.

rationnels, il en est de même du sous-système considéré, d'après la remarque finale du numéro précédent.

De sorte que, *pour qu'un sous-système de* P *soit rationnel, il faut et il suffit qu'il admette les transformations du pseudo-groupe spécifique de* $\mathfrak{F}$.

Remarque I. — Il résulte de ce qui précède que *le pseudo-groupe spécifique de* $\mathfrak{F}$ *est l'ensemble des auto-transformations canoniques de* $\mathfrak{F}$ *qui laissent invariants, à la fois, tous les sous-systèmes rationnels du système* P *associé à* $\mathfrak{F}$.

Remarque II. — Dans les cas extrêmes que nous avons exclus, celui où $\mathfrak{F}$ est *général*, et celui où toutes les racines de $\mathfrak{F}$ sont rationnelles, il y a encore, aux termes des énoncés ci-dessus, un pseudo-groupe spécifique. C'est, dans le premier cas, le pseudo-groupe d'invariance $\mathfrak{I}$ de $\mathfrak{F}$; et, dans le second cas, le pseudo-sous-groupe de $\mathfrak{I}$ qui est formé de la seule transformation identique.

12. Des solutions conjuguées.

On peut donner des résultats qui précèdent une forme plus concrète en mettant en évidence les liens qui unissent les solutions des sous-systèmes rationnels de P. Remarquons d'abord qu'il résulte de la théorie des sous-systèmes adjoints et des sous-systèmes principaux que *les solutions de* P *se répartissent entre ses divers sous-systèmes spécifiques*.

Soit, d'autre part, Σ un sous-système de P admettant le pseudo-groupe spécifique K. S'il admet une solution $(u_1, \ldots, u_n)$ de P, il admet toutes celles qui s'en déduisent par les diverses transformations de K, c'est-à-dire toutes les solutions du sous-système spécifique dont cette solution $(u_1, \ldots, u_n)$ de P est une solution. Donc les solutions de Σ sont alors celles de un ou plusieurs sous-systèmes spécifiques.

On conclut donc du théorème fondamental qui termine le numéro précédent que *pour qu'un sous-système de* P *soit rationnel, il faut et il suffit, ou bien que ce soit un sous-système spécifique, ou bien que ses solutions se répartissent entre plusieurs sous-systèmes spécifiques*.

Les choses deviennent plus nettes si l'on introduit la terminologie suivante. On dira qu'une solution $(u'_1, \ldots, u'_n)$ de P est *conjuguée* à une autre $(u_1, \ldots, u_n)$, si elle en résulte par une des transformations du pseudo-groupe spécifique K de $\mathcal{F}$. La solution $(u_1, \ldots, u_n)$ résultant alors de $(u'_1, \ldots, u'_n)$ par la pseudo-inverse de cette transformation, $(u_1, \ldots, u_n)$ est aussi *conjuguée* à $(u'_1, \ldots, u'_n)$ et l'on peut dire que $(u_1, \ldots, u_n)$ et $(u'_1, \ldots, u'_n)$ sont *deux solutions de* P *conjuguées*.

Cela posé, l'ensemble des solutions de P qui sont conjuguées à une même solution $(u_1, \ldots, u_n)$ est aussi formé de toutes les solutions conjuguées à une solution quelconque de P appartenant à cet ensemble. On dira qu'il constitue *une famille complète de solutions de* P *conjuguées* (deux à deux).

On voit que *les solutions de tout sous-système spécifique de* P *forment une famille complète de solutions conjuguées de* P, *et réciproquement.*

On peut donc énoncer les théorèmes suivants :

1° *Les solutions de* P *se répartissent en familles complètes de solutions conjuguées;*

2° *Toute famille complète de solutions conjuguées est l'ensemble des solutions d'un sous-système rationnel de* P (sous-système spécifique);

3° *Les sous-systèmes rationnels de* P *sont ceux dont les solutions sont, dans leur ensemble, les solutions de* P *qui constituent une ou plusieurs familles complètes de solutions conjuguées.*

En somme, *une solution quelconque de* P *est inséparable de ses conjuguées*, en ce qui concerne sa détermination (plus ou moins complète) par des systèmes d'équations rationnelles.

Remarque. — D'après ce qui précède, un sous-système rationnel de P qui admet une solution d'un sous-système spécifique les admet toutes, puisqu'il admet toutes les solutions conjuguées à cette solution. *Les sous-systèmes spécifiques sont donc irréductibles.*

13. Le problème de Galois.

Nous avons, dans ce qui précède, caractérisé l'ensemble des sous-systèmes de P qui sont rationnels dans un domaine de rationalité Δ

donné : ce sont ceux qui admettent les transformations $x' = \theta(x)$ du pseudo-groupe spécifique K de $\mathfrak{F}$ relatif à Δ.

Considérons maintenant, avec Galois, les fonctions de $x_1, \ldots, x_n$, rationnelles dans Δ, et une solution quelconque de P,

$$x_i = \xi_i \qquad (i = 1, 2, \ldots, n), \tag{57}$$

et cherchons à quelle condition la valeur $R(\xi_1, \ldots, \xi_n)$ que prend, pour cette solution, une de ces fonctions $R(x_1, \ldots, x_n)$ sera rationnelle dans Δ.

S'il en est ainsi, l'équation

$$R(x_1, \ldots, x_n) = R(\xi_1, \ldots, \xi_n) \tag{58}$$

constituera avec P un sous-système rationnel de P, puisqu'elle admet la solution (57) : ce sous-système Σ sera donc invariant par toute transformation $x' = \theta(x)$ du pseudo-groupe spécifique K et, par suite, l'équation

$$R[\theta_0(x_1), \ldots, \theta_0(x_n)] = R(\xi_1, \ldots, \xi_n), \tag{59}$$

où $x' = \theta_0(x)$ est la pseudo-inverse de $x' = \theta(x)$, admettra, en particulier, la solution (57) de (58). On aura donc

$$R[\theta_0(\xi_1), \ldots, \theta_0(\xi_n)] = R(\xi_1, \ldots, \xi_n). \tag{60}$$

C'est dire que $R(x_1, \ldots, x_n)$ prend la même valeur quand on y remplace $(x_1, \ldots, x_n)$ par la solution $(\xi_1, \ldots, \xi_n)$ considérée ou par l'une quelconque de ses conjuguées.

Si, réciproquement, cette condition est remplie, l'équation (58) sera une conséquence du sous-système spécifique dont les solutions sont la solution (57) de P et ses conjuguées.

Prenons ce sous-système S sous la *forme type* introduite au n° 5, en associant aux inconnues $x_1, \ldots, x_n$ l'inconnue auxiliaire de Galois $V = m_1 x_1 + \ldots + m_n x_n$; et soit

$$V = m_1 x_1 + \ldots + m_n x_n, \qquad x_i = \varphi_i(V) \qquad (i = 1, 2, \ldots, n), \qquad \psi(V) = 0 \tag{61}$$

cette forme type. L'équation

$$R[\varphi_1(V), \ldots, \varphi_n(V)] = R(\xi_1, \ldots, \xi_n) \tag{62}$$

devra être une conséquence de $\psi(V) = 0$.

Or, on peut supposer que R est entier en $x_1, \ldots, x_n$ et que les $\varphi_i(V)$ sont entiers en V; de sorte que le premier membre de (62) sera un polynome $A(V)$ et que $A(V) - R(\xi_1, \ldots, \xi_n)$ devra être divisible par $\psi(V)$. Mais la division de $A(V)$, qui est rationnel, par $\psi(V)$, qui l'est aussi, donne une identité

$$A(V) = \psi(V)B(V) + C(V), \tag{63}$$

où $B(V)$ et $C(V)$ sont rationnels; et l'on en déduit

$$A(V) - R(\xi_1, \ldots, \xi_n) = \psi(V)B(V) + [C(V) - R(\xi_1, \ldots, \xi_n)], \tag{64}$$

qui est l'identité donnée par la division du premier membre par $\psi(V)$. Le reste de cette division devant être nul, on a, dès lors, l'identité en V

$$R(\xi_1, \ldots, \xi_n) = C(V), \tag{65}$$

d'où il résulte que $R(\xi_1, \ldots, \xi_n)$ est rationnel.

On a donc la solution du *problème de Galois* sous la forme :

Pour qu'une fonction rationnelle de $x_1, \ldots, x_n$ prenne une valeur rationnelle quand on y remplace $(x_1, \ldots, x_n)$ par une solution du système P, *associé à l'équation algébrique $\mathcal{F}$ considérée, il faut et il suffit qu'elle prenne la même valeur quand on y remplace $(x_1, \ldots, x_n)$ soit par cette solution, soit par l'une quelconque de ses conjuguées.*

11. Le groupe de Galois.

Pour ramener l'énoncé ci-dessus à la forme classique du théorème fondamental de Galois, il n'y a qu'à tenir compte de la définition des solutions (n° 12).

Soit, comme précédemment,

$$x_i = \xi_i \ (i = 1, 2, \ldots, n), \tag{66}$$

une solution quelconque de P, que nous représenterons par $(\xi_1, \ldots, \xi_n)$. Ses conjuguées s'en déduisent en lui appliquant les diverses transformations $x' = \theta(x)$ du pseudo-groupe spécique K de $\mathcal{F}$. Ce sont donc les diverses solutions

$$[\theta(\xi_1), \ldots, \theta(\xi_n)]. \tag{67}$$

Or, la solution $(\xi_1, \ldots, \xi_n)$ est formée des racines de $\mathcal{F}$, rangées dans un certain ordre; et chaque transformation $x' = \theta(x)$ de K, étant l'une des auto-transformations canoniques de $\mathcal{F}$ (n° 3), effectue sur les racines de $\mathcal{F}$, considérées comme des objets distincts, une certaine permutation concrète ϖ. Les conjuguées d'une solution quelconque de P s'en déduisent donc en y effectuant, sur les racines de $\mathcal{F}$, les diverses permutations ϖ ainsi *induites* par les diverses transformations du pseudo-groupe spécifique K de $\mathcal{F}$.

Ces permutations forment un groupe Γ, holoédriquement isomorphe au pseudo-groupe spécifique K. Nous l'appellerons le *groupe de Galois* de $\mathcal{F}$, relatif au domaine de rationalité Δ considéré. Et, d'après ce qui vient d'être dit, les conjuguées d'une solution de P sont les diverses solutions de P qui s'en déduisent en y effectuant, sur les racines de $\mathcal{F}$, les diverses permutations du groupe de Galois de $\mathcal{F}$. Nous aurons ainsi, pour le théorème du numéro précédent, l'énoncé classique :

Pour qu'une fonction rationnelle de $x_1, \ldots, x_n$ prenne une valeur rationnelle quand on y remplace $(x_1, \ldots, x_n)$ par une solution de P, *il faut et il suffit qu'elle prenne la même valeur quand on y remplace $(x_1, \ldots, x_n)$ soit par cette solution, soit par l'une quelconque de celles qui s'en déduisent par les permutations du groupe de Galois*, Γ, *de l'équation.*

Ou encore, en langage abrégé :

Pour qu'une fonction rationnelle des racines de l'équation $\mathcal{F}$ ait une valeur numérique rationnelle, il faut et il suffit qu'elle demeure invariante, numériquement, par les diverses transformations du groupe de Galois de l'équation.

Remarque I. — La notion du groupe de Galois se présente ainsi d'une manière concrète qui paraît conforme aux idées mêmes de Galois. Mais on peut lui donner aussi une forme abstraite.

La solution $(\xi_1, \ldots, \xi_n)$ de P, considérée, est formée des racines de $\mathcal{F}$, prises dans un certain ordre. On peut s'en servir pour écrire la transformation générale $x' = \theta(x)$ du pseudo-groupe spécifique K sous la forme (comparez n° 3)

$$x' = \xi_{f_\alpha} \Phi(x, \xi_\alpha) \qquad (\alpha = 1, 2, \ldots, n), \tag{68}$$

où la permutation $(\rho_1, \ldots, \rho_n)$ des indices $(1, 2, \ldots, n)$ devra faire partie d'un certain ensemble P de telles permutations. Cette transformation change chaque racine ξ_i en ξ_{ρ_i}; la permutation ϖ qu'elle effectue sur les racines de $\mathcal{F}$ se traduit donc ainsi par la substitution (i, ρ_i) $(i = 1, 2, \ldots, n)$, appliquée aux indices des ξ. Le groupe de Galois Γ est, par suite, représenté par le groupe G formé par ces diverses substitutions.

Mais il faut noter que cette représentation de Γ change si l'on numérote les racines autrement : G est alors remplacé par un de ses transformés par les diverses substitutions des indices $(1, 2, \ldots, n)$; de sorte qu'au groupe de Galois unique Γ correspond une famille de groupes de substitutions, homologues entre eux.

Remarque II. — On peut encore présenter les choses autrement, d'un point de vue analytique, en opérant sur les variables x_i, au lieu d'opérer sur les racines de $\mathcal{F}$.

Si l'on applique, en effet, à ces variables, dans les équations (66) de la solution $(\xi_1, \ldots, \xi_n)$ de P, la transformation (68), on obtient les équations

$$x'_i = \xi_{\rho_i} \qquad (i = 1, 2, \ldots, n) \tag{69}$$

de sa transformée $(\xi_{\rho_1}, \ldots, \xi_{\rho_n})$; et cela équivaut à effectuer dans (66), (toujours sur les x_i), la transformation

$$x'_i = x_{\rho_i} \qquad (i = 1, 2, \ldots, n); \tag{70}$$

ce qui équivaut, d'autre part, à effectuer, sur les indices des x, la substitution (ρ_i, i) $(i = 1, 2, \ldots, n)$.

Les substitutions (ρ_i, i) étant les inverses des substitutions (i, ρ_i), qui constituent le groupe G, image du groupe de Galois, forment le même groupe G, et l'ensemble des transformations (70) qui leur correspondent est un groupe H, holoédriquement isomorphe à ce groupe G, et, par conséquent, au groupe de Galois, comme au pseudo-groupe spécifique.

On se retrouve en présence des propriétés précédemment constatées, au n° 9, pour les sous-systèmes principaux. Et l'on voit que H n'est pas autre chose que le groupe d'automorphie du sous-système spécifique S qui a pour solutions $(\xi_1, \ldots, \xi_n)$ et ses conjuguées.

Les conjuguées de $(\xi_1, \ldots, \xi_n)$, étant les solutions de ce système S, se déduisent évidemment les unes des autres par les transformations du groupe d'automorphie H de ce système. Mais il résulte de ce qu'on a vu pour les sous-systèmes principaux, que si l'on passe d'une famille complète de solutions conjuguées à une autre, c'est-à-dire d'un sous-système spécifique S à un autre S′, on a, en général, affaire à un autre groupe d'automorphie H′. Car le groupe d'automorphie du système S′ est le transformé de H par l'une quelconque des transformations du groupe d'automorphie $\mathfrak{A}$ de P qui fait passer d'une solution S à une solution S′.

Ici encore, on rencontre donc, comme équivalents du groupe de Galois, une classe de sous-groupes homologues.