BULLETIN DE LA S. M. F.

A. E. PELLET

Mémoire sur la théorie algébrique des équations

Bulletin de la S. M. F., tome 15 (1887), p. 61-103

<http://www.numdam.org/item?id=BSMF_1887__15__61_1>

Mémoire sur la théorie algébrique des équations;

par M. A.-E. Pellet.

(Séance du 16 février 1887.)

Je me propose, dans ce Mémoire, d'établir les théorèmes généraux de la théorie algébrique des équations indépendamment de la théorie des substitutions. J'applique ensuite la méthode générale aux équations dont dépend la division du cercle en un nombre premier de parties égales et aux équations qui se ramènent aux équations binômes par une transformation linéaire. L'idée première de ce travail a été exposée dans une thèse présentée à la Faculté des Sciences de Paris, en 1878.

I.

Généralités.

1. On peut définir la notion de quantité en partant de l'idée de nombre et s'appuyant sur les principes du Calcul infinitésimal;

alors la conception de Descartes pour les quantités réelles et celle d'Argant pour les quantités imaginaires ne servent que de support à la notion et viennent en aide au raisonnement en donnant prise à l'imagination, surtout dans les théories de l'Analyse infinitésimale. Mais on peut partir de ces conceptions de Descartes et d'Argant pour définir les quantités; alors les quatre opérations fondamentales, addition et soustraction, multiplication et division, se définissent par la Géométrie; dans le cas où les quantités sont commensurables, les résultats de ces opérations coïncident avec ceux de l'Arithmétique. Un avantage de cette façon d'envisager les choses est de délimiter avec précision le domaine de l'Algèbre de celui de l'Analyse infinitésimale. L'Algèbre est l'étude générale des quantités, réelles ou imaginaires, en se bornant toutefois à un nombre fini d'opérations, tandis que l'Analyse infinitésimale est l'ensemble des théories où l'on envisage un nombre infini d'opérations.

2. Une fonction *entière* de plusieurs quantités est une fonction de ces quantités qui peut s'exprimer par les trois premières opérations, addition, soustraction et multiplication; une fonction *rationnelle* est une fonction qui peut s'exprimer par les quatre opérations fondamentales, addition, soustraction, multiplication et division.

Nous considérerons surtout dans ce Mémoire les fonctions rationnelles. Soient

$$a_1,\ a_2,\ a_3,\ \ldots,\ a_k.$$

k quantités non commensurables regardées comme connues : toute quantité, fonction rationnelle de ces quantités, est dite *rationnelle actuellement* ou simplement *rationnelle;* toute quantité ne pouvant pas s'exprimer rationnellement, au moyen des k quantités $a_1, a_2, \ldots, a_k$, est actuellement irrationnelle. Nous supposons que, parmi les k quantités $a_1, a_2, \ldots, a_k$, aucune ne puisse s'exprimer rationnellement en fonction des autres, sans quoi on pourrait diminuer leur nombre.

Dans le cas où aucune quantité n'est donnée spécialement, les seules quantités rationnelles sont les nombres entiers et fractionnaires, fonctions entières et rationnelles de l'unité. Les irrationnelles qui se présentent tout d'abord sont les racines des équa-

tions du second degré à coefficients entiers. Soit

$$Dx^2 + Ex + F = 0$$

une telle équation, D, E, F étant des entiers n'ayant pas de diviseur commun. Posons $E^2 - 4DF = g^2 A$, g et A étant des entiers, la dernier A non divisible par le carré d'un nombre premier et positif ou négatif selon le signe de $E^2 - 4DF$; et $y^2 - A = 0$, si A est pair ou congru à $-1 \pmod 4$; $y^2 + y + A_1 = 0$, A_1 représentant $\frac{1 - A}{4}$, si A est congru à $1 \pmod 4$.

Il est clair que toute fonction rationnelle de x peut s'exprimer rationnellement en fonction de y, et inversement. Mais une fonction rationnelle de x n'est un *nombre entier algébrique* que dans le cas où elle se ramène à une fonction entière de y. On dit qu'une quantité est un nombre entier algébrique lorsqu'elle est racine d'une équation à coefficients entiers, le coefficient de la plus haute puissance de l'inconnue étant l'*unité;* une fonction entière de telles quantités jouit de la même propriété, et, en particulier, est un nombre entier si elle est commensurable. Un nombre entier algébrique est dit unité complexe, lorsque son inverse est encore un nombre entier algébrique. Parmi les fonctions entières de y, il y a des unités complexes qui sont toutes des puissances entières de l'une d'elles, lorsque A est un nombre positif; dans le cas où A est négatif, il n'y a d'unité complexe que pour les valeurs -1 et -3 de A. (Kronecker, *Comptes rendus,* année 1883, 1er semestre; et 1884, 2e semestre). Lorsque A est égal à l'un des nombres

$$(a) \qquad -1, \quad \pm 2, \quad \pm 3, \quad 5, \quad -7, \quad -11, \quad 13,$$

les fonctions entières de y jouissent de la propriété fondamentale des nombres entiers ordinaires; elles ne sont décomposables que d'une seule manière en un produit de facteurs premiers (Dedekind, *Bulletin des Sciences mathématiques,* 1877). Pour ces valeurs de A, les fonctions entières de y sont dites *nombres entiers complexes*. Ces propriétés n'ont plus lieu lorsque A n'est pas un nombre de la suite a.

3. Il y a la plus grande analogie entre la *divisibilité* des nombres entiers, ordinaires ou complexes, et la divisibilité des fonc-

tions entières d'une variable. Lorsque deux fonctions entières $f(x)$ et $f_1(x)$ n'ont pas de diviseur commun, on peut trouver deux autres fonctions P et Q, telles que

$$Pf(x) + Qf_1(x) = 1.$$

De là résulte qu'une fonction irréductible, qui divise le produit de deux fonctions, divise au moins l'une d'elles ; et qu'une fonction entière ne peut se décomposer que d'une seule manière en un produit de facteurs irréductibles.

Nous rappelons qu'on dit qu'une fonction entière est irréductible lorsqu'elle n'est divisible par aucune fonction entière à coefficients rationnellement connus, de degré inférieur. Gauss a le premier démontré que, si une fonction entière à coefficients entiers est le produit de deux fonctions entières à coefficients rationnels, elle est aussi le produit de deux fonctions entières à coefficients entiers; le théorème s'applique encore lorsque les coefficients sont des entiers complexes et permet dans ces cas de décomposer un polynôme en ses facteurs quelquefois avec facilité.

D'après ce qui précède, une fonction ne peut s'annuler pour un nombre de valeurs de la variable, supérieur au degré de la fonction, quelles que soient les quantités considérées comme connues. Lorsque l'équation obtenue, en égalant la fonction à o, est une équation binôme ou se ramène aux équations binômes, on voit facilement qu'elle a autant de racines qu'il y a d'unités dans son degré, en tenant compte de leurs degrés de multiplicité. Mais les méthodes du Calcul infinitésimal sont nécessaires pour montrer que le théorème s'étend à tous les cas. Les irrationnelles, racines d'équations algébriques à coefficients entiers, se désignent sous le nom de *nombres algébriques*. Cette classe de quantités est très étendue, mais elle est loin de comprendre toutes les quantités incommensurables. Liouville a donné un caractère (*Journal de Mathématiques,* t. V) permettant d'affirmer dans certains cas qu'une quantité donnée n'est racine d'aucune équation à coefficients rationnels d'un degré inférieur à un nombre donné, quelconque d'ailleurs. M. Hermite a plus tard montré que le nombre e, base des logarithmes népériens, ne satisfait à aucune équation algébrique à coefficients entiers, démonstration étendue au nombre π, rapport de la circonférence au diamètre, par M. Lindemann.

Enfin, M. Cantor, dans sa théorie des ensembles, a rattaché la proposition à son véritable principe (*Acta mathematica*, année 1883). Son raisonnement montre que, en figurant les quantités d'après le mode d'Argant, on peut relier deux points quelconques du plan par un trait continu ne passant par aucun des points pour lesquels la quantité correspondante est racine d'une équation à coefficients entiers. Un nombre algébrique est dit *nombre entier algébrique* lorsque le coefficient de la plus haute puissance de l'inconnue est 1, dans l'équation qui le définit, les autres étant entiers.

4. Lorsque nous conviendrons de regarder comme connue une certaine irrationnelle, nous dirons, suivant l'usage, que nous adjoignons cette quantité aux quantités connues. L'adjonction aux quantités connues d'une quantité qui n'est racine d'aucune équation à coefficients rationnellement connus revient à adjoindre une quantité indéterminée. Dans l'étude algébrique des équations, on n'adjoint aux quantités connues que des irrationnelles algébriques, c'est-à-dire que l'on peut définir à l'aide des quantités primitives par des équations à coefficients rationnellement connus, et le problème principal est la recherche des irrationnelles dont la connaissance permet de former rationnellement les diverses racines d'une ou de plusieurs équations données.

Lagrange a démontré que, étant données tant d'irrationnelles algébriques qu'on voudra, on peut toujours les exprimer toutes en fonction rationnelle d'une même irrationnelle.

En effet, on pourra former une équation, à coefficients rationnellement connus, admettant pour racines ces irrationnelles, et qui n'aura pas de racines égales. La proposition se présente alors comme corollaire du théorème suivant, qui est fondamental :

Soit $V_0 = \varphi(x_0, x_1, \ldots, x_{m-1})$ une fonction rationnelle des m racines de l'équation $f(x) = 0$, n'ayant pas de racines égales, cette fonction pouvant acquérir par les permutations des racines $1, 2, 3, \ldots, m$ valeurs distinctes; ces $1, 2, 3, \ldots, m$ valeurs de V sont racines d'une équation à coefficients rationnels, $\pi(V) = 0$, qui peut être réductible. Chacune des m racines $x_0, x_1, \ldots, x_{m-1}$, peut s'exprimer rationnellement en fonction de l'une des valeurs de V; par suite, les diverses valeurs de V peuvent s'exprimer rationnellement en fonction l'une de l'autre; $\pi(V) = 0$ se décom-

pose en facteurs irréductibles d'égal degré, et ce degré est indépendant de la fonction prise pour V, pourvu qu'elle satisfasse aux conditions posées. Soit $F(V)$ un des diviseurs irréductibles de $\pi(V)$; V est appelée la *fonction résolvante* et $F(V) = 0$ l'*équation résolvante* de l'équation $f(x) = 0$ (Serret, *Algèbre supérieure;* Camille Jordan, *Traité des substitutions et des équations algébriques.*)

5. *Soient* $\varphi(z) = 0$ *une équation irréductible, et* $z_0, z_1, \ldots, z_{m-1}$ *ses m racines; soit en outre* $f(z, z_0)$ *une fonction entière de z, à coefficients fonctions rationnelles de* z_0, *irréductible;* $f(z, z_1), \ldots, f(z, z_{m-1})$ *sont également irréductibles, et, si la fonction entière* $F(z, z_0)$ *est divisible par* $f(z, z_0)$, $F(z, z_1)$ *le sera par* $f(z, z_1)$, $F(z, z_2)$ *par* $f(z, z_2)$, *et ainsi des autres.*

Si $f(z, z_i)$ n'est pas irréductible, soit $\beta(z, z_i)$ un de ses diviseurs; ζ étant une indéterminée, effectuons la division des polynômes $f(z, \zeta)$, $\beta(z, \zeta)$ et désignons par $\lambda(z, \zeta)$, $\theta(z, \zeta)$ le quotient et le reste de cette division; on aura

$$f(z, \zeta) = \beta(z, \zeta)\lambda(z, \zeta) + \theta(z, \zeta).$$

D'après notre hypothèse, on a identiquement $\theta(z, z_i) = 0$; ainsi, dans le polynôme $\theta(z, \zeta)$, les coefficients des diverses puissances de z s'annulent pour $\zeta = z_i$; par conséquent, ces coefficients s'annuleront aussi si l'on remplace ζ par une quelconque des racines de l'équation $\varphi(z) = 0$, puisqu'elle est supposée irréductible, et en particulier pour $\zeta = z_0$; $f(z, z_0)$ admettrait donc le diviseur $\beta(z, z_0)$ et ne serait pas irréductible.

La première partie du théorème est donc démontrée; pour démontrer la seconde partie, on remplacerait dans $F(z, z_0)$ et $f(z, z_0)$, z_0 par ζ et l'on effectuerait la division comme précédemment; on verrait que le reste est identiquement nul pour $\zeta = z_0$ et que par suite il est nul aussi lorsqu'on y remplace ζ par une autre racine de $\varphi(z) = 0$.

6. $\theta(x)$ *étant une fonction rationnelle de x, soit* μ *le nombre de valeurs distinctes qu'elle prend lorsqu'on remplace x successivement par les m racines de l'équation* $f(x) = 0$ *irréductible*

et de degré m; μ *est un diviseur de m et ces* μ *valeurs sont racines d'une équation irréductible.*

Désignons par $x_0, x_1, \ldots, x_{m-1}$ les m racines de $f(x) = 0$. Celles de ces racines qui donnent pour $\theta(x)$ la valeur $\theta(x_0)$, satisfaisant à la fois aux deux équations $f(x) = 0$ et $\theta(x) - \theta(x_0) = 0$, appartiennent au plus grand commun diviseur des premiers membres de ces équations, et, réciproquement, les racines de ce plus grand commun diviseur égalé à 0 satisfont à la fois aux deux équations précédentes. Soit $\chi[x, \theta(x_0)]$ ce plus grand commun diviseur : je dis que $\chi[x, \theta(x_i)]$ sera le plus grand commun diviseur de $f(x)$ et $\theta(x) - \theta(x_i)$. En effet, $\chi[x, \theta(x_i)]$ divise $f(x)$ et $\theta(x) - \theta(x_i)$ d'après le n° 5. De plus, il n'y a pas de polynôme de degré supérieur à $\chi[x, \theta(x_i)]$ divisant à la fois $f(x)$ et $\theta(x) - \theta(x_i)$; car on en déduirait, d'après le théorème qui fait l'objet de ce n° 5, un polynôme de degré supérieur à $\chi[x, \theta(x_0)]$, divisant $f(x)$ et $\theta(x) - \theta(x_0)$. Maintenant, si $\chi[x, \theta(x_0)] = 0$ et $\chi[x, \theta(x_i)] = 0$ ont une racine commune, elles ont toutes leurs racines communes. En effet, la racine commune appartient à la fois à $f(x) = 0$ et $\theta(x) - \theta(x_0) = 0$ d'une part, à $f(x)$ et $\theta(x) - \theta(x_i) = 0$ d'autre part; or les deux équations $\theta(x) - \theta(x_0) = 0$ et $\theta(x) - \theta(x_i) = 0$ ne peuvent avoir de racine commune que dans le cas où $\theta(x_0) = \theta(x_i)$, et alors $\chi[x, \theta(x_0)] = \chi[x, \theta(x_i)]$.

Il résulte de ce qui précède que les m racines de $f(x) = 0$ se partagent en $\frac{m}{\nu}$ groupes de ν racines, ν étant le degré de $\chi[x, \theta(x_0)]$; les racines de chaque groupe donnent la même valeur pour $\theta(x)$, et cette valeur varie d'un groupe à l'autre.

Si l'on adjoint $\theta(x_0)$ aux quantités connues, $\chi[x, \theta(x_0)]$ devient un polynôme rationnel; ce polynôme est irréductible. En effet, s'il admettait un diviseur $\chi_1[x, \theta(x_0)]$ à coefficients, fonctions rationnelles de $\theta(x_0)$, $\chi[x, \theta(x_i)]$ admettrait le diviseur $\chi_1[x, \theta(x_i)]$. Or, soient $y_0, y_1, \ldots, y_{\mu-1}$ les μ valeurs de $\theta(x)$, μ désignant le rapport $\frac{m}{\nu}$. Ces μ valeurs sont racines d'une équation à coefficients rationnels; car on a

$$y_0^n + y_1^n + \ldots + y_{\mu-1}^n = \frac{1}{\nu}[\theta(x_0)^n + \theta(x_1)^n + \ldots + \theta(x_{m-1})^n],$$

et le second membre, fonction symétrique des racines de l'équa-

tion $f(x) = 0$, est rationnel; les coefficients de l'équation en y sont des fonctions entières des μ valeurs qu'il acquiert lorsqu'on donne à n successivement les valeurs $1, 2, \ldots, \mu$. D'après cela, le produit $\chi_1(x, y_0)\chi_1(x, y_1)\chi_1(x, y_2)\ldots\chi_1(x, y_{\mu-1})$ serait rationnel et diviserait le polynôme $f(x)$, tout en étant de degré inférieur, ce qui est impossible, puisque $f(x)$ est supposé irréductible.

Enfin l'équation qui a pour racines les μ valeurs $y_0, y_1, \ldots, y_{\mu-1}$ est irréductible. En effet, si elle ne l'était pas, soient μ' le degré de l'un de ses diviseurs, et $y_0, y_1, \ldots, y_{\mu'-1}$ ses μ' racines. Le produit

$$\chi(x, y_0)\chi(x, y_1)\ldots\chi(x, y_{\mu'-1})$$

aurait ses coefficients rationnels et diviserait $f(x)$, tout en étant de degré inférieur.

7. Ce théorème conduit à des conséquences importantes relativement aux équations résolvantes. Soient $x_0, x_1, \ldots, x_{m-1}$ les m racines d'une équation $f(x) = 0$, irréductible ou non, mais n'ayant pas de racines égales; désignons par V_0 une fonction résolvante de cette équation, et par $F(V) = 0$ son équation résolvante de degré N. Les racines de l'équation $f(x) = 0$ sont des fonctions rationnelles de V_0; soient

$$x_0 = \psi_0(V_0). \qquad x_1 = \psi_1(V_0). \qquad x_2 = \psi_2(V_0). \quad \ldots, \quad x_{m-1} = \psi_{m-1}(V_0).$$

On a

$$f[\psi_0(V_0)] = 0;$$

par suite, $f[\psi_0(V)] = 0$ admet toutes les racines de l'équation $F(V) = 0$, puisque celle-ci est irréductible. Ainsi les diverses valeurs qu'acquiert la fonction $\psi_0(V)$, lorsqu'on substitue à V les diverses racines de $F(V) = 0$, sont racines de $f(x) = 0$. Si donc $f(x) = 0$ est irréductible, les valeurs distinctes comprises dans la suite $\psi_0(V_0), \psi_0(V_1), \ldots, \psi_0(V_{N-1})$ sont au nombre de m, degré de $f(x) = 0$, et N est un multiple de m. Si $f(x)$ n'est pas irréductible, soit $f(x) = f_1(x) f_2(x)\ldots f_i(x)$, $f_1(x), \ldots, f_i(x)$ étant des polynômes entiers irréductibles. Si x_0 est racine de $f_1(x) = 0$, par exemple, $\psi_0(V)$ prend, par la substitution à V des diverses racines de l'équation $F(V) = 0$, des valeurs égales aux diverses

racines de $f_1(x) = 0$; et le degré N de $F(V)$ est un multiple des degrés des divers polynômes $f_1(x), f_2(x), \ldots, f_i(x)$. Bien plus, le degré de $F(V)$ est un multiple des degrés des équations résolvantes des diverses équations $f_1(x) = 0, f_2(x) = 0, \ldots, f_i(x) = 0$. Soient, en effet, V' une fonction résolvante de l'équation

$$f_1(x) = 0$$

et $F_1(V') = 0$ son équation résolvante. V'_0 est une fonction rationnelle de V_0. Soit $V'_0 = \Pi_0(V_0)$; on a

$$F[\Pi_0(V_0)] = 0 :$$

donc $F_1[\Pi_0(V)] = 0$ admet toutes les racines de l'équation

$$F(V) = 0.$$

Donc $\Pi_0(V)$ acquiert, par la substitution à V des diverses racines de l'équation $F(V) = 0$, des valeurs égales aux racines de $F_1(V') = 0$, et, puisque celle-ci est irréductible, le nombre de valeurs distinctes de $\Pi(V)$ est égal au degré de $F_1(V') = 0$.

Soit

$$z_0 = \Pi(x_0, x_1, \ldots, x_{m-1})$$

une fonction rationnelle des racines de l'équation $f(x) = 0$; substituons dans z_0, à la place des quantités x, leurs valeurs en fonction de V_0; on en déduira $z_0 = \Pi_1(V_0)$. $\Pi_1(V)$ acquiert, par la substitution à V des diverses racines de l'équation $F(V) = 0$, un nombre ν de valeurs distinctes (ν est un diviseur de N), parmi lesquelles se trouve z_0, et ces valeurs sont racines d'une équation irréductible. De plus, $F(V)$ admet un diviseur à coefficients fonctions rationnelles de z_0, irréductible si l'on n'adjoint que cette quantité aux quantités connues de degré $\frac{N}{\nu}$; ce diviseur égalé à 0 est la nouvelle équation résolvante après l'adjonction de z_0.

II.

Des équations holodromes.

8. Nous appellerons *équations holodromes* les équations irréductibles dont toutes les racines peuvent s'exprimer rationnellement en fonction de l'une d'elles; les équations résolvantes ren-

trent dans cette classe d'équations. Soient $F(x) = 0$ une équation holodrome de degrê m, et x_0, $x_1 = \theta_1(x_0)$, $x_2 = \theta_2(x_0)$, ..., $x_{m-1} = \theta_{m-1}(x_0)$ ses m racines, $\theta_1, \theta_2, \ldots, \theta_{m-1}$ désignant des fonctions rationnelles. La suite x_i, $\theta_1(x_i)$, ..., $\theta_{m-1}(x_i)$ est, dans un ordre différent, la même que la suite $x_0, x_1, \ldots, x_{m-1}$. On peut supposer que les fonctions θ soient entières; remplaçons x_0 par une variable x, et considérons la suite des fonctions

$$x_1, \quad \theta_1(x), \quad \theta_2(x), \quad \ldots, \quad \theta_{m-1}(x). \tag{1}$$

$\theta_i[\theta_j(x)]$ est une fonction entière de x, qui, divisée par $F(x)$, donne pour reste une des m fonctions (1), $\theta_i(x)$, $\theta_j(x)$ étant deux quelconques des fonctions de cette suite, de sorte que l'on peut dire que les fonctions (1) forment un groupe relativement à l'équation $F(x) = 0$. De plus, au lieu de $\theta_i[\theta_i(x)]$, on écrit $\theta_i^2(x)$, et généralement $\theta_i[\theta_i^{n-1}(x)] = \theta_i^n(x)$.

Adjoignons une racine Z_0 de l'équation irréductible $\Phi(Z) = 0$, qui permet de décomposer $F(x) = 0$, et soient $f(x, Z_0)$ un facteur irréductible de $F(x)$ de degré μ, et

$$x_0, \quad \psi_1(x_0), \quad \ldots, \quad \psi_{\mu-1}(x_0) \tag{2}$$

ses μ racines. $\theta_i(x_0)$ étant une racine de $F(x) = 0$ non comprise dans la suite précédente,

$$\theta_i(x_0), \quad \theta_i\psi_1(x_0), \quad \ldots, \quad \theta_i\psi_{\mu-1}(x_0) \tag{3}$$

sont μ racines de $F(x) = 0$, dont toute fonction symétrique est aussi symétrique par rapport aux racines de l'équation

$$f(x, Z_0) = 0$$

et, par conséquent, peut s'exprimer rationnellement en fonction de Z_0. L'équation qui admet pour racines les μ quantités (3) est irréductible, car autrement on en déduirait un diviseur pour $f(x, Z_0)$. Les suites (2) et (3) sont distinctes; si elles ne contiennent pas toutes les racines de l'équation $F(x) = 0$, on formera une nouvelle suite de μ quantités, racines de $F(x) = 0$, et d'une équation à coefficients fonctions rationnelles de Z_0, irréductible, et ainsi de suite. Donc, après l'adjonction de Z_0, $F(x)$ se décompose en facteurs irréductibles d'égal degré, et ce degré, que nous avons désigné par μ, est un diviseur de m. Remarquons que les

μ fonctions

$$x, \quad \psi_1(x), \quad \psi_2(x), \quad \ldots, \quad \psi_{\mu-1}(x)$$

forment un groupe non seulement relativement à l'équation

$$f(x, Z_0) = 0,$$

mais aussi relativement à l'équation $F(x) = 0$; de même la suite (3) donne le groupe

$$x, \quad \theta_i\psi_1\theta_i^{-1}(x), \quad \ldots, \quad \theta_i\psi_{\mu-1}\theta_i^{-1}(x);$$

en effet, $\psi_i\psi_j(x_0)$ est une racine de $f(x, Z_0) = 0$ et, par suite, est égale à l'une des quantités (2), etc. Quant à la suite (3), si l'on pose $x_i = \theta_i(x_0)$, on a

$$x_0 = \theta_i^{-1}(x_i)$$

et elle coïncide avec la suite

$$x_i, \quad \theta_i\psi_1\theta_i^{-1}(x_i), \quad \ldots, \quad \theta_i\psi_{\mu-1}\theta_i^{-1}(x_i).$$

On aura ainsi un groupe pour chaque facteur de $F(x)$, après l'adjonction de Z_0; seulement il peut arriver que ces différents groupes de fonctions coïncident, comme nous le verrons plus loin, ou qu'elles aient toutes un certain nombre de fonctions communes.

9. Z_1 étant une autre racine de $\Phi(Z) = 0$, $f(x, Z_1)$ est irréductible comme $f(x, Z_0)$, et, si l'on désigne par x une racine de l'équation $f(x, Z_1) = 0$, les μ racines de cette équation seront

$$x_1, \quad \psi_1(x_1), \quad \psi_2(x_1), \quad \ldots, \quad \psi_{\mu-1}(x_1).$$

Si donc les équations $f(x, Z_1) = 0$ et $f(x, Z_0) = 0$ ont une racine commune, elles ont toutes leurs racines communes, et l'adjonction de Z_1 produit le même effet que l'adjonction de Z_0. Dans tous les cas, l'adjonction de Z_1 conduit aux mêmes groupes de fonctions relativement à l'équation $F(x) = 0$. Soient $Z_0, Z_1, Z_2, \ldots, Z_{N-1}$ les N racines de l'équation $\Phi(Z) = 0$; le produit

$$f(xZ_0)\, f(x, Z_1) \ldots f(x, Z_{N-1})$$

est égal à une puissance de $F(x)$. Si l'on désigne par q l'exposant de cette puissance, on peut partager les N fonctions $f(x, Z)$ en $\frac{N}{q}$ groupes de q fonctions égales entre elles. Soit a une quantité rationnelle ou, si l'on veut, un nombre rationnel, tel que $f(a, Z)$

prenne seulement q valeurs égales à $f(a, Z_0)$ lorsqu'on remplace Z successivement par N racines de $\Phi(z) = 0$; posons

$$f(a, Z_0) = z_0.$$

D'après le n° 6, z_0 est racine d'une équation irréductible de degré $\frac{N}{q}$ à coefficients rationnellement connus. L'adjonction de z_0 permet de décomposer $\Phi(Z)$; l'un de ses facteurs de degré q admet pour racines, en l'égalant à 0, les q valeurs de Z qui donnent à $f(a, Z)$ la valeur $f(a, Z_0)$, et les coefficients de $f(x, Z_0)$ s'expriment rationnellement en fonction de z_0. Si l'on remplace z_0 par les autres racines de l'équation en z, $\varphi(z) = 0$, on obtient les autres fonctions $f(x, Z_i)$. Posons $\frac{N}{q} = n$, on a $\mu n = m$.

Les racines de $\varphi(z) = 0$ sont fonctions rationnelles des racines de $F(x) = 0$ comme de celles de $\Phi(Z) = 0$. Désignons en effet par $f'(x, z_0)$ ce que devient $f(x, Z_0)$ lorsqu'on a exprimé ses coefficients en fonction de z_0. Les équations $f'(x_0, z) = 0$ et $\varphi(z) = 0$, x_0 désignant une racine de l'équation $f'(x, z_0) = 0$, ont une seule racine commune z_0, qu'on pourra obtenir pour les opérations qui donnent le plus grand commun diviseur de $f'(x_0, z)$ et de $\varphi(z)$.

10. Réciproquement, soient

$$x, \quad \psi_1(x), \quad \psi_2(x) \quad \ldots \quad \psi_{\mu-1}(x)$$

μ fonctions de la suite (1) formant un groupe relativement à l'équation $F(x) = 0$; x_0 étant une racine de $F(x) = 0$,

$$(\alpha) \qquad x_0, \quad \psi_1(x_0), \quad \psi_2(x_0), \quad \ldots, \quad \psi_{\mu-1}(x_0),$$

sont μ racines de cette équation; soit x_1 une racine de $F(x) = 0$ ne faisant pas partie de cette suite;

$$x_1, \quad \psi_1(x_1), \quad \psi_2(x_1), \quad \ldots, \quad \psi_{\mu-1}(x_1)$$

sont également μ racines de $F(x) = 0$: elles sont différentes des μ racines (α). En effet, si l'on avait $\psi_i(x_1) = \psi_j(x_0)$, on en déduirait $\psi_i^{-1}\psi_i(x_1) = x_1 = \psi_i^{-1}\psi_j(x_0)$, et par suite x_1 serait une des racines (α) contre l'hypothèse. Ainsi μ est un diviseur de m, degré de l'équation $F(x) = 0$. La fonction

$$(a - x)[a - \psi_1(x)][a - \psi_2(x)] \ldots [a - \psi_{\mu-1}(x)].$$

où a est une indéterminée rationnelle, acquiert $\frac{m}{\mu}$ valeurs distinctes lorsqu'on substitue successivement à x les diverses racines de l'équation $F(x) = 0$. Ces valeurs sont racines d'une équation irréductible à coefficients rationnels, et l'adjonction d'une racine de cette dernière équation décompose $F(x)$ en $\frac{m}{\mu}$ facteurs irréductibles de degré μ.

11. Supposons que l'équation $\Phi(Z) = 0$ soit elle-même holodrome; et soit, comme précédemment, $f(x, Z_0)$ un des facteurs irréductibles de $F(x)$, après l'adjonction de Z_0, racine de $\Phi(Z) = 0$. Si l'on désigne par $\theta(x_0)$ une racine de $F(x) = 0$ n'appartenant pas à $f(x, Z_0) = 0$, les μ quantités

$$\theta(x_0), \quad \psi_1\theta(x_0), \quad \psi_2\theta(x_0), \quad \ldots, \quad \psi_{\mu-1}\theta(x_0),$$

qui sont racines d'une équation de la forme $f(x, Z_1) = 0$, Z_1 étant une racine de $\Phi(Z) = 0$, et d'autre part les μ quantités

$$\theta(x_0), \quad \theta\psi_1(x_0), \quad \theta\psi_2(x_0) \quad \ldots, \quad \theta\psi_{\mu-1}(x_0)$$

sont racines d'équations à coefficients fonctions rationnelles de Z_0, puisque Z_1 est une fonction rationnelle de Z_0. Or, dans ces deux suites, il y a une quantité commune $\theta(x_0)$; elles sont donc les mêmes à l'ordre près; de sorte que les deux groupes de fonctions

$$\begin{array}{c} x, \quad \psi_1(x), \quad \psi_2(x), \quad \ldots, \quad \psi_{\mu-1}(x), \\ x, \quad \theta\psi_1\theta^{-1}(x), \quad \theta\psi_2\theta^{-1}(x), \quad \ldots, \quad \theta\psi_{\mu-1}\theta^{-1}(x), \end{array}$$

ne diffèrent que par l'ordre. Nous exprimerons cette propriété en disant que le premier groupe de fonctions est échangeable à la fonction θ, relativement à l'équation $F(x) = 0$. Ainsi :

Lorsqu'on adjoint à une équation holodrome $F(x) = 0$ *une racine d'une équation* $\Phi(Z) = 0$, *également holodrome, les groupes de fonctions correspondant aux divers facteurs irréductibles sont les mêmes; et ce groupe est permutable à toutes les fonctions* θ, *telles que* $F[\theta(x)] = 0$ *en même temps que* $F(x) = 0$.

Réciproquement, soient x, $\psi_1(x)$, $\psi_2(x)$, $\ldots$, $\psi_{\mu-1}(x)$, μ fonctions de la suite (1) formant un groupe relativement à l'équation $F(x) = 0$, échangeable à toutes les fonctions de cette suite (1),

a étant une indéterminée rationnelle, la fonction

$$(a-x)[a-\psi_1(x)][a-\psi_2(x)]\dots[a-\psi_{\mu-1}(x)]$$

acquiert $\frac{m}{\mu}$ valeurs distinctes lorsqu'on substitue à x les diverses racines de l'équation $F(x)=0$; l'équation qui admet ces $\frac{m}{\mu}$ valeurs pour racines est holodrome. En effet, soient

$$(a-x_0)[a-\psi_1(x_0)]\dots[a-\psi_{\mu-1}(x_0)]=z_0,$$
$$[a-\theta(x_0)][a-\psi_1\theta(x_0)]\dots[a-\psi_{\mu-1}\theta(x_0)]=z_1$$

deux des valeurs considérées, θ étant une des fonctions (1) autre que ψ. On a, puisque le groupe des fonctions ψ est permutable à toutes les fonctions de la suite (1),

$$z_1=[a-\theta(x_0)][a-\theta\psi_1(x_0)]\dots[a-\theta\psi_{\mu-1}(x_0)];$$

or toute fonction symétrique des μ quantités $x_0, \psi_1(x_0), \dots, \psi_{\mu-1}(x_0)$ est exprimable rationnellement en fonction de z_0 ; donc z_1, qui est aussi une fonction symétrique de ces μ quantités, d'après sa seconde forme, s'exprime rationnellement en fonction de z_0. On voit de plus que, lorsque l'équation $\Phi(Z)=0$ est holodrome, l'équation $\varphi(z)=0$, qui produit le même effet que $\Phi(Z)=0$ et qu'on formera comme il a été dit au n° 9, est aussi holodrome.

12. L'équation $\Phi(Z)=0$ n'étant pas holodrome, il peut se faire que l'équation $\varphi(z)=0$, qui produit le même effet, soit holodrome, et alors on retombe dans le cas précédent. Considérons le cas où l'équation $\varphi(z)=0$ n'est pas holodrome : z_0 et z_1 étant deux racines de $\varphi(z)=0$, l'adjonction de l'une ou de l'autre permet de décomposer $F(x)$ en facteurs d'égal degré μ ; soient $f(x, z_0)$ et $f_1(x, z_1)$, deux facteurs s'annulant pour une même valeur de x, x_0. Les racines de $f(x, z_0)=0$ étant

$$x_0,\quad \psi_1(x_0),\quad \psi_2(x_0),\quad \dots,\quad \psi_{\mu-1}(x_0),$$

celles de $f_1(x, z_1)=0$ pourront être représentées par

$$x_0,\quad \theta_1\psi_1\theta_1^{-1}(x_0),\quad \dots,\quad \theta_1\psi_{\mu-1}\theta_1^{-1}(x_0);$$

ces deux suites sont forcément distinctes, et il en est de même des groupes de fonctions qu'on obtient en remplaçant x_0 par une

variable x, en supposant que z_0 et z_1 ne puissent s'exprimer rationnellement en fonction l'une de l'autre.

Soit $f_i(x, z_i)$ le facteur de $F(x)$ qui s'annule pour x_0 lorsqu'on adjoint z_i et

$$x_0, \quad \theta_i\psi_1\theta_i^{-1}(x_0), \quad \ldots, \quad \theta_i\psi_{\mu-1}\theta_i^{-1}(x_0)$$

les μ racines de l'équation $f_i(x, z_i) = 0$. Remplaçant x_0 par une variable x, on a un groupe de fonctions correspondant à z_i; et par suite n groupes pour les n racines de $\varphi(z) = 0$. Le groupe correspondant à l'adjonction d'une racine de l'équation résolvante de $\varphi(z) = 0$ se compose des fonctions communes à tous ces groupes, lesquelles forment évidemment un groupe permutable à toutes les fonctions θ du n° 8. En effet, le plus grand commun diviseur des premiers membres des équations

$$f_0(x, z_0) = 0, \qquad f_1(x, z_1) = 0, \qquad \ldots, \qquad f_{n-1}(x, z_{n-1}) = 0,$$

est rationnel après l'adjonction d'une racine de l'équation résolvante de $\varphi(z) = 0$; soit $\chi(x)$ ce plus grand commun diviseur; z_i est une fonction rationnelle de x_0, invariable lorsqu'on remplace x_0 par les autres racines de $f(x, z_i) = 0$; il en résulte que la fonction résolvante de l'équation $\varphi(z) = 0$ est une fonction rationnelle de x_0, invariable lorsqu'on remplace x_0 par les diverses racines de $\chi(x) = 0$; $\chi(x)$ est donc irréductible (6).

13. Nous dirons que deux équations sont *équivalentes* lorsque les racines de l'une pourront s'exprimer rationnellement en fonction des racines de l'autre, qu'une équation holodrome est *simple* lorsqu'elle ne pourra se réduire qu'à l'aide d'une équation holodrome équivalente (CAMILLE JORDAN, *Théorie des substitutions et des équations algébriques*).

Il est clair que deux équations holodromes équivalentes sont de même degré. Étant données deux équations simples non équivalentes, l'adjonction des racines de l'une aux quantités connues laisse l'autre simple. Étant données trois équations simples non équivalentes deux à deux, il peut se faire que l'adjonction des racines de deux de ces équations réduise la troisième, mais les trois équations sont alors de même degré. En effet, adjoignons seulement les racines de l'une des équations, les deux autres restent simples; maintenant ces deux équations sont équivalentes, puisque

l'adjonction de l'une réduit l'autre; donc elles sont de même degré. Ainsi les trois équations sont de même degré deux à deux. Ce que nous venons de dire de trois équations simples peut se dire d'un nombre quelconque autre que deux d'équations simples.

14. Soit $F(x) = 0$ une équation holodrome de degré m et $\varphi(z) = 0$ une équation simple de degré ν, permettant de la réduire. Après l'adjonction d'une racine de $\varphi(z) = 0$, $F(x)$ se décomposera en ν équations holodromes et équivalentes de degré $\frac{m}{\nu}$. Il peut se faire que $F(x) = 0$ se réduise à l'aide d'autres équations simples, non équivalentes à $\varphi(z) = 0$; et que parmi elles il s'en trouve de degré ν; soit $\varphi_1(z) = 0$ l'une d'elles, et ainsi de suite. On arrivera à un certain nombre d'équations simples

$$(\alpha) \qquad \varphi(z) = 0, \quad \varphi_1(z) = 0, \quad \varphi_{\alpha-1}(z) = 0,$$

toutes de degré ν, permettant chacune de réduire $F(x) = 0$ et telles que l'une quelconque d'entre elles reste simple lorsqu'on adjoint aux quantités connues les racines de toutes les précédentes et que toute autre équation simple de degré ν permettant de réduire $F(x) = 0$ se réduise après l'adjonction des racines de ces α équations.

Au lieu de partir de $\varphi(z) = 0$, on pourrait partir de toute autre équation simple de degré ν, permettant de réduire $F(x) = 0$, et alors, en opérant comme plus haut, on arriverait à une autre suite

$$(\beta) \qquad \varphi'(z) = 0, \quad \varphi'_1(z) = 0, \quad \varphi'_2(z) = 0, \quad \varphi'_{\beta-1}(z) = 0,$$

jouissant des mêmes propriétés que la précédente. Les équations résolvantes des deux équations

$$(1) \qquad \varphi(z)\,\varphi_1(z)\,\varphi_2(z)\ldots\varphi_{\alpha-1}(z) = 0,$$

$$(2) \qquad \varphi'(z)\,\varphi'_1(z)\ldots\varphi'_{\beta-}(z) = 0$$

sont équivalentes. En effet, les racines de $\varphi'(z) = 0$ peuvent s'exprimer rationnellement en fonction des racines de l'équation (1); de même, celles de $\varphi'_1(z) = 0$, $\varphi'_2(z) = 0, \ldots, \varphi'_{\beta-1}(z) = 0$; réciproquement, les racines des équations $\varphi_1(z) = 0, \varphi_2(z) = 0, \ldots,$ $\varphi_{\alpha-1}(z) = 0$ s'expriment rationnellement en fonction des racines de l'équation (2). La résolvante de l'équation (1) est de degré ν^α. En effet, si l'on adjoint une racine de l'équation $\varphi_1(z) = 0$, ce

degré est divisé par ν, et il en est de même chaque fois que l'on adjoint une racine des équations (α). La résolvante de l'équation (2) est, pour la même raison, de degré $\nu\beta$. Ces deux résolvantes sont de même degré, puisqu'elles sont équivalentes; donc $\beta = \alpha$.

Il est clair que ce que nous venons de dire des équations simples à coefficients rationnels, réduisant $F(x) = 0$, de degré ν, peut se répéter, pour l'ensemble des équations, d'un autre degré quelconque.

15. Soit $\psi(z) = 0$ l'équation holodrome équivalente à l'ensemble des équations simples à coefficients rationnels, permettant de réduire $F(x) = 0$, telles qu'aucune d'elles ne puisse se réduire par l'adjonction des racines des autres, et que, de plus, toute autre équation simple, réduisant $F(x) = 0$, se réduise par l'adjonction d'une racine de $\varphi(z) = 0$. Le degré de $\psi(z)$ est égal au produit des degrés de ces équations simples. Nous appellerons ces équations, simples et à coefficients rationnels avant l'adjonction de toute irrationnelle, *équations simples du premier ordre;* et toute fonction rationnelle des racines de ces équations, *fonction algébrique du premier ordre.* De même nous appellerons *équations simples du second ordre et fonctions algébriques du second ordre* les équations simples dont les coefficients sont des fonctions algébriques du premier ordre, et les fonctions rationnelles des racines de ces équations; et, en général, *équations simples du* $\mu^{ième}$ *ordre et fonctions algébriques du* $\mu^{ième}$ *ordre* les équations simples dont les coefficients sont des fonctions algébriques du $(\mu - 1)^{ième}$ ordre, ou du moins ne sont holodromes qu'après l'adjonction de fonctions algébriques du $(\mu - 1)^{ième}$ ordre, et les fonctions rationnelles des racines de ces équations (voir *Algèbre supérieure* de M. Serret, t. II, n° 513).

m étant le degré de $F(x) = 0$, n celui de $\psi(z) = 0$,, z_0 une racine de $\psi(z) = 0$, après l'adjonction de z_0, $F(x) = 0$ se décompose en n équations holodromes équivalentes de degré $\frac{m}{n}$; soit $f(x, z_0) = 0$ l'une d'elles; le groupe de fonctions de $f(x, z_0) = 0$ est permutable au groupe de fonctions de $F(x) = 0$. Soit

$$\pi(\zeta, z_0) = 0$$

une équation holodrome et simple après l'adjonction de z_0, de

degré ν_1, et permettant de réduire $f(x, z_0) = 0$. Après l'adjonction d'une racine de l'équation $\pi(\zeta, z_0) = 0$, $f(x, z_0) = 0$ se décompose en ν_1 équations holodromes de degré $\frac{m}{n\nu_1}$ équivalentes, et le groupe de fonctions, qui est le même pour toutes ces équations, sera permutable à toutes les fonctions du groupe de

$$f(x, z_0) = 0,$$

mais en général il ne le sera pas à toutes les fonctions de groupe de $F(x) = 0$; z_1 étant une autre racine de $\psi(z) = 0$, $\pi(\zeta, z_1) = 0$ permettra de décomposer $f(x, z_1)$ (5); mais $f(x, z_1) = 0$ est équivalente à $f(x, z_0) = 0$; donc $\pi(\zeta, z_1) = 0$ est une autre équation simple après l'adjonction de z_0, permettant de décomposer $f(x, z_0)$, de sorte qu'il y aura un certain nombre de racines de

$$\psi(z) = 0 : z_0, z_1, z_2, \ldots, z_{\alpha'-1},$$

qui, substituées à z_0 dans $\pi(\zeta, z_0)$, donneront des équations simples permettant de réduire $f(x, z_0) = 0$, telles que l'une quelconque d'entre elles reste simple après l'adjonction des racines de toutes les autres, et que l'équation simple obtenue en substituant à z_0, dans $\pi(\zeta, z_0) = 0$, une autre racine de $\psi(z) = 0$ se réduise après l'adjonction de ces α' équations. Remarquons que α' peut être égal à 1; les coefficients de $\pi(\zeta, z_0)$ peuvent même être rationnels avant l'adjonction de z_0, mais l'équation $\pi(\zeta) = 0$ n'est holodrome qu'après l'adjonction de z_0.

Au lieu de partir de $\pi(\zeta, z_0) = 0$, on pourrait partir de toute autre équation simple obtenue en substituant à z_0 une autre racine de $\psi(z) = 0$; on arriverait à une autre suite $z'_0, z'_1, \ldots, z'_{\beta'-1}$. Mais, en raisonnant comme au numéro précédent, on voit que $\beta' = \alpha'$, et que l'ensemble des nouvelles équations est équivalent à l'ensemble des premières.

16. La résolvante de l'équation

$$\pi(\zeta, z_0), \quad \pi(\zeta, z_1), \quad \ldots, \quad \pi(\zeta, z_{\alpha'-1}) = 0$$

est de degré $\nu_1^{\alpha'}$, et l'adjonction d'une racine de cette équation résolvante permet de décomposer $f(x, z_0) = 0$ en $\nu_1^{\alpha'}$ équations équivalentes de degré $\frac{m}{n\nu_1^{\alpha'}}$. Soit $\Pi(\zeta, z_0) = 0$ cette équation résol-

vante. Si l'on remplace, dans les coefficients de cette équation, z_0 par une autre racine de $\psi(z) = 0$, l'équation nouvelle obtenue est holodrome et équivalente à la première. En substituant ainsi à z_0 les diverses racines de $\psi(z) = 0$, on obtient un certain nombre d'équations distinctes, c'est-à-dire n'ayant pas les mêmes racines, nombre qui est un diviseur de n, et peut d'ailleurs se réduire à l'unité; cette équation, dans le dernier cas, a pour coefficients des quantités rationnelles avant l'adjonction de z_0, mais n'est holodrome qu'après l'adjonction de z_0. Le produit des premiers membres de ces équations, qui est indépendant de l'irrationnelle z_0, donne, égalé à 0, une équation dont la résolvante, en ne considérant pas z_0 comme connue, mais seulement les irrationnelles primitives, est de degré $\nu_1^{\alpha'} n'$, n' étant un diviseur de n autre que 1. En effet, cette équation résolvante ne peut être décomposée qu'à l'aide des équations simples du premier ordre, qui décomposent $\psi(z) = 0$, et ses équations du second ordre sont $\pi(\zeta, z_0) = 0$, $\pi(\zeta, z_1) = 0, \ldots, \pi(\zeta, z_{\alpha'-1}) = 0$; $n' > 1$, car autrement $\Pi(\zeta, z_0) = 0$ serait à coefficients rationnels, et holodrome avant l'adjonction de z_0. Cette équation résolvante décompose $F(x) = 0$ en $\nu_1^{\alpha'} n'$ équations holodromes, équivalentes, qui ont même groupe de fonctions, et ce groupe est permutable à toutes les fonctions du groupe de $F(x) = 0$. Il en résulte qu'après l'adjonction d'une racine de $\Pi(\zeta, z_0) = 0$, $f(x, z_0) = 0$ se décompose en $\nu_1^{\alpha'}$ équations holodromes équivalentes, dont le groupe unique est permutable aux fonctions du groupe de $f(x, z_0) = 0$, mais encore à toutes les fonctions du groupe $F(x) = 0$. Ce que nous avons dit des équations simples du second ordre peut se répéter pour les équations des divers ordres.

Ainsi une équation holodrome $F(x) = 0$ se réduit à l'aide d'une suite d'équations simples; cette suite n'est pas entièrement déterminée, mais la suite des degrés de ces équations simples l'est, abstraction faite de l'ordre, et le produit de ces degrés est égal à celui de $F(x)$. Si l'on considère les groupes de fonctions des équations en lesquelles se décompose successivement $F(x) = 0$, chacun de ces groupes est contenu dans le précédent et échangeable à toutes ses fonctions (Camille Jordan, *Traité des substitutions*, p. 266 et suivantes).

III.

De la décomposition des équations.

17. Soit $f(x) = 0$ une équation irréductible non holodrome de degré m, et $F(V) = 0$ son équation résolvante. Cette équation résolvante se décompose en équations simples, comme il vient d'être dit. Parmi ces équations simples, quelques-unes réduiront $f(x) = 0$. Supposons que les premières, qui permettent de réduire $f(x) = 0$, appartiennent au $\mu^{\text{ième}}$ ordre, de sorte que l'ensemble des équations simples d'ordre inférieur laissent $f(x) = 0$ irréductible; soit $F_1(v) = 0$ l'équation holodrome équivalente à l'ensemble de ces équations simples, v_0 une de ses racines et $\pi(z, v_0) = 0$ une équation simple de degré ν, permettant de réduire $f(x) = 0$. Après l'adjonction d'une racine z_0 de cette équation, $f(x)$ se décompose en facteurs d'égal degré. En effet, soit $\varphi(x, z_0)$ un facteur irréductible de $f(x)$; $\varphi(x, z_1)$, $\varphi(x, z_2)$, ..., $\varphi(x, z_{\nu-1})$ sont également irréductibles et diviseurs de $f(x)$ (5); leur produit est donc une puissance de $f(x)$. D'ailleurs, z_i étant une fonction rationnelle de z_0, les équations

$$\varphi(x, z_0) = 0 \qquad \text{et} \qquad \varphi(x, z_i) = 0$$

n'ont pas de racine commune ou ont toutes leurs racines communes. Ainsi, après l'adjonction de z_0, les facteurs en lesquels se décompose $f(x)$ sont compris dans la suite $\varphi(x, z_0)$, $\varphi(x, z_1)$, ..., $\varphi(x, z_{\nu-1})$. Le nombre de ces facteurs est un diviseur de m, degré de $f(x)$ et de ν; soit n ce nombre; le degré de $\varphi(x, z_0)$ est $\frac{m}{n}$. Les autres équations simples, obtenues en substituant à v_0, dans les coefficients de l'équation $\pi(z, v_0) = 0$, une autre racine de $F_1(v) = 0$, décomposent $f(x) = 0$ d'une manière analogue. Soient $v_0, v_1, \ldots, v_{\alpha-1}$ les racines de $F_1(v) = 0$, donnant, comme au n° 15, une suite d'équations simples

$$\pi(z, v_0) = 0, \qquad \pi(z, v_1) = 0, \qquad \pi(z, v_2) = 0, \qquad \ldots, \qquad \pi(z, v_{\alpha-1}) = 0,$$

telles que l'une quelconque reste simple après l'adjonction des racines de toutes les autres, et que toutes les équations simples $\pi(z, v_i) = 0$, v_i étant une racine de $F_1(v) = 0$, se réduisent après l'adjonction des racines de ces α équations simples. Chacune de ces

équations simples divisera par n le degré de $f(x)$, et leur ensemble par n^α.

Deux cas peuvent se présenter; n^α est égal à m ou bien lui est inférieur. Dans le premier cas, l'équation $f(x) = 0$ est dite *primitive;* $F(V) = 0$ est alors équivalente à l'ensemble des équations

$$F_1(v) = 0, \qquad \pi(z, v_0)\,\pi(z, v_1).\pi(z, v_2)\ldots\pi(z, v_{\alpha-1}) = 0.$$

Si n^α n'est pas égal à m, soit $F_2(v') = 0$ l'équation holodrome à coefficients rationnels avant l'adjonction de toute irrationnelle, autre que celles qui entrent dans les coefficients de $f(x) = 0$, équivalente à $F_1(v) = 0$ et $\pi(z, v_0)\,\pi(z, v_1)\ldots\pi(z, v_{\alpha-1}) = 0$. Après l'adjonction d'une racine v'_0 de $F_2(v') = 0$, $f(x) = 0$ se décompose en n^α équations d'égal degré, et l'on pourra former une équation à coefficients rationnels

$$y^{n^\alpha} + A_1 y^{n^\alpha - 1} \ldots = 0,$$

telle que

$$f(x) = [M(y_1)x^{m'} + \ldots][M(y_2)x^{m'} + \ldots][\ldots]\ldots,$$

$m' = \frac{m}{n^\alpha}$, et $y_1, y_2, \ldots, y_{n^\alpha}$ étant les racines de l'équation en y.

Ainsi une équation qui n'est pas primitive peut se ramener à un certain nombre d'équations primitives, et le produit des degrés de ces équations est égal au degré de l'équation proposée.

18. Lorsque le degré d'une équation holodrome est un nombre premier p, cette équation est évidemment simple, et l'on peut représenter ses racines par

$$x, \quad \theta(x), \quad \theta^2(x), \quad \ldots, \quad \theta^{p-1}(x),$$

x étant l'une d'elles et θ une fonction rationnelle. Abel a montré que, dans ce cas, on peut exprimer les racines de l'équation à l'aide de radicaux (Serret, *Algèbre supérieure*, Sect. V, Chap. III). Réciproquement, lorsqu'une équation est soluble par radicaux, ses équations simples sont toutes de degré premier; en effet, l'équation $y^p - A = 0$ devient abélienne après l'adjonction des racines de l'équation $\frac{x^p - 1}{x - 1} = 0$, qui est abélienne.

D'après ce qui précède, lorsqu'une équation de degré premier est soluble par radicaux, elle est susceptible de devenir abélienne.

Cette condition est suffisante. Soit $f(x) = 0$ une équation de degré m, premier ou non, irréductible et non abélienne actuellement, et qui devienne abélienne après l'adjonction de certaines irrationnelles qui la laissent irréductible. Quel que soit le nombre des irrationnelles adjointes, on peut les exprimer toutes en fonctions rationnelles d'unè racine d'une équation holodrome; soient $F(z) = 0$ cette équation holodrome et z_0 une de ses racines. x_0 étant une racine de $f(x) = 0$, les autres, par hypothèse, peuvent être représentées par

$$\psi(z_0, x_0), \quad \psi^2(z_0, x_0), \quad \ldots, \quad \psi^{m-1}(z_0, x_0),$$

ψ étant une fonction rationnelle de x_0 et de z_0, et $\psi^2(z_0, x_0)$ représentant $\psi[z_0, \psi(z_0, x_0)]$, et ainsi des autres. Soit $\chi_i(z_0)$, χ_i étant une fonction rationnelle, une autre racine de $F(z_0) = 0$; $\psi[\chi_i(z_0), x_0]$ est aussi racine de $f(x) = 0$; par conséquent, cette quantité est égale à l'un des termes de la suite précédente $\psi^i(z_0, x_0)$. On a

$$\psi[\chi_i(z_0), x_0] = \psi^i(z_0, x_0),$$

d'où

$$\psi[\chi_i^2(z_0), x_0] = \psi^i[\chi_i(z_0), x_0] = \psi^{i^2}(z_0, x_0)$$

et, d'une manière générale,

$$\psi[\chi_i^k(z_0), x_0] = \psi^{i^k}(z_0, x_0).$$

Soit e le nombre de termes distincts compris dans la suite

$$z_0, \quad \chi_i(z_0), \quad \chi_i^2(z_0), \quad \ldots,$$

d'après ce qui précède

$$\psi^{i^e}(z_0, x_0) = \psi(z_0, x_0),$$

d'où $i^e \equiv 1 \pmod{m}$; ce qui exige que i soit un nombre premier avec m. Ainsi, lorsqu'on remplace, dans $\psi(z_0, x_0)$, z_0 par les diverses racines de $F(z) = 0$, on obtient un nombre ν de valeurs distinctes au plus égal à $\varphi(m)$, nombre des entiers inférieurs à m et premiers avec m. Il en sera de même lorsqu'on remplacera x_0 par une indéterminée rationnelle a; les ν valeurs qu'on obtient alors sont racines d'une équation irréductible, et les coefficients des diverses puissances de x_0, dans $\psi(z_0, x_0)$, peuvent s'exprimer

rationnellement en fonction de $\psi(z_0, a)$. D'ailleurs, comme on a

$$\psi[\chi_i(z_0), x_0] = \psi^i(z_0, x_0),$$

on voit que $\psi[\chi_i(z_0), a]$ pourra s'exprimer rationnellement en fonction de $\psi(z_0, a)$.

Ainsi l'équation qui a pour racines ces ν valeurs distinctes est holodrome, et l'on peut prendre, pour $F(z) = 0$, une équation de degré ν.

Soient $\chi_j(z_0)$ une racine autre que $\chi_i(z_0)$ de l'équation

$$F(z) = 0 \qquad \text{et} \qquad \psi[\chi_j(z_0), x_0] = \psi^j(z_0, x_0);$$

il viendra

$$\psi[\chi_j\chi_i(z_0), x_0] = \psi^j[\chi_i(z_0), x_0] = \psi^{ji}(z_0, x_0);$$

de même

$$\psi[\chi_i\chi_j(z_0), x_0] = \psi^i[\chi_j(z_0), x_0] = \psi^{ij}(z_0, x_0);$$

d'où

$$\chi_i\chi_j(z_0) = \chi_j\chi_i(z_0).$$

Les fonctions χ_i, χ_j sont donc échangeables entre elles, et l'équation $F(z) = 0$ est résoluble algébriquement d'après un théorème d'Abel. De plus les ν nombres, tels que i, j, forment un groupe relativement au module m, c'est-à-dire que le produit de deux quelconques d'entre eux est congru à l'un des termes de cette suite, suivant le module m, et ν est par suite un diviseur de $\varphi(m)$. Le degré de l'équation résolvante de $f(x) = 0$ est égal à $m\nu$. Lorsque m est premier, $\varphi(m)$ est égal à $m - 1$, et l'équation $F(z) = 0$ est abélienne, puisque les nombres i, j sont les diverses puissances de l'un d'entre eux convenablement choisi; on en déduit que, deux racines d'une telle équation étant données, les autres s'en déduisent rationnellement. Ces théorèmes ont été établis, pour la première fois, par Gallois, dans son célèbre Mémoire, paru en 1846 dans le tome XI du *Journal de Liouville*.

19. Nous sommes ainsi arrivés aux théorèmes généraux de la théorie algébrique des équations, indépendamment de la théorie des substitutions. Comme l'a démontré Galois, cette dernière est corrélative de la théorie des équations; mais la méthode que nous avons suivie peut, dans certains cas, être plus simple ou pré-

senter, sous un jour nouveau, les propositions de la théorie des substitutions.

Reprenons les notations du n° 7. Soit $f(x) = 0$ une équation de degré m, n'ayant pas de racines égales; désignons par V_0 une fonction résolvante de cette équation, et par $F(V) = 0$ son équation résolvante de degré N. Les racines de l'équation $f(x) = 0$ sont des fonctions rationnelles de V_0; soient

$$x_0 = \psi_0(V_0), \quad x_1 = \psi_1(V_0), \quad x_2 = \psi_2(V_0), \quad \ldots, \quad x_{n-1} = \psi_{n-1}(V_0).$$

$V_0, V_1, V_2, \ldots, V_{N-1}$ étant les diverses racines de $F(V) = 0$,

$$\psi_0(V_i), \quad \psi_1(V_i), \quad \ldots, \quad \psi_{n-1}(V_i)$$

représentent, dans un certain ordre, les m racines de l'équation $f(x) = 0$; en donnant à i successivement les valeurs 0, 1, 2, ..., N — 1, on obtient donc N permutations entre les racines; les substitutions, pour passer de l'une d'elles à toutes les autres, forment un groupe de substitutions conjuguées.

Soit maintenant $z_0 = \Pi(x_0, x_1, \ldots, x_{m-1})$ une fonction rationnelle des m racines de l'équation $f(x) = 0$; remplaçant les x par leurs valeurs en fonction de V_0, on aura

$$z_0 = \Pi_1(V_0).$$

La substitution à V, dans $\Pi_1(V)$, des diverses racines de $F(V) = 0$, revient à effectuer, dans la fonction

$$\Pi(x_0, x_1, x_2, \ldots, x_{m-1}),$$

les diverses substitutions de ce groupe. Ainsi, en appelant ce groupe le *groupe conjugué propre à l'équation* $f(x) = 0$, comme c'est l'usage, on a le théorème suivant :

Si, dans une fonction $\Pi(x_0, x_1, \ldots, x_{m-1})$ *des racines d'une équation* $f(x) = 0$, *n'ayant pas de racines égales, on effectue les diverses substitutions du groupe conjugué propre à l'équation, les valeurs distinctes qu'acquiert la fonction sont racines d'une équation irréductible;* l'adjonction d'une de ces valeurs aux quantités connues réduit le groupe de substitutions propres à l'équation à celles du groupe primitif, qui laissent invariable la fonction

$$\Pi(x_0, x_1, \ldots, x_{m-1}).$$

Lorsque l'équation $f(x) = 0$ est primitive, elle n'est réduite que par les équations simples de $F(V) = 0$ d'ordre le plus élevé. Soient $F_1(v) = 0$ l'équation holodrome équivalente à l'ensemble des équations simples d'ordre inférieur, v_0 une de ses racines; après l'adjonction de v_0, $F(V) = 0$ se décompose en équations équivalentes; soit $F_2(V, v_0) = 0$ l'une d'elles, et

$$\pi(z, v_0) = 0$$

une équation simple réduisant l'équation précédente; les autres équations simples de $F_2(V, v_0) = 0$ s'obtiendront en substituant à v_0 dans les coefficients de $\pi(z, v_0) = 0$ les autres racines de $F_1(v) = 0$; et toutes ces équations simples réduiront $f(x) = 0$; de plus, le groupe de fonctions de $F_2(V, v_0) = 0$ est permutable aux fonctions du groupe de $F(V) = 0$. Le degré de $F_2(V, v_0) = 0$ est égal au produit des degrés des équations

$$\pi(z, v_0) = 0, \qquad \pi(z, v_1) = 0, \qquad \pi(z, v_{\alpha-1}) = 0,$$

telles que l'une quelconque reste simple après l'adjonction des racines de toutes les autres, et que toutes les équations simples $\pi(z, v_i) = 0$, v_i étant une racine de $F_1(v) = 0$, se réduisent après l'adjonction des racines de ces α équations simples.

Dans le cas où $f(x) = 0$ est l'équation générale de degré m, son groupe est formé de toutes les substitutions possibles entre ses m racines, N est égal à 1, 2, 3, ..., m. Or, si m est supérieur à 4, tout groupe auquel toute substitution est permutable contient le groupe alterné (C. Jordan, *Traité des substitutions*, p. 63). Donc si $m > 4$, le degré de $F_1(v)$ est égal à 2, et l'on peut prendre

$$F_1(v) = v^2 - \Delta,$$

Δ étant le dernier terme de l'équation aux carrés des différences des racines; $F_2(V, v_0) = 0$ est de degré $\frac{1.2.3...m}{2}$; ses équations simples distinctes ne peuvent être qu'au nombre de deux,

$$\pi(z, v_0) = 0 \qquad \text{et} \qquad \pi(z, -v_0) = 0;$$

mais $\frac{1.2.3...m}{2}$ n'étant pas un carré parfait, ces deux équations sont équivalentes et l'équation $F_2(V, v_0) = 0$ est simple (C. Jordan, *loc. cit.*, p. 66).

IV.

De la division du cercle en parties égales.

20. Les racines primitives de l'équation $x^m - 1 = 0$, c'est-à-dire celles dont les diverses puissances reproduisent toutes les autres, sont au nombre de $\varphi(m)$, nombre des entiers inférieurs à m et premiers avec m; Gauss a montré que l'équation de degré $\varphi(m)$ qui admet pour racines ces racines primitives est irréductible, lorsque m est une puissance d'un nombre premier; Kronecker a démontré la même proposition pour le cas de m quelconque. Soit $f(x) = 0$ cette équation; q étant un diviseur de $\varphi(m)$, on peut former une équation de degré q permettant de décomposer $f(x)$ en q facteurs d'égal degré $\frac{\varphi(m)}{q}$. Lorsque m est une puissance d'un nombre premier autre que 2, la congruence $x^{\varphi(m)} - 1 \equiv 0 \pmod m$ admet des racines primitives, l'équation $f(x) = 0$ est abélienne, et il n'y a qu'une équation de degré q permettant de la décomposer en q facteurs d'égal degré. Gauss a donné cette équation dans le cas où m est un nombre premier pour q égal à 2, 3 et 4. Nous allons établir les résultats de Gauss, en suivant une marche différente qui simplifie les calculs.

Soient g une racine primitive du module premier p, q un diviseur de $p - 1$, et $\omega = \frac{p-1}{q}$; considérons la congruence

$$g^{\alpha+xq} + g^{\beta+yq} + 1 \equiv 0 \pmod p. \tag{1}$$

Nous désignerons par $n_{\alpha,\beta}$ le nombre de systèmes distincts suivant le module p de g^{xq} et g^{yq} satisfaisant à cette congruence. On a $g^{x'q} \equiv g^{xq} \pmod p$, si $x' - x$ est divisible par ω, et $n_{\alpha,\beta} = n_{\alpha',\beta'}$, si les nombres α', β' sont respectivement congrus à α, β suivant le module q; ainsi nous supposerons les nombres x et y réduits suivant le module ω, et les nombres α et β suivant le module q. Enfin on voit immédiatement que $n_{\alpha,\beta} = n_{\beta,\alpha}$.

La congruence (1) peut s'écrire des deux autres manières

$$g^{\alpha-\beta+xq} + g^{-\beta+yq} + 1 \equiv 0, \qquad g^{\beta-\alpha+xq} + g^{-\alpha+yq} + 1 \equiv 0 \pmod p;$$

d'où les relations

$$n_{\alpha,\beta} = n_{\beta,\alpha} = n_{\alpha-\beta,-\beta} = n_{\beta-\alpha,-\alpha}.$$

Donnons à x et y les ω^2 systèmes de valeurs dont ces nombres sont susceptibles dans la somme $g^{\alpha+xq} + g^{\beta+yq}$; cette somme prendra $\omega n_{\alpha-\delta,\beta-\delta}$ valeurs de la forme $-g^{\delta+zq} \pmod p$ et s'annulera ω fois $\pmod p$ si la congruence

$$\alpha - \beta + xq \equiv \frac{\omega q}{2} \pmod\omega$$

a une solution; dans le cas où cette dernière congruence n'a pas de solution, la somme $g^{\alpha+xq} + g^{\beta+yq}$ ne peut s'annuler $\pmod p$. Donc, si ω est pair, on a

$$1 + \sum_{\alpha=0}^{\alpha=q-1} n_{\alpha,\alpha} = \omega, \qquad \sum_{\alpha=0}^{\alpha=q-1} n_{\alpha,\alpha+\beta} = \omega,$$

β désignant un nombre non divisible par q; et, si ω est un nombre impair,

$$1 + \sum_{\alpha=0}^{\alpha=q-1} n_{\alpha,\alpha+\frac{q}{2}} = \omega, \qquad \sum_{\alpha=0}^{\alpha=q-1} n_{\alpha,\alpha+\beta} = \omega,$$

β désignant un nombre non congru à $\frac{q}{2} \pmod q$.

Des relations qui viennent d'être établies, on peut déduire les nombres $n_{\alpha,\beta}$ pour q égal à 2. En effet, on a alors, que ω soit pair ou impair, $n_{01} = n_{11}$ et, si ω est pair,

$$1 + n_{00} + n_{11} = \frac{p-1}{2}, \qquad 2n_{11} = \frac{p-1}{2};$$

d'où

$$n_{00} = \frac{p-5}{4}, \qquad n_{11} = n_{01} = \frac{p-1}{4}.$$

Si ω est impair,

$$n_{00} + n_{11} = \frac{p-1}{2}, \qquad 1 + 2n_{11} = \frac{p-1}{2};$$

d'où

$$n_{00} = \frac{p+1}{4}, \qquad n_{11} = n_{01} = \frac{p-3}{4}$$

Pour q égal à 4, on obtient entre les nombres $n_{\alpha,\alpha}$ une relation

qui nous sera utile. On a, si $\frac{p-1}{4}$ est pair,

$$1 + n_{00} + n_{11} + n_{22} + n_{33} = \frac{p-1}{4},$$

$$n_{33} + 2n_{12} + n_{11} = \frac{p-1}{4},$$

$$2n_{22} + 2n_{12} = \frac{p-1}{4};$$

les deux dernières donnent $2n_{22} = n_{11} + n_{33}$.

Si $\frac{p-1}{4}$ est impair,

$$n_{00} + n_{11} + n_{22} + n_{33} = \frac{p-1}{4},$$

$$n_{33} + 2n_{12} + n_{11} = \frac{p-1}{4},$$

$$1 + 2n_{22} + 2n_{12} = \frac{p-1}{4};$$

et, comme dans le cas précédent, on déduit

$$1 + 2n_{22} = n_{11} + n_{33}.$$

Le nombre des systèmes de solutions de la congruence quadrinôme $g^{\alpha+xq} + g^{\beta+yq} + g^{\gamma+zq} + 1 \equiv 0 \pmod{p}$ peut s'exprimer à l'aide des nombres $n_{\alpha,\beta}$ et, dans certains cas, de plusieurs manières; ce qui conduit à des équations du second degré entre les nombres positifs $n_{\alpha,\beta}$. C'est de ces relations que Gauss a déduit ces nombres $n_{\alpha,\beta}$, dans les cas de $q = 3$ et de $q = 4$; mais nous trouverons des relations analogues dans l'étude de l'équation $x^p - 1 = 0$.

21. Soit θ une racine autre que 1 de l'équation $x^p - 1 = 0$; la somme

$$\sum_{i_1=0}^{i_1=\omega-1} \theta g^{i_1 q},$$

où ω désigne le rapport $\frac{p-1}{q}$, acquiert q valeurs distinctes lorsqu'on substitue à θ les diverses racines de $\frac{x^p-1}{x-1} = 0$; on les obtient en donnant à i les valeurs 0, 1, 2, ..., $q-1$ dans l'expres-

sion

$$s_i = \sum_{i_1=0}^{i_1=\omega-1} \theta g^{i+i_1 q}.$$

L'équation de degré q, qui a pour racines les quantités s_i, est abélienne, et elle permet de décomposer $\frac{x^p - 1}{x - 1}$ en q facteurs de degré ω. Les quantités s_i ont été désignées sous le nom de *périodes des racines d'ordre p de l'unité*. Nous désignerons par S_k la somme

$$\sum_{i=0}^{i=q-1} s_i^k;$$

on a

$$S_1 = -1.$$

La $k^{\text{ième}}$ puissance de s_i est égale à

$$\Sigma \theta g^{i(g^{i_1 q} + g^{i_2 q} + \ldots + g^{i_k q})},$$

le signe Σ s'étendant aux ω^k termes qu'on obtient en donnant à chacun des nombres $i_1, i_2, \ldots, i_k$ les ω valeurs $0, 1, 2, \ldots, \omega - 1$. D'après cela, soient ωN_k le nombre de fois que la somme

$$\sigma = g^{i_1 q} + g^{i_2 q} + \ldots + g^{i_k q}$$

s'annule suivant le module p; ωN_{kj} le nombre des valeurs de σ satisfaisant à la congruence $x^\omega - g^{j\omega} \equiv 0 \pmod p$, c'est-à-dire pouvant se mettre sous la forme $g^{j+lq} \pmod p$; on a

$$s_i^k = \omega N_k + N_{k0} s_i + N_{k1} s_{i+1} + \ldots + N_{k,q-1} s_{i+q-1},$$

d'où

$$S_k = q\omega N_{k1} + S(N_{k0} + N_{k1} + \ldots + N_{k,q-1}).$$

Mais on a évidemment

$$N_k + N_{k0} + N_{k1} + \ldots + N_{k,q-1} = \omega^{k-1};$$

donc

$$S_k = (\omega q + 1) N_k - \omega^{k-1} = p N_k - \omega^{k-1},$$

en se rappelant que $S_1 = -1$.

Soit

$$x^q + P_1 x^{q-1} + P_2 x^{q-2} + \ldots + P_q = 0$$

l'équation aux q périodes. Les formules de Newton donnent

$$S_k + P_1 S_{k-1} + P_2 S_{k-2} + \ldots + k P_k = 0,$$

si k est égal ou plus petit que q; et

$$S_k + P_1 S_{k-1} + P_2 S_{k-2} + \ldots + P_q S_{k-q} = 0,$$

si k est plus grand que q. Les premières déterminent les coefficients $P_1, P_2, \ldots, P_q$ en fonction de $S_1, S_2, \ldots, S_q$; les dernières donnent des relations entre les nombres entiers S_k, qu'on peut exprimer en fonction des nombres $n_{\alpha,\beta}$ du numéro précédent.

22. Nous considérerons d'abord le cas de ω pair.

Alors on a

$$N_2 = 1, \qquad N_{2,\alpha} = n_{-\alpha,-\alpha};$$

pour abréger, nous poserons $N_{2\alpha} = n_\alpha$; N_3 est égal à $N_{20} = n_0$, et enfin on voit facilement que

$$N_4 = N_{30} = \omega + \sum_{i=0}^{i=q-1} n_i^2.$$

On a, par suite

$$P_1 = 1, \qquad P_2 = -\frac{(q-1)\omega}{2}, \qquad P_3 = \frac{-p(n_0+1)+\omega^2}{3} - \frac{p-3\omega-1}{6};$$

ce qui donne

$$x^2 + x + \frac{1-p}{4} = 0$$

pour l'équation aux deux périodes; et

$$x^3 + x^2\,\frac{p-1}{3}\,x - \frac{p(n_0+1)-\omega^2}{3} = 0$$

pour l'équation aux trois périodes.

Le nombre n_0 est inconnu dans la dernière équation; mais on a la relation

$$S_4 + P_1 S_3 + P_2 S_2 - P_3 = 0;$$

substituant aux lettres S et P leurs valeurs en fonction des nombres n_0, n_1, n_2, il vient

$$3(n_0^2 + n_1^2 + n_2^2) + 4 n_0 - \omega^2 + 1 = 0;$$

et l'on a déjà

$$1 + n_0 + n_1 + n_2 = \omega = \frac{p-1}{3}.$$

Ces deux équations suffisent pour déterminer les trois nombres n, qui doivent être positifs. Posons

$$n_1 - n_2 = \nu,$$

d'où

$$n_1^2 + n_2^2 = \frac{(\omega - 1 - n_0)^2 + \nu^2}{2};$$

la première devient

$$9n_0^2 - 2(3\omega - 7)n_0 + 3\nu^2 + \omega^2 - 6\omega + 5 = 0,$$

équation qui, multipliée par q, se met sous la forme

$$27\nu^2 + (9n_0 - 3\omega + 7)^2 = 4p.$$

Posons

$$9n_0 - 3\omega + 7 = \mathrm{L};$$

les deux conditions

$$\mathrm{L} \equiv 1 \pmod 3, \qquad 27\nu^2 + \mathrm{L}^2 = 4p$$

déterminent L et, par suite, n_0; n_1, n_2 peuvent se permuter entre eux, en changeant la racine primitive prise pour g. L'équation aux trois périodes devient, en faisant $3x + 1 = y$,

$$y^3 - 3py - p\mathrm{L} = 0.$$

23. Nous supposons toujours ω pair. Les q périodes s_i sont réelles; en effet on a

$$s_i = \sum_{i_1=0}^{i_1=\omega-1} \theta g^{i+i_1 q} = \sum_{i_1=0}^{i_1=\frac{\omega}{2}-1} \left[\theta g^{i+i_1 q} + \theta^{-g^{i+i_1 q}}\right],$$

en remarquant que $g^{\frac{\omega q}{2}} \equiv -1 \pmod p$; et la quantité entre crochets, somme de quantités imaginaires conjuguées, est réelle. Par suite

$$s_2^2 > s_1 > \frac{s_2^2}{q},$$

ou, en remplaçant S_2 par $p - \omega$ et S_4 par $pN_4 - \omega^3$,

$$\frac{\omega^3 + (p-\omega)^2}{p} > N_4 > \frac{\omega^3}{q} + \frac{(p-\omega)^2}{qp}.$$

Mais N_4 est égal à

$$\omega + \sum_{i=0}^{i=q-1} n_i^2;$$

donc

$$\frac{(p-\omega)^2(q-1)}{pq} + \frac{(\omega-1)^2}{q} > \sum_{i=0}^{i=q-1} n_i^2 > \frac{(\omega-1)^2}{q},$$

et l'on a

$$\Sigma n_i = \omega - 1.$$

Désignons par ν le plus petit des nombres n_i; alors la somme des carrés des $q-1$ autres est égale ou supérieure à $\frac{(\omega-1-\nu)^2}{q-1}$; donc

$$\frac{(p-\omega)^2(q-1)}{pq} + \frac{(\omega-1)^2}{q} \geq \frac{(\omega-1-\nu)^2}{q-1} + \nu^2,$$

inégalité qui peut s'écrire

$$\frac{(p-\omega)^2(q-1)}{pq} \geq \left(\frac{\omega-1}{q} - \nu\right)^2,$$

et, comme ν est inférieur à $\frac{\omega-1}{q}$,

$$\nu \geq \frac{\omega-1}{q} - \frac{(p-\omega)(q-1)}{\sqrt{pq}}.$$

Les nombres n_i sont inférieurs à $\omega - 1 - (q-1)\nu$, ou, en remplaçant ν par sa valeur,

$$\frac{\omega-1}{q} + \frac{(p-\omega)(q-1)^2}{\sqrt{pq}} \geq n_i \geq \frac{\omega-1}{q} - \frac{(p-\omega)(q-1)}{\sqrt{pq}}.$$

Le nombre n_i représente le nombre des systèmes de solutions de la congruence

$$g^{-i}(x^q + y^q) + 1 \equiv 0 \pmod{p = q\omega + 1},$$

pour lesquels aucun des deux nombres x, y n'est divisible par p.

Lorsqu'on remplace ω par les nombres pairs successifs dans l'expression $\omega q + 1$, on obtient une infinité de nombres premiers: d'après les inégalités que nous venons d'établir pour tous ces nombres premiers correspondant aux valeurs de ω supérieures à une certaine limite, la congruence

$$x^q + y^q \equiv z^q \pmod{p = q\omega + 1}$$

admet des systèmes de solutions pour lesquels aucun des nombres x, y, z n'est divisible par p. Si le contraire avait lieu, l'impossibilité de résoudre en nombres entiers l'équation $x^q + y^q = z^q$, impossibilité annoncée par Fermat, serait démontrée, puisque l'un des nombres x, y ou z devrait être divisible par une infinité de nombres premiers. Pour q égal à 3 ou 4, la proposition que nous venons d'établir résulte immédiatement de l'équation aux trois et aux quatre périodes, comme l'a remarqué Libri [*Mémoire sur la théorie des nombres* (*Journal de Crelle*, t. 9), rappelé par le P. Pepin (*Comptes rendus*, 1880, 2e semestre)].

24. Lorsque ω est impair, q est forcément pair. On a

$$N_2 = 0, \qquad N_{2\alpha} = n_{\frac{q}{2}-\alpha, \frac{q}{2}-\alpha};$$

nous poserons, pour abréger l'écriture,

$$N_{2\alpha} = n_\alpha, \qquad N_3 = n_{\frac{q}{2}}, \qquad N_4 = N_{3, \frac{q}{2}} = 2 \sum_{i=0}^{i=\frac{q}{2}-1} n_i n_{\frac{q}{2}+i}.$$

Par suite

$$S_1 = -1, \qquad S_2 = -\omega, \qquad S_3 = p n_{\frac{q}{2}} - \omega^2;$$

d'où

$$P_1 = 1 \qquad P_2 = \frac{\omega + 1}{2}, \qquad P_3 = -\frac{2p n_{\frac{q}{2}} - (\omega+1)(2\omega+1)}{6}.$$

Ainsi, pour q égal à 2, on a, pour l'équation aux deux périodes, si $\frac{p-1}{2}$ est impair,

$$x^2 + x + \frac{1+p}{4} = 0.$$

La méthode que nous venons d'exposer ne suppose pas le nombre q premier; les formules s'appliquent donc au cas où q est un nombre composé; mais alors il y a en outre des relations qui simplifient les calculs.

25. Soit $q = 4$. On a

$$s_i^2 = \varepsilon\omega + n_0 s_i + n_1 s_{i+1} + n_2 s_{i+2} + n_3 s_{i+3},$$

ε représentant 1 ou 0, suivant que $\frac{p-1}{4} = \omega$ est pair ou impair. Dans les deux cas, $s_0 + s_2$, $s_1 + s_3$ sont les deux racines de l'équation aux deux périodes

$$y^2 + y + \frac{1-p}{4} = 0.$$

Or

$$s_0^2 + s_2^2 = 2\varepsilon\omega + (n_0 + n_2)y_0 + (n_1 + n_3)y_1,$$
$$s_1^2 + s_3^2 = 2\varepsilon\omega + (n_0 + n_2)y_1 + (n_1 + n_3)y_0,$$
$$s_0 s_2 = \frac{(s_0 + s_2)^2 - s_0^2 - s_2^2}{3} = \frac{\omega(1 - 2\varepsilon) - (n_0 + n_2 + 1)y_0 - (n_1 + n_3)y_1}{2};$$

ainsi il sera facile de former l'équation ayant pour racines s_0, s_2, connaissant n_0, n_1, n_2, n_3.

Des équations écrites plus haut, on déduit

$$s_0^2 - s_2^2 = (n_0 - n_2)(s_0 - s_2) + (n_1 - n_3)(s_1 - s_3),$$

ou

$$(n_0 - n_2 - y_0)(s_0 - s_2) + (n_1 - n_3)(s_1 - s_3) = 0,$$

de même

$$(n_0 - n_2 - y_1)(s_1 - s_3) + (n_1 - n_3)(s_2 - s_0) = 0.$$

Éliminant entre ces deux dernières équations $s_0 - s_2$, $s_1 - s_3$, il vient

$$(n_1 - n_3)^2 + (n_0 - n_2 - y_0)(n_0 - n_2 - y_1) = 0$$

ou

$$4(n_1 - n_3)^2 + [2(n_0 - n_2) + 1]^2 = p.$$

Nous distinguerons maintenant les deux cas de ω pair et ω impair.

Premier cas : ω *pair*. — D'après le n° 20, on a les équations

$$1 + n_0 + n_1 + n_2 + n_3 = \omega. \qquad 2n_2 = n_1 + n_3.$$

On en déduit

$$n_0 = \omega - 1 - 3n_2, \qquad 2(n_0 - n_2) + 1 = 2\omega - 1 - 8n_2 = a;$$

a est déterminé par les deux conditions

$$16b^2 + a^2 = p, \qquad a \equiv -1 \pmod 4;$$

n_0, n_2 sont donc déterminés sans ambiguïté; n_1, n_3 peuvent se permuter en changeant la racine primitive prise pour g.

Les quatre périodes de l'unité sont données par l'équation

$$x^2 - yx - \frac{p - 1 + (a+1)(2+4y)}{16} = 0,$$

en remplaçant y successivement par y_0, y_1; la condition trouvée $4(n_1 - n_3)^2 + (2n_0 - 2n_2 + 1)^2 = p$ exprime que les deux équations obtenues sont équivalentes. En posant $a = 4m - 1$, l'équation en x peut s'écrire

$$x^2 - yx - (b^2 + m^2 + my) = 0,$$

ce qui donne, pour l'équation aux quatre périodes

$$(x^2 - b^2 - m^2)^2 + (x^2 - b^2 - m^2)(x - m) + \frac{1-p}{4}(x - m)^2 = 0.$$

Second cas : ω *impair*. — D'après le n° 20, on a les équations du premier degré

$$n_0 + n_1 + n_2 + n_3 = \omega, \qquad 1 + 2n_0 = n_1 + n_3;$$

d'où

$$n_2 = \omega - 1 - 3n_0, \qquad 2n_0 - 2n_2 + 1 = 8n_0 - 2\omega + 3;$$

posons

$$2\omega - 3 - 8n_0 = a;$$

les deux conditions

$$4b^2 + a^2 = p, \qquad a \equiv -1 \pmod 4$$

déterminent complètement a, et par suite n_0, n_2.

Les quatre périodes de l'unité sont données par l'équation

$$x^2 - yx + \frac{3p + 1 - (a+1)(2+4y)}{16} = 0$$

ou, en posant $a = 4m - 1$,

$$x^2 - yx + \frac{3b^2 + 1}{4} + m(3m - 2) - my = 0,$$

y devant prendre successivement les valeurs des deux racines de l'équation

$$y^2 + y + \frac{1 - p}{4} = 0.$$

V.

Des équations se ramenant aux équations binômes par une transformation linéaire.

26. Si, dans une équation binôme, on remplace l'inconnue par une fonction linéaire $\frac{ax + b}{a'x + b'}$ de x, l'équation transformée ordonnée suivant les puissances décroissantes de x devient

$$a_0 x^m + m a_1 x^{m-1} + \ldots + \frac{m(m-1)\ldots(m-i+1)}{1.2\ldots i} a_i x^{m-i} + \ldots = 0,$$

trois termes consécutifs de la suite $a_0, a_1, \ldots, a_m$, satisfaisant à une relation linéaire homogène

$$\alpha_0 a_i + \alpha_1 a_{i+1} + \alpha_2 a_{i+2} = 0;$$

les quantités $a_0, a_1, \ldots, a_m$ sont donc $m + 1$ termes consécutifs d'une série récurrente provenant d'une fraction dont le dénominateur est du second degré.

Réciproquement, soit

$$f(x) = \sum_{i=0}^{i=m} \frac{m(m-1)\ldots(m-i+1)}{1.2\ldots i} a_i x^{m-i},$$

les quantités $a_0, a_1, \ldots, a_m$ satisfaisant à la loi de récurrence

$$\alpha_0 a_i + \alpha_1 a_{i+1} + \alpha_2 a_{i+2} = 0;$$

on a identiquement

$$(\lambda' - \lambda) f(x) = (a_0 \lambda' - a_1)(x + \lambda)^m - (a_0 \lambda - a_1)(x + \lambda')^m,$$

λ et λ' étant les deux racines de l'équation

$$\alpha_0 + \alpha_1 \lambda + \alpha_2 \lambda^2 = 0,$$

supposées distinctes; dans le cas où elles sont égales, on a

$$f(x) = a_0(x+\lambda)^m - m(a_0\lambda - a_1)(x+\lambda)^{m-1}.$$

Supposons les coefficients de $f(x)$ réels, et cherchons le nombre des racines réelles de l'équation $f(x) = 0$. Ces racines s'obtiennent en substituant à y, dans la fonction linéaire $\frac{\lambda' y - \lambda}{1-y}$, les m racines de l'équation

$$(a_0\lambda' - a_1)y^m - (a_0\lambda - a_1) = 0. \tag{1}$$

1° Les racines de l'équation en λ sont imaginaires. Les racines de l'équation en y sont aussi imaginaires, et leur module est égal à 1; si, dans la quantité $\frac{\lambda' y - \lambda}{1-y}$, y étant une racine de l'équation (1), on remplace $\sqrt{-1}$ par $-\sqrt{-1}$, elle ne change pas

$$\frac{\lambda\frac{1}{y} - \lambda'}{1 - \frac{1}{y}} = \frac{\lambda' y - \lambda}{1-y};$$

donc les m racines de l'équation $f(x) = 0$ sont réelles.

2° Les racines de l'équation en λ sont réelles et inégales : la quantité $\frac{\lambda' y - \lambda}{1-y}$ est réelle ou imaginaire en même temps que y. L'équation $f(x) = 0$ a le même nombre de racines réelles que l'équation en y : une seule si m est impair; deux si, m étant pair, $\frac{a_0\lambda - a_1}{a_0\lambda' - a_1}$ est positif; aucune si, m étant pair, $\frac{a_0\lambda - a_1}{a_0\lambda' - a_1}$ est négatif.

Les équations du troisième degré et l'équation dont dépend $\operatorname{tang}\frac{a}{m}$, étant donnée $\operatorname{tang} a$, rentrent dans la classe précédente.

27. Désignons par $\mathfrak{F}(\theta) = 0$ l'équation ayant pour racines les $\varphi(m)$ racines primitives de l'équation binôme $x^m - 1 = 0$; y_0 étant une racine de l'équation (1), les autres seront θy_0, $\theta^2 y_0$, ..., $\theta^{m-1} y_0$, ... ; et les racines de l'équation $f(x) = 0$ sont données par la formule $x_k = \frac{\lambda'\theta^k y_0 - \lambda}{1 - \theta^k y_0}$, en donnant à k les valeurs 0, 1, 2, ..., $m-1$. Posons

$$\psi(x) = \frac{\lambda'\theta(x+\lambda) - \lambda(x+\lambda')}{x + \lambda' - \theta(x+\lambda)};$$

il vient

$$x_1 = \psi(x_0), \qquad x_2 = \psi(x_1)$$

et, en général,

$$x_{k+1} = \psi(x_k);$$

d'où

$$x_k = \psi^k(x_0) \qquad \text{et} \qquad \psi^m(x) = x,$$

quel que soit x.

Réciproquement, soit $\psi(x) = \dfrac{ax+b}{a'x+b'}$ une fonction linéaire, le déterminant $ab' - ba'$ étant différent de o. Identifiant avec la forme précédente, il vient

$$(1) \qquad \frac{a}{a'} = \frac{\lambda'\theta - \lambda}{1-\theta}, \qquad \frac{b'}{a'} = \frac{\lambda' - \theta\lambda}{1-\theta}, \qquad \frac{b}{a'} = -\lambda\lambda';$$

d'où

$$\frac{b'-a}{a'} = -(\lambda + \lambda');$$

et λ, λ' sont les deux racines de l'équation

$$(2) \qquad a'\lambda^2 - (b'-a)\lambda - b = 0;$$

si elles sont distinctes, la valeur de θ est déterminée et satisfait à l'équation

$$\theta^2 + \frac{(a+b')^2 + 2(a'b - ab')}{a'b - ab'}\,\theta + 1 = 0.$$

Si les racines de cette équation sont des racines de l'unité, la suite des fonctions x, $\psi(x)$, $\psi^2(x)$, ..., $\psi^k(x)$ est terminée; en tout cas, on a

$$\psi^k(x) = \frac{\lambda'\theta^k(x+\lambda) - \lambda(x+\lambda')}{x + \lambda' - \theta^k(x+\lambda)}.$$

Si les racines de l'équation (2) sont égales, on ne peut satisfaire aux trois équations (1). Effectuons la transformation

$$x = \frac{\lambda' y - \lambda}{1-y}, \qquad \psi(x) = \frac{\lambda'\chi(y) - \lambda}{1-\chi(y)},$$

d'où

$$\chi(y) = \frac{(a'\lambda\lambda' - b'\lambda + a\lambda' - b)y - a'\lambda^2 + (b'-a)\lambda + b}{[a'\lambda'^2 - (b'-a)\lambda' - b]y - a'\lambda\lambda' + b'\lambda' - a\lambda + b}.$$

Prenant pour λ' la valeur de la racine double de l'équation

$$a'\lambda^2 - (b'-a)\lambda - b = 0,$$

il vient

$$\chi(y)=y+\frac{2a'}{a+b'}(\lambda-\lambda'),\qquad \chi^k(y)=y+\frac{2ka'}{a+b'}(\lambda-\lambda'),$$

et l'on en déduit

$$\psi^k(x)=\frac{\left(a-b'+\dfrac{a+b'}{m}\right)x+2b}{2a'x-\left(a-b'-\dfrac{a+b'}{m}\right)}.$$

28. Si l'on se donne les deux premiers coefficients a_0, a_1 de la fonction $f(x)$ du n° **26**, et les trois coefficients $\alpha_0, \alpha_1, \alpha_2$ de la relation $\alpha_0 a_i+\alpha_1 a_{i+1}+\alpha_2 a_{i+2}=0$, tous les autres coefficients de la fonction $f(x)$ sont déterminés. Nous supposerons les trois nombres α entiers et les deux quantités a_0, a_1 quelconques, a_0 étant toutefois différent de 0. D'après ce qui précède, les m racines de l'équation $f(x)=0$ sont représentées par x, $\psi(x)$, ..., $\psi^{m-1}(x)$, x étant l'une d'elles, et $\psi(x)$ la fonction linéaire

$$\frac{(\lambda'\theta-\lambda)x-\lambda\lambda'(1-\theta)}{(1-\theta)x-(\lambda\theta-\lambda')},$$

où λ, λ' sont les deux racines supposées distinctes de l'équation $\alpha_0+\alpha_1\lambda+\alpha_2\lambda^2=0$, et θ une racine primitive de l'équation $\theta^m-1=0$. On a

$$\frac{\lambda'\theta-\lambda}{1-\theta}=\frac{\alpha_1+z}{2\alpha_2},\qquad \frac{\lambda\theta-\lambda'}{1-\theta}=\frac{\alpha_1-z}{2\alpha_2},$$

z étant définie par l'équation

$$z^2=(\alpha_1^2-4\alpha_0\alpha_2)\left(\frac{\theta+1}{1-\theta}\right)^2;$$

d'où, en posant $\alpha_1^2-4\alpha_0\alpha_2=A$,

$$\theta=\frac{z-\sqrt{A}}{z+\sqrt{A}}.$$

Si l'on remplace θ par sa valeur en fonction de z dans l'équation de degré $\varphi(m)$ donnant les racines primitives de $\theta^m-1=0$, on obtient une équation à coefficients entiers et n'ayant que des termes de degré pair en z. Cette équation est irréductible ou se décompose en deux autres de degré $\frac{\varphi(m)}{2}$ irréductibles; car, en remplaçant

$\frac{z^2}{A}$ par y^2 ou y, on obtient une équation irréductible (20). Il est facile de voir quand elle peut se décomposer pour m égal à un nombre premier p ou au double d'un nombre premier. D'après une formule de Gauss (SERRET, *Algèbre supérieure*),

$$4\frac{x^p-1}{x-1} = Y^2+(-1)^{\frac{p-1}{2}}pZ^2;$$

ainsi l'équation en z prend la forme $Y^2+pAZ^2=0$, si m est égal à p ou $2p$, p étant un nombre premier congru à $-1 \pmod 4$, Y et Z étant des fonctions entières de z; et la forme $Y^2-pZ^2=0$, si m est égal à p ou $2p$, p étant premier et congru à $1 \pmod 4$. Donc, si m est égal à p ou $2p$, p étant premier et de la forme $4q+3$, l'équation en z se ramène à deux autres de degré $\frac{p-1}{2}$, à coefficients entiers pour les valeurs de A égales à $-pa^2$; l'équation en z est irréductible dans tout autre cas pour m premier ou égal au double d'un nombre premier.

Soient

$$z_i = \sqrt{A}\frac{1+\theta^i}{1-\theta^i} = \chi_i(z), \qquad z_j = \sqrt{A}\frac{1+\theta^j}{1-\theta^j} = \chi_j(z);$$

quel que soit le nombre entier i, $\chi_i(z)$ est une fonction rationnelle de z; mais, si le nombre i est premier avec m, z peut réciproquement s'exprimer en fonction rationnelle de z_i. Les entiers i et j étant tous deux premiers avec m, on a

$$\chi_j\chi_i(z) = \sqrt{A}\frac{1+\theta^{ij}}{1-\theta^{ij}} = \chi_i\chi_j(z);$$

les fonctions χ_i, χ_j sont donc échangeables entre elles, conformément à ce qui a été démontré au n° 18.

29. Cherchons dans quel cas les coefficients de la fonction $\psi(x)$ sont des nombres entiers, et par suite l'équation $f(x)=0$, abélienne. On a

$$\psi(x) = \frac{(\alpha_1-z)x-2\alpha_0}{2\alpha_2 x-(\alpha_1+z)};$$

dans tous les cas, les coefficients des diverses fonctions $\psi(x)$, $\psi^2(x), \ldots, \psi^{m-1}(z)$ sont des fonctions rationnelles de z; et, d'après ce qui a été dit plus haut, l'équation en z ne peut se ramener à

une équation du premier degré que dans les cas de m égal à 2, 3, 4 ou 6.

Soit d'abord m égal à 6. L'équation en θ est $\theta^2 - \theta + 1 = 0$; l'équation en z qu'on obtient en substituant à θ la fonction $\frac{z - \sqrt{A}}{z + \sqrt{A}}$ est $z^2 + 3A = 0$; posons

$$A = \alpha_1^2 - 4\alpha_0\alpha_2 = -3a^2.$$

d'où

$$\alpha_0 = \frac{\alpha_1^2 + 3a^2}{4\alpha_2}.$$

On peut prendre pour α_1 et a des nombres entiers quelconques de même parité, pour α_2 un diviseur quelconque du nombre entier $\frac{\alpha_1^2 + 3a^2}{4}$; α_0 est alors déterminé; toutefois α_0, α_1, α_2 ne doivent pas avoir de diviseur commun; z est égal à $\pm 3a$, $\alpha_1 \mp 3a$ est un nombre pair et la fonction $\psi(x)$ devient

$$\frac{\frac{\alpha_1 - 3a}{2}x - \alpha_0}{\alpha_2 x - \frac{\alpha_1 + 3a}{2}};$$

son déterminant est égal à $-\frac{\alpha_1^2 - 9a^2}{4} + \alpha_0\alpha_2 = 3a^2$.

Soit $m = 3$. L'équation en θ est $\theta^2 + \theta + 1 = 0$, l'équation en z, $3z^2 + A = 0$; posons encore $A = -3a^2 = \alpha_1^2 - 4\alpha_0\alpha_2$; d'où $\alpha_0\alpha_2 = \frac{\alpha_1^2 - 3a^2}{4}$; a, α_0, α_1, α_2 peuvent être choisis comme précédemment; z est égal à $\pm a$; $\alpha_1 \mp a$ est un nombre pair et la fonction $\psi(x)$ devient

$$\frac{\frac{\alpha_1 - a}{2}x - \alpha_0}{\alpha_2 x - \frac{\alpha_1 + a}{2}};$$

son déterminant est égal à $-\frac{\alpha_1^2 - a^2}{4} + \alpha_0\alpha_2 = a^2$; si a^2 est égal à 1, les racines de l'équation $f(x) = 0$ se développent en fractions continues terminées par les mêmes quotients (Serret, *Algèbre supérieure*). L'équation aux trois périodes rentre dans ce cas; le nombre que nous désignons ici par a correspond au nombre que

nous avons appelé ν au n° 22 et qui est défini par l'équation

$$27\nu^2 + L^2 = 4p.$$

Soit $m = 4$. L'équation en θ est $\theta^2 + 1 = 0$, l'équation en z, $z^2 + A = 0$; posons $A = \alpha_1^2 - 4\alpha_0\alpha_2 = -a^2$, d'où $\alpha_0\alpha_2 = \frac{\alpha_1^2 + a^2}{4}$. On peut prendre pour α_1, a des nombres pairs quelconques, pour α_2 un diviseur du nombre entier $\frac{\alpha_1^2 + a^2}{4}$, tel que α_0, α_1, α_2 n'aient pas de diviseur commun. z est égal à $\pm a$; $\alpha_1 \pm a$ est un nombre pair et la fonction $\psi(x)$ devient

$$\frac{\frac{\alpha_1 - a}{2}x - \alpha_0}{\alpha_2 x - \frac{\alpha_1 + a}{2}}.$$

Le déterminant de $\psi(x)$ est égal à $\frac{a^2}{2}$; comme dans le cas de $m = 6$, ce déterminant ne peut jamais devenir égal à ± 1, puisque a et par suite $\frac{a^2}{2}$ sont des nombres pairs.

Soit enfin $m = 2$; considérons le cas où l'équation proposée $Dx^2 + Ex + F = 0$ a ses coefficients entiers. On peut satisfaire à la relation $\alpha_0 D + \alpha_1 E + \alpha_2 F = 0$ d'une infinité de manières, en prenant pour les α des nombres entiers; il en résulte

$$x_2 = \frac{\alpha_1 x_1 - \alpha_0}{\alpha_2 x_1 - \alpha_1},$$

x_1, x_2 étant les deux racines de l'équation. Elles se développeront en fractions continues terminées par les mêmes quotients si l'on peut satisfaire à la condition $\alpha_1^2 - \alpha_0\alpha_2 = \pm 1$, ou par l'élimination de α_0,

$$D\alpha_1^2 + \alpha_1\alpha_2 E + \alpha_2^2 F = \pm D,$$

avec la condition $\frac{\alpha_1^2 \pm 1}{\alpha_2} =$ entier. Cette dernière équation est toujours possible lorsque D ou F est égal à ± 1; $\alpha_2 x_1 - \alpha_1$ est une unité complexe lorsque $D = \pm 1$.

30. Lorsque les racines d'une équation irréductible sont reliées par une équation linéaire $ax_1x_2 + bx_1 + cx_2 + d = 0$, ou plus généralement lorsque les racines d'une équation $f(x) = 0$, de degré

m, peuvent se partager en $\frac{m}{\mu}$ groupes de μ racines, les racines d'un groupe pouvant être représentées par x, $\theta(x)\ldots\theta^{\mu-1}(x)$, x étant l'une d'elles, θ une fonction rationnelle et linéaire, $\theta^{\mu}(x)$ étant identiquement égale à x, on peut, par une transformation linéaire, ramener l'équation à la forme $F(y^{\mu}) = 0$, F désignant une fonction entière. Ainsi, dans le cas où la relation est

$$ax_1x_2 + b(x_1 + x_2) + c = 0,$$

on peut ramener l'équation à la forme $F(y^2) = 0$. Si a n'est pas nul, on simplifie les calculs en ramenant l'équation à être réciproque par une substitution linéaire et entière, $x = \alpha t + \beta$; puis il suffit de remplacer t par $\frac{y+\gamma}{y-\gamma}$ pour avoir une équation paire. Soit l'équation du quatrième degré

$$f(x) = x^4 + 6qx^2 + 4rx + s = 0.$$

On a, pour déterminer α et β, les équations

$$[6f'(\beta)]^2 - f(\beta)[f'''(\beta)]^2 = 0, \qquad \alpha^2 = \frac{6f'(\beta)}{f'''(\beta)},$$

ou

$$\beta^3 + \frac{s - 9q^2}{2r}\beta^2 - 3q\beta - \frac{r}{2} = \varphi(\beta) = 0, \qquad \alpha^2 = \varphi'(\beta).$$

Et l'on voit immédiatement que, si les coefficients de $f(x)$ sont réels, il y a deux valeurs réelles et positives pour α^2 si les trois racines de l'équation $\varphi(\beta) = 0$ sont réelles, et une valeur réelle et positive pour α^2 si $\varphi(\beta) = 0$ a deux racines imaginaires.