SUR UNE NOTION QUI COMPREND CELLE DE LA DIVISIBILITÉ ET SUR LA THÉORIE GÉNÉRALE DE L'ÉLIMINATION

PAR

J. MOLK

À STRASBOURG.

Introduction.

Les voies nouvelles ouvertes à l'Algèbre par les travaux de GAUSS, d'ABEL et de GALOIS ont été le point de départ des recherches de M. KRONECKER sur la théorie générale de l'élimination. Ces recherches sont intimement liées à celles qui ont pour objet l'étude des systèmes de diviseurs d'un système de fonctions entières. Je me suis proposé, dans ce mémoire, d'exposer les unes et les autres, en me plaçant au point de vue arithmétique de M. KRONECKER.

Pour bien faire saisir l'esprit des méthodes employées il m'a semblé nécessaire de préciser tout d'abord l'idée d'irréductibilité dans un domaine de rationalité donné. J'ai ensuite développé les premiers éléments de la théorie des systèmes de diviseurs dont l'introduction en Algèbre est due à M. KRONECKER. Après avoir exposé quelques théorèmes sur l'élimination d'une variable entre deux équations, j'ai enfin abordé l'objet même de ce mémoire, la théorie générale de l'élimination.

Je désirerais surtout éclaircir quelques points du grand mémoire que M. KRONECKER a publié, en Septembre 1881, à l'occasion du cinquantième

Acta mathematica. 6. Imprimé 23 Mai 1884.

anniversaire du doctorat de M. KUMMER.(1) Ce mémoire semble appelé à imprimer une direction nouvelle à l'Algèbre. Le but que je me suis proposé serait entièrement atteint si mon travail pouvait amener quelques géomètres à approfondir les idées aussi difficiles que nombreuses qui y sont contenues.

C'est à ce mémoire, à quelques autres publications de M. KRONECKER et plus particulièrement à son Cours professé à l'Université de Berlin que j'ai emprunté presque tous les matériaux de ce travail. Je me suis efforcé de les grouper et de les éclairer, de les ordonner aussi méthodiquement que le comportait la nature du sujet, et de les rendre ainsi accessibles à tous. A cet effet, je n'ai pas hésité à répéter, à plusieurs reprises, des choses bien connues de tous ceux qui s'occupent d'Algèbre. D'autre part, j'ai cherché à caractériser et à bien mettre en évidence les questions qui, pour moi du moins, restent à résoudre. M. KRONECKER a bien voulu s'intéresser à mon travail et je lui dois les plus précieux encouragements pendant tout le temps que j'y ai consacré.

CHAPITRE I.

Méthodes particulières à l'Algèbre.

1. L'Arithmétique et l'Algèbre prennent une place a part dans l'ensemble des sciences mathématiques. Leur objet propre est, en dernière analyse, l'étude des propriétés des nombres entiers positifs et des fonctions entières à coefficients entiers, positifs, d'une ou de plusieurs variables indépendantes.

Ces deux études ne diffèrent pas essentiellement l'une de l'autre. Une fonction entière, à coefficients entiers, positifs, d'un certain nombre de variables représente, en effet, d'une manière commode, un système de nombres entiers et ne représente pas autre chose. On obtient ce système

---

(1) L. KRONECKER: *Grundzüge einer arithmetischen Theorie der algebraischen Grössen.* Festschrift zu Herrn E. E. KUMMERS Doctor-Jubiläum. Berlin, Reimer 1882.

en remplaçant successivement, dans la fonction entière considérée, les variables par tous les systèmes de valeurs entières plus petites qu'un entier, laissé, à dessein, *indéterminé* dans les recherches générales, afin de pouvoir être choisi convenablement dans chaque recherche particulière. L'indétermination du nombre *fini* d'entiers du système que l'on considère, et la manière d'obtenir facilement ces entiers, sont toutes deux mises en évidence en représentant ce système par une fonction entière.

L'Arithmétique et l'Algèbre ont ainsi un domaine bien défini; les nombres entiers, positifs, les systèmes de nombres entiers représentés par des fonctions entières à coefficients entiers, positifs, y sont considérés comme *existant,* tout comme le mouvement en cinématique et la matière dans les sciences naturelles. Les nombres rationnels, négatifs, imaginaires, ainsi que les nombres irrationnels et transcendants ne font pas partie de ce domaine. Ils n'ont du nombre que le nom; en réalité ce sont de purs symboles.

En Analyse le point de vue est différent. On commence par généraliser l'idée même de quantité. GAUSS l'a le premier fait d'une manière systématique mais sans séparer entièrement le domaine de la Géométrie de celui de l'Arithmétique. Plus tard M. WEIERSTRASS a suivi une méthode essentiellement différente où l'on ne s'attache d'abord à aucun domaine déterminé mais où, au contraire, le but que l'on se propose, en généralisant l'idée de quantité, est de *déterminer* le domaine nécessaire et suffisant dans lequel on puisse effectuer toutes les opérations directes et inverses qui se présentent dans les calculs. Mais que l'on se place au point de vue de GAUSS ou à celui de M. WEIERSTRASS il importe de remarquer que le désir de pouvoir répondre *positivement* à une série de questions, qui sont en partie du domaine de la Géométrie, a seul amené les mathématiciens à introduire successivement de nouveaux symboles en Analyse. On comprend alors qu'en se plaçant au point de vue spécial de l'Arithmétique, en assignant à cette science un domaine déterminé, celui des nombres entiers, positifs, et en ne voulant pas introduire dans tous les raisonnements une idée étrangère à l'objet que l'on a en vue, il convienne de n'employer qu'une partie des symboles de l'Analyse, celle qui ne nous fait quitter qu'en apparence le domaine de l'Arithmétique.

Les symboles dits rationnels, positifs et négatifs remplissent cette condition. A tout moment une égalité contenant des nombres rationnels,

positifs ou négatifs, peut être transformée en une égalité entièrement équivalente et ne contenant que des nombres entiers et positifs. Un nombre *fini* d'opérations permet toujours de grouper les symboles rationnels suivant les besoins du calcul et de remplacer ces groupes par des nombres entiers positifs à l'aide des égalités qui définissent ces symboles, égalités qui peuvent toujours être sous-entendues et qui seules ont une existence réelle en Arithmétique.

La même chose a lieu pour les fonctions entières ou rationnelles, à coefficients entiers ou rationnels, positifs ou négatifs, d'un nombre quelconque de variables. Aussi les adjoindrons-nous également au domaine de l'Arithmétique.

Les fonctions entières d'une variable, égalées à zéro, définissent de nouveaux nombres, les nombres algébriques. Mais nous remarquons une grande différence entre l'introduction de ces nombres et celle des nombres rationnels, car nous ne pouvons pas à tout moment remplacer une égalité contenant des nombres algébriques par une égalité équivalente et ne contenant que des nombres entiers et positifs. En réalité, lorsqu'on définit positivement les nombres algébriques, on quitte vraiment, et non plus en apparence seulement pour la commodité des calculs, le domaine de l'Arithmétique pour entrer dans un domaine plus vaste. Il convient donc d'éviter l'emploi de ces nombres. Leur introduction, en Arithmétique, est d'ailleurs inutile en théorie; nous verrons plus loin par quoi il faut chercher à les remplacer.

Cependant lorsqu'on fait de nouvelles recherches, il est presque indispensable, dans l'état actuel de la science, de se servir de nombres algébriques; c'est, il est vrai, un simple artifice de langage, mais il fait image et nous permet de séparer facilement dans notre pensée les différentes racines conjuguées et d'abréger ainsi les démonstrations. La même chose a lieu en Géométrie par exemple, où il est souvent bien commode de ne pas s'astreindre tout d'abord à faire de la Géométrie de position, mais, au contraire, de supposer connus certains éléments qui sont du domaine de la Mécanique.

Sans doute il est nécessaire, pour être en droit de séparer ainsi les racines et de les représenter *séparément* par des symboles, de montrer comment, après avoir ramené le cas général à celui de la recherche des racines réelles d'une équation à coefficients réels, on peut, dans ce cas

particulier, *déterminer un intervalle dans lequel l'équation donnée ne saurait être vérifiée par plus d'un nombre rationnel, avec une approximation donnée, suffisamment grande.* Il faut, en un mot, montrer ce que l'on doit entendre par racine d'une équation algébrique, au point de vue arithmétique auquel nous nous sommes placés.

Mais ces considérations m'écarteraient par trop de l'objet que j'ai principalement en vue. Elles rentrent dans un autre ordre d'idées et il convient de les exposer avec la théorie des *Caractéristiques.* (1) En supposant cette lacune comblée, il n'y a aucun inconvénient, dans des recherches nouvelles, à se servir de ces symboles algébriques, si l'on a soin d'y joindre l'égalité qui les définit. Il est cependant toujours *nécessaire,* lorsqu'on se propose d'approfondir les principes de l'Algèbre, de se passer, autant que possible, de cet instrument étranger au domaine de cette science.

Ce que je dis des nombres algébriques s'applique mot pour mot aux fonctions algébriques.

2. Mais la faiblesse de notre esprit ne nous permet pas plus d'aborder directement les questions fondamentales de l'Algèbre que celles de l'Arithmétique. Il nous est nécessaire de saisir à la fois tout l'ensemble d'une question, toutes les faces sous lesquelles elle se présente, pour pouvoir tirer des conclusions; et notre puissance d'abstraction est, en général, si faible que nous avons besoin d'auxiliaires. Ces auxiliaires nous sont donnés par la nature elle-même. Ce sont les quantités indéterminées. C'est à GAUSS que revient la gloire de les avoir introduites en Arithmétique. POISSON et plusieurs autres mathématiciens éminents, ont certainement aperçu, en partie du moins, leur importance; mais c'est à M. KRONECKER qu'il était réservé de faire voir clairement le rôle fondamental qu'elles sont appelées à jouer en Algèbre.

Je distingue entre *indéterminées* et *variables.*

Nous ne pouvons pas disposer des indéterminées dans le cours d'une démonstration. Ce sont ou bien de simples liens destinés à joindre une série d'opérations à effectuer ou de valeurs à trouver, et alors nous n'avons aucune prise sur elles, ou bien encore des abstractions que nous laissons à dessein indéterminées dans une même recherche afin d'embrasser un grand nombre de cas particuliers dans un seul calcul et alors, le calcul

(1) Comparez KRONECKER, Monatsberichte der Berliner Akademie 1869.

terminé, nous pouvons leur donner une valeur quelconque. Dans ce dernier cas, je les nommerai plus particulièrement variables-indéterminées.

Les variables, au contraire, peuvent prendre des valeurs particulières dans le cours d'une démonstration. Elles nous sont, en effet, données par la nature même de nos recherches et nous nous proposons précisément de rechercher les valeurs particulières qu'il faut leur donner, ou encore les restrictions auxquelles elles doivent être soumises pour satisfaire aux conditions d'un problème déterminé.

Nous verrons, dans la suite, que l'emploi de variables *auxiliaires* est parfois fort utile. Il permet d'effectuer des transformations qui affranchissent les expressions considérées de certains cas particuliers dont l'étude spéciale ne serait d'aucun profit pour les résultats à obtenir.

On pourrait objecter à ce que j'ai dit des nombres et fonctions algébriques que ce sont tout aussi bien des auxiliaires légitimes que les quantités indéterminées. Cela n'est point douteux quant à la rigueur des démonstrations. Dans l'état actuel de la science, il peut même être souvent plus avantageux, pour obtenir ou énoncer rapidement des résultats nouveaux, d'employer comme auxiliaires les fonctions algébriques que de faire usage des quantités indéterminées. Mais lorsqu'il s'agit de voir clairement le rôle que joue chaque élément dans l'exposé des principes et des méthodes de l'Algèbre, il ne saurait y avoir de doute sur l'avantage de l'emploi des quantités indéterminées sur celui des nombres et fonctions algébriques.

En effet, l'existence même approximative de ces derniers est une idée très-complexe dans le domaine que nous nous sommes fixés. On peut presque dire qu'elle joue le même rôle en Algèbre que l'intégrale de CAUCHY en Analyse. C'est parce qu'ils supposent et renferment plusieurs hypothèses essentielles que ces deux merveilleux instruments permettent d'obtenir rapidement un grand nombre de transformations, l'un d'expressions algébriques, l'autre d'expressions transcendantes. Avant d'avoir cherché à s'en passer, on ne se rend que très-difficilement compte de toute la simplification qu'ils introduisent l'un en Algèbre, l'autre en Analyse. Loin de les critiquer je crois, au contraire, qu'il convient, actuellement, de les placer, dans ces deux sciences, au début de toute recherche nouvelle. Mais je crois aussi que, précisément parce qu'ils renferment tous deux tant d'hypothèses essentielles, ils n'éclairent pas suffisamment les principes de la science, et c'est pourquoi, en me bornant à

l'Algèbre, je disais plus haut que lorsqu'on se propose d'en approfondir les principes, il est préférable de chercher à se passer de leur aide.

Les indéterminées, au contraire, ne nous font point quitter le domaine des quantités rationnelles. Elle n'exigent point d'autres symboles que ceux que nous connaissons déjà, les symboles qui correspondent aux quatre opérations. Elles ont de plus un grand avantage, celui d'unir en quelque sorte l'Arithmétique à l'Algèbre, la théorie des nombres à celle des fonctions entières d'une et de plusieurs variables, comme nous le verrons dans la suite.

Je rappelle qu'une *forme* est une fonction entière dans laquelle les variables sont remplacées par des indéterminées.

L'*association* (1) des quantités indéterminées au domaine de l'Algèbre amène naturellement à joindre à l'étude des nombres entiers et des fonctions entières, celle des *formes* dont les coefficients sont soit des nombres entiers, soit des fonctions entières.

Il me reste à parler des nombres transcendants et imaginaires.

Les nombres transcendants, comme le rapport d'une circonférence à son diamètre, ne joueront pour nous que le rôle d'indéterminées. Si, en effet, nous démontrons un théorème en les supposant indéterminées et que nous remplacions ensuite ces indéterminées par les nombres transcendants donnés, rien ne saurait être changé dans notre domaine algébrique.

Les nombres imaginaires, de même que les nombres algébriques ne joueront aussi pour nous que le rôle d'indéterminées; mais, comme ils sont définis par des égalités ayant une existence réelle dans le domaine que nous considérons, il nous faudra tenir compte, dans nos calculs, de ces égalités, ce qui revient à remplacer les équations par des congruences.

Ainsi, par exemple, $\sqrt{2}$ n'est qu'un symbole; ce qu'il y a de réel, pour nous, c'est l'égalité $x^2 = 2$ qui définit $\sqrt{2}$. Si nous joignons au symbole l'égalité correspondante rien n'empêche d'en faire usage; chaque fois que dans le courant d'un calcul paraîtra $\sqrt{2}.\sqrt{2}$, l'égalité adjointe nous montre que nous devons remplacer ce produit par le nombre 2; en d'autres termes, que toute équation

$$F(\sqrt{2}) = 0$$

(1) Comparez KRONECKER: Festschrift, § 22.

où F désigne une fonction entière à coefficients rationnels, est équivalente à la congruence

$$F(u) \equiv 0 \pmod{x^2 - 2}$$

dans laquelle u désigne une indéterminée.

La même chose a lieu pour les nombres imaginaires que l'on emploie ordinairement en Analyse, le module de la congruence étant alors $(x^2 + 1)$. Dans des recherches spéciales d'Arithmétique il peut être convenable d'employer d'autres imaginaires que $\sqrt{-1}$; cela revient à remplacer le module $(x^2 + 1)$ par un autre module qui simplifie d'avantage la recherche particulière que l'on effectue.

3. Ce que j'ai dit du domaine particulier à l'Arithmétique et à l'Algèbre indique la marche à suivre dans tout exposé des résultats principaux obtenus dans ces deux sciences.

Les définitions devront être algébriques et non pas logiques seulement.

Il ne suffit pas de dire: »Une chose est ou elle n'est pas». Il faut montrer ce que veut dire être et ne pas être, dans le domaine particulier dans lequel nous nous mouvons. Alors seulement nous faisons un pas en avant. Si nous définissons, par exemple, une fonction irréductible comme une fonction qui n'est pas réductible, c'est à dire qui n'est pas décomposable en d'autres fonctions d'une nature déterminée, nous ne donnons point de définition algébrique, nous n'énonçons qu'une simple vérité logique. Pour qu'*en Algèbre,* nous soyons en droit de donner cette définition, il faut qu'elle soit précédée de l'exposé d'une méthode nous permettant d'obtenir à l'aide d'un nombre fini d'opérations rationnelles, les facteurs d'une fonction réductible. Seule cette méthode donne aux mots *réductible* et *irréductible* un sens algébrique.

Un raisonnement comme celui-ci: »Si des quantités données, en nombre infini, sont comprises entre des limites finies, il existe nécessairement une limite inférieure de ces quantités», est parfaitement logique. Il n'est point algébrique. Ce qu'il faut c'est donner une méthode pour déterminer, à l'aide d'un nombre fini d'opérations rationnelles, cette limite inférieure. Alors seulement nous faisons de l'Algèbre.

Il convient enfin d'éviter particulièrement toute incursion dans le domaine de la Géométrie. L'idée de continuité géométrique doit nous être d'autant plus étrangère que nous grouperons les nombres, non d'après

leur grandeur, mais d'après leurs propriétés algébriques. Pour éviter tout malentendu, je m'efforcerai d'introduire une terminologie aussi peu géométrique que possible, comme l'a d'ailleurs fait M. KRONECKER dans sa Festschrift, en suivant ainsi l'exemple de GAUSS qui empruntait généralement sa nomenclature aux sciences biologiques.

4. En résumé: Quelle que soit la science naturelle dont on se propose d'aborder l'étude, on a soin de définir les éléments dont le groupement suivant des propriétés déterminées constitue en quelque sorte cette science. Les uns ont une existence réelle, ce sont eux que l'on a tout particulièrement en vue. Les autres sont des éléments auxiliaires; leur réduction à un nombre aussi petit que possible constitue un grand progrès; car elle permet d'apercevoir sans intermédiaires et, par suite, plus clairement les liens cachés qui semblent unir les différents phénomènes.

Autre chose est d'élargir les horizons d'une science ou d'en approfondir les principes. Dans les premiers cas toutes les méthodes peuvent être utiles et ce serait méconnaître l'unité de notre esprit que de le contester. Dans le second cas, au contraire, il faut chercher à se maintenir rigoureusement dans le domaine particulier à la science que l'on a en vue. Car ce n'est pas approfondir les principes d'une science dont le domaine est bien défini que d'en développer les éléments à l'aide de principes étrangers à ce domaine.

La méthode que je viens d'indiquer n'aurait-elle d'ailleurs que l'avantage de faire voir clairement où et comment les principes étrangers à notre domaine simplifient les recherches, qu'il conviendrait encore de l'employer dans la mesure du possible.

L'Algèbre est la première des sciences naturelles. Je viens de définir son domaine, les éléments qui le composent, les éléments auxiliaires dont l'introduction n'offre aucune espèce de difficulté, et ces autres éléments auxiliaires dont malgré tous nos efforts nous ne pouvons encore nous passer entièrement dans nos recherches.

Chapitre II.

Diviseurs des fonctions entières.

§ 1.

Divisibilité des fonctions entières dans un domaine naturel de rationalité. (1)

1. Une propriété fondamentale des nombres entiers est leur *divisibilité.*

Comme un nombre contenu dans un nombre n doit être nécessairement plus petit que n, il suffit, pour trouver les diviseurs de n, de voir si les nombres $2, 3, \ldots, (n-1)$, sont contenus dans n. Un nombre fini d'opérations nous permet donc de montrer qu'un entier positif n est ou bien un produit de nombres premiers et de *trouver* alors ces nombres premiers, ou bien que n est lui-même nombre premier, c'est à dire sans autres diviseurs que lui-même et l'unité. Dans le premier cas on dit que n est un nombre composé, et l'on montre à l'aide de l'algorithme du plus grand commun diviseur que sa décomposition en facteurs premiers est univoque.

Il en est de même des fonctions entières à coefficients entiers.

Considérons d'abord *une* fonction d'une variable. Ses coefficients peuvent avoir un diviseur commun que nous savons trouver par un nombre fini d'opérations, comme je viens de le rappeler. Nous pouvons ainsi mettre toute fonction entière à coefficients entiers sous la forme d'un produit dont l'un des facteurs est un nombre entier et l'autre une fonction entière dont les coefficients sont des entiers sans diviseur commun. Dans des recherches sur la divisibilité des fonctions entières il est donc permis de supposer les coefficients de chacune de ces fonctions, sans diviseur commun.

Considérons ensuite *deux* fonctions d'une variable, $F(x)$ et $G(x)$. Lorsque le quotient de $F(x)$ par $G(x)$ est une fonction entière à coefficients entiers, $H(x)$, nous dirons que $F(x)$ contient $G(x)$, est divisible par $G(x)$

(1) Comparez Kronecker, Journal de Crelle T. 94 et Festschrift § 4.

et que $G(x)$ est contenue dans $F(x)$, est un diviseur de $F'(x)$. Nous écrirons, soit $F(x) = H(x)G(x)$, soit $F(x) \equiv 0 \pmod{G(x)}$, suivant qu'il convient de mettre en évidence la fonction $H(x)$, ou non.

Je vais montrer comment l'on peut, ou bien trouver tous les diviseurs d'une fonction donnée $F(x)$, ou bien montrer que cette fonction $F(x)$ n'a pas de diviseur. Si le degré de $F(x)$ est $2n$ ou $(2n+1)$ il suffit évidemment de donner une méthode permettant de trouver, à l'aide d'un nombre fini d'opérations, ses diviseurs de degré au plus égal à n. Mais d'après la formule d'interpolation de LAGRANGE toute fonction entière $\Phi(x)$ de degré au plus égal à n, peut être mise sous la forme

$$\Phi(x) = \sum_{k=0}^{n} \Phi(r_k) \frac{\mathfrak{F}(x)}{x - r_k} \frac{1}{\mathfrak{F}'(r_k)}$$

où $r_0, r_1, \ldots, r_n$ désignent $(n+1)$ nombres arbitrairement choisis et $\mathfrak{F}(x)$ le produit

$$\prod_{k=0}^{n} (x - r_k).$$

En posant

$$g_k(x) = \frac{\mathfrak{F}(x)}{x - r_k} \frac{1}{\mathfrak{F}'(r_k)}$$

et

$$\Phi(r_k) = c_k$$

nous ordonnons $\Phi(x)$ suivant les fonctions $g_k(x)$, de degré n. Nous avons ainsi

$$\Phi(x) = \sum_{k=0}^{n} c_k g_k(x)$$

où $g_k(r_h) = 0$ pour $h \gtrless k$; et $g_k(r_k) = 1$.

Pour que $\Phi(x)$ soit contenue dans $F(x)$, il faut que $\Phi(r_h) = c_h$ soit contenue dans $F(r_h)$, pour $h = 0, 1, 2, \ldots, n$. Cherchons donc tous les diviseurs positifs et négatifs du nombre $F(r_h)$; ils seront en nombre fini; désignons-les par $c_h, c_h', c_h'', \ldots, c_h^{(m_h)}$. Répétons cette opération pour $h = 0, 1, 2, \ldots, n$; nous aurons certainement un nombre fini

de combinaisons $\sum_{k=0}^{n} c_k g_k(x)$. Chacune de ces combinaisons *peut* être un diviseur de $F(x)$ et il ne saurait y avoir d'autre diviseur de $F(x)$. Un nombre fini de divisions de deux polynômes nous permet donc de voir si $F(x)$ contient un facteur à coefficients entiers ou s'il n'en contient pas.

Nous pouvons maintenant, les nombres entiers étant considérés comme des fonctions entières de degré zéro, partager en deux classes les fonctions entières à coefficients entiers: Celles qui en contiennent d'autres; nous les nommerons *réductibles*. Et celles qui n'en contiennent pas d'autres; nous les nommerons *irréductibles*.

Dans la pratique les calculs se simplifient; mais ici l'important était de montrer que la réductibilité et l'irréductibilité des fonctions ont un sens algébrique, et que nous avons, par suite, le droit d'introduire ces notions dans la science qui fait l'objet de nos recherches.

Si $F_1(x)$ est contenue dans $F(x)$ nous répéterons sur $F_1(x)$ les mêmes raisonnements que nous venons de faire sur $F(x)$, et comme le degré de chaque diviseur est plus petit que celui de la fonction dans laquelle il est contenu, un nombre fini d'opérations nous permettra de décomposer $F(x)$ en un produit de puissances de fonctions entières *irréductibles*.

2. *Cette décomposition est univoque.* En effet, si le produit $\Phi(x).\Psi(x)$ de deux fonctions entières à coefficients entiers, est divisible par une fonction irréductible $F(x)$, l'une des deux fonctions $\Phi(x)$, $\Psi(x)$, est elle-même divisible par $F(x)$. Lorsque $F(x)$ se réduit à un nombre premier, la démonstration se déduit immédiatement du théorème qu'un produit de deux nombres ne peut être divisible par un nombre premier p que si l'un des deux nombres est divisible par p, et ce théorème est un corollaire de *l'algorithme* d'Euclide. Lorsque le degré de $F(x)$ est plus grand que zéro, si $\Phi(x)$ n'est pas divisible par $F(x)$, comme $F(x)$ est irréductible, $\Phi(x)$ et $F(x)$ n'ont point de diviseur commun. Mais alors, à l'aide de *l'algorithme* d'Euclide étendu aux fonctions d'une variable, nous pouvons toujours trouver deux fonctions entières $\varphi(x)$ et $f(x)$ vérifiant l'égalité

$$\varphi(x)\Phi(x) + f(x)F(x) = 1$$

ou

$$\varphi(x)\Phi(x)\Psi(x) + f(x)F(x)\Psi(x) = \Psi(x).$$

Comme, par hypothèse, le produit $\Phi(x)\Psi(x)$ est divisible par $F(x)$, cette égalité nous montre que $F(x)$ est contenu dans $\Psi(x)$, en ce sens, du moins, que

$$m \,.\, \Psi(x) = F(x) \,.\, G(x)$$

$G(x)$ étant une fonction entière à coefficients entiers, et m un nombre entier.

GAUSS a le premier démontré [1] 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. La démonstration est élémentaire et se déduit du théorème cité, que si le produit de deux fonctions entières à coefficients entiers est divisible par un nombre premier p, l'une de ces deux fonctions est elle-même divisible par p.

Comme les coefficients de $\Psi(x)$ sont entiers, et que $F(x)$ est irréductible, nous voyons donc ici que m divise tous les coefficients de $G(x)$.

Supposons maintenant que, par le procédé indiqué plus haut, nous obtenions deux décompositions d'une même fonction entière à coefficients entiers, et, par suite, l'égalité

$$\prod_{(h)} p_h^{i_h} \cdot \prod_{(k)} P_k^{\mu_k}(x) = \prod_{(r)} q_r^{s_r} \cdot \prod_{(\rho)} Q_\rho^{\sigma_\rho}(x) \qquad \begin{pmatrix} h=1, 2, \ldots, \alpha \\ k=1, 2, \ldots, \alpha \\ r=1, 2, \ldots, b \\ \rho=1, 2, \ldots, \beta \end{pmatrix}$$

dans laquelle p, q, i, s, μ, σ sont des nombres, p et q, en particulier, des nombres irréductibles, et $P(x)$, $Q(x)$ des fonctions irréductibles.

Le nombre p_1, par exemple, est alors manifestement contenu dans le terme de droite de cette égalité; chacune des fonctions $Q(x)$ étant irréductible, il faut que p_1 soit contenu dans le produit

$$\prod_{(r)} q_r^{s_r} \qquad (r=1, 2, \ldots, b)$$

donc qu'il soit égal à l'un des nombres $q_1, q_2, \ldots, q_b$. En divisant par ce nombre les deux termes de l'égalité, et en répétant le même raisonnement pour chacun des entiers p et pour chacun des entiers q, aussi longtemps qu'il en reste, nous voyons que l'égalité précédente se réduit à

$$\prod_{(k)} P_k^{\mu_k}(x) = \prod_{(\rho)} Q_\rho^{\sigma_\rho}(x). \qquad \begin{pmatrix} k=1, 2, \ldots, \alpha \\ \rho=1, 2, \ldots, \beta \end{pmatrix}$$

---

[1] *Disquisitiones arithmeticæ*, p. 42.

Mais alors, à cause du théorème précédent, la fonction *irréductible* $P_1(x)$ est égale à l'une des fonctions *irréductibles* $Q(x)$. Divisant, de part et d'autre, par cette fonction, et répétant le même raisonnement sur chacune des fonctions $P(x)$ et $Q(x)$ autant de fois que cela est nécessaire, nous voyons que les deux décompositions de la fonction donnée en facteurs irréductibles, sont identiques.

3. Considérons maintenant une fonction de plusieurs variables indépendantes

$$F(x', x'', \ldots, x^{(n)}).$$

En posant

$$x' = x^{g^0}, \quad x'' = x^{g^1}, \quad x''' = x^{g^2}, \quad \ldots, \quad x^{(n)} = x^{g^{n-1}}$$

et en choisissant g assez grand pour que tous les termes du polynôme

$$F(x', x'', \ldots, x^{(n)})$$

soient de degré différent en x, nous transformerons ce polynôme en une fonction d'une seule variable, $\Phi(x)$, dont tous les termes sont linéairement indépendants. Il est commode de considérer tous les exposants de x comme des nombres écrits dans le système dont la base est g. On voit alors immédiatement qu'il est impossible que $F(x', x'', \ldots, x^{(n)})$ ait un facteur quelconque lorsque $\Phi(x)$ n'en a pas; car à toute égalité

$$F(x', x'', \ldots, x^{(n)}) = F_1(x', x'', \ldots, x^{(n)}) F_2(x', x'', \ldots, x^{(n)})$$

en correspond une autre

$$\Phi(x) = \Phi_1(x)\Phi_2(x)$$

Φ_1 et Φ_2 désignant les transformées respectives de F_1 et F_2, par les substitutions indiquées. Pour reconnaître si $F(x', x'', \ldots, x^{(n)})$ a des diviseurs ou non, il suffit donc de rechercher tous les diviseurs possibles de $\Phi(x)$, ce que nous savons faire à l'aide d'un nombre fini d'opérations, puis de voir si les fonctions de plusieurs variables qui correspondent à ces diviseurs sont vraiment facteurs de $F(x', x'', \ldots, x^{(n)})$ ou non, ce qui n'exige qu'un nombre fini de divisions.

Il est donc légitime d'étendre l'idée d'irréductibilité aux fonctions de plusieurs variables indépendantes. Nous allons en donner une seconde

démonstration, une démonstration par induction; elle nous fera voir plus complètement l'analogie qu'offre la divisibilité des fonctions d'une et de plusieurs variables indépendantes.

Supposons que nous puissions décomposer en ses facteurs irréductibles, chaque fonction entière à coefficients entiers de n variables indépendantes, $x_1, x_2, \ldots, x_n$. Comme nous avons été amené à le faire pour les fonctions d'une variable, nous dirons que $\varphi(x_1, x_2, \ldots, x_n)$ est contenue dans une fonction donnée $f(x_1, x_2, \ldots, x_n)$ lorsque cette dernière peut être mise sous la forme d'un produit de deux fonctions entières *à coefficients entiers*, dont l'une est précisément $\varphi(x_1, x_2, \ldots, x_n)$; et par hypothèse nous pouvons trouver tous les facteurs de $f(x_1, x_2, \ldots, x_n)$, toutes les fonctions contenues dans une fonction quelconque de n variables.

Soit maintenant une fonction de $(n + 1)$ variables indépendantes

$$F(x_0, x_1, \ldots, x_n).$$

Ordonnons cette fonction par rapport à x_0, et désignons par $f_k(x_1, x_2, \ldots, x_n)$ le coefficient de x_0^k. Toute fonction de $x_1, x_2, \ldots, x_n$ contenue dans $F(x_0, x_1, \ldots, x_n)$ est facteur commun de toutes les fonctions $f_k(x_1, x_2, \ldots, x_n)$ que nous savons décomposer en leurs facteurs irréductibles. Nous pouvons donc décomposer $F(x_0, x_1, \ldots, x_n)$ en deux facteurs dont l'un ne dépend que de n variables, et dont l'autre $G(x_0, x_1, \ldots, x_n)$ ordonné par rapport à x_0 a des coefficients sans diviseur commun. Mais alors nous pouvons répéter sur $G(x_0, x_1, \ldots, x_n)$ considérée comme fonction de x_0 seulement, les mêmes raisonnements que nous avons faits sur $F(x)$ tout à l'heure. Seulement les coefficients ne sont plus des nombres entiers, mais des fonctions entières à coefficients entiers de $x_1, x_2, \ldots, x_n$. Conservons les mêmes notations que dans le cas d'une variable. La formule de LAGRANGE nous fait voir qu'un nombre fini d'opérations suffit pour reconnaître si $G(x_0; x_1, x_2, \ldots, x_n)$ a des diviseurs ou non et dans le premier cas, pour trouver ces diviseurs. Pour que $\Phi(x_0; x_1, x_2, \ldots, x_n)$ soit contenue dans $G(x_0; x_1, x_2, \ldots, x_n)$ il faut que $\Phi(r_h; x_1, x_2, \ldots, x_n)$ soit contenue dans $G(r_h; x_1, x_2, \ldots, x_n)$. Par hypothèse, nous pouvons trouver tous les diviseurs d'une fonction de n variables seulement; nous pouvons donc, par un nombre fini d'opérations déterminer tous les systèmes c_k pour lesquels $\sum_{(k)} c_k g_k(x_0)$ peut être diviseur de $G(x_0; x_1, x_2, \ldots, x_n)$; un nombre fini de divisions nous donne enfin tous les facteurs de $G(x_0; x_1, x_2, \ldots, x_n)$.

Cette méthode nous permet de mettre $F(x_0, x_1, \ldots, x_n)$ sous la forme d'un produit de fonctions irréductibles indépendantes de x_0, et de fonctions qui, considérées comme fonctions de x_0 seulement, n'en contiennent plus d'autres. Nous allons maintenant montrer que cette décomposition ne saurait dépendre du choix de la variable suivant laquelle nous ordonnons la fonction $F(x_0, x_1, \ldots, x_n)$.

Il suffit, pour cela, de démontrer que si le produit de deux fonctions $\Phi(x_0, x_1, \ldots, x_n)$ et $\Psi(x_0, x_1, \ldots, x_n)$ est divisible par une fonction irréductible $\varphi(x_1, x_2, \ldots, x_n)$, l'une des deux fonctions Φ ou Ψ, est divisible par φ.

Soient

$$\Phi = a_0 + a_1 x_0 + a_2 x_0^2 + \ldots$$

$$\Psi = b_0 + b_1 x_0 + b_2 x_0^2 + \ldots$$

les a et b désignant des fonctions entières à coefficients entiers de $x_1, x_2, \ldots, x_n$. Si Φ n'est pas divisible par φ, et si a_i est le premier des coefficients a ne contenant pas φ, l'expression

$$\Phi \cdot \Psi - (a_0 + a_1 x_0 + \ldots + a_{i-1} x_0^{i-1})\Psi$$

et par suite

$$(a_i x_0^i + a_{i+1} x_0^{i+1} + \ldots)(b_0 + b_1 x_0 + b_2 x_0^2 + \ldots)$$

sera divisible par φ. Il en résulte que les coefficients de toutes les puissances de x_0 sont divisibles par φ; ces coefficients sont

$$a_i b_0, \quad a_i b_1 + a_{i+1} b_0, \quad a_i b_2 + a_{i+1} b_1 + a_{i+2} b_0, \quad \ldots .$$

Supposons que si le produit de deux fonctions de n variables seulement est divisible par une fonction irréductible, également de n variables, l'une des deux premières fonctions soit nécessairement divisible par la dernière; nous voyons alors que a_i n'étant pas divisible par φ, b_0 contiendra φ; donc aussi $a_i b_1$ et par suite b_1; donc aussi $a_i b_2$ et par suite b_2; etc. Tous les coefficients de $\Psi(x_0)$ contenant φ, il en sera de même de la fonction $\Psi(x_0)$ elle-même, et le théorème est démontré.

Ceci posé, considérons un des facteurs $f(x_0, x_1, \ldots, x_n)$ de $F(x_0, x_1, \ldots, x_n)$; nous pouvons supposer que la fonction $f(x_0, x_1, \ldots, x_n)$ ne contienne pas de

facteurs indépendants de x_0; car si elle en contenait nous pourrions les déterminer et les joindre aux facteurs de $F(x_0, x_1, \ldots, x_n)$ indépendants de x_0.

Puisque $F(x_0, x_1, \ldots, x_n)$ considérée comme fonction de x_0, est divisible par $f(x_0, x_1, \ldots, x_n)$, nous avons, en désignant par k une fonction entière des $(n+1)$ variables $x_0, x_1, \ldots, x_n$ et par h une fonction entière des n variables $x_1, x_2, \ldots, x_n$,

$$F(x_0;\ x_1, \ldots, x_n) = f(x_0;\ x_1, \ldots, x_n)\frac{k(x_0;\ x_1, \ldots, x_n)}{h(x_1, \ldots, x_n)}.$$

Mais F est une fonction *entière* des $(n+1)$ variables $x_0, x_1, \ldots, x_n$, donc la fonction $h(x_1, \ldots, x_n)$ est contenue dans le produit $f.k$; et comme h n'est pas contenue dans f, il faut, d'après le théorème démontré, que h soit contenue dans k; nous avons ainsi

$$F(x_0, x_1, \ldots, x_n) = f(x_0, x_1, \ldots, x_n)g(x_0, x_1, \ldots, x_n)$$

f et g étant des fonctions entières des $(n+1)$ variables $x_0, x_1, \ldots, x_n$.

Nous pouvons donc ou bien décomposer une fonction entière donnée $F(x_0, x_1, \ldots, x_n)$ en d'autres fonctions entières, ou bien montrer que $F(x_0, x_1, \ldots, x_n)$ ne contient aucun facteur entier, et, par suite, classer les fonctions de plusieurs variables indépendantes, comme celles d'une seule variable, en fonctions réductibles et irréductibles; nous pouvons alors énoncer le résultat obtenu en disant que *toute* fonction entière à coefficients entiers est décomposable en ses facteurs irréductibles.

Il nous reste cependant à montrer que le théorème supposé exact pour n variables indépendantes, dans le courant de la démonstration précédente, l'est encore pour $(n+1)$ variables indépendantes.

Si le produit $\Phi(x_0, x_1, \ldots, x_n).\Psi(x_0, x_1, \ldots, x_n)$ est divisible par la fonction *irréductible* $f(x_0, x_1, \ldots, x_n)$, qui, étant irréductible, ne contient aucun facteur indépendant de x_0, et si $\Phi(x_0, x_1, \ldots, x_n)$ ne contient pas $f(x_0, x_1, \ldots, x_n)$, Φ et f considérées comme fonctions de x_0 seulement, seront également sans diviseur commun, et, par suite, nous pourrons déterminer deux fonctions entières de $x_0; x_1, x_2, \ldots, x_n$; Φ_1 et f_1, telles que l'expression $\Phi f_1 + \Phi_1 f$ soit égale à une fonction entière de

$x_1, x_2, \ldots, x_n$ seulement que nous désignerons par $G(x_1, x_2, \ldots, x_n)$. Mais alors nous avons aussi

$$\frac{\Psi\Phi}{f} \cdot f_1 + \Psi\Phi_1 = \frac{G\Psi}{f}.$$

Comme le produit $\Psi\Phi$ est, par hypothèse, divisible par f, l'expression $\frac{G\Psi}{f}$, considérée comme fonction de x_0 seulement, est une fonction entière à coefficients entiers; désignons-la par $H(x_0)$; alors

$$G \,.\, \Psi(x_0) = f(x_0) H(x_0).$$

Puisque la fonction $f(x_0)$ ne contient pas de facteur indépendant de x_0, $f(x_0)$ ne peut être divisible par G; donc $H(x_0)$ contient G; donc $\Psi(x_0)$ contient $f(x_0)$; et nous venons de montrer que si Ψ considérée comme fonction de x_0, contient f, il en est de même de Ψ considérée comme fonction entière à coefficients entiers de ses $(n + 1)$ variables indépendantes $x_0, x_1, \ldots, x_n$.

Nous avons supposé que $f(x_0; x_1, \ldots, x_n)$ était non seulement irréductible en x_0, mais encore ne contenait aucun facteur indépendant de x_0, tout comme dans le cas d'une seule variable indépendante nous n'avons nommée irréductible une fonction de x que lorsqu'elle ne contenait aucune autre fonction de x, et aucun nombre.

Ce théorème nous permet aussi de montrer que la décomposition d'une fonction de plusieurs variables en ses facteurs irréductibles est univoque. La démonstration est identique à celle que nous avons donnée dans le cas d'une seule variable.

En résumé, nous venons de voir que les fonctions entières d'une et de plusieurs variables indépendantes se ramènent aux fonctions *irréductibles* de ces variables.

Toute la démonstration précédente a été faite par induction. J'ai d'abord démontré les théorèmes pour une variable indépendante, puis, les supposant vérifiés pour n variables je les ai démontrés pour $(n + 1)$ variables indépendantes.

4. Les développements précédents ont lieu pour des variables indépendantes quelconques. Pour plus de clarté, je désignerai maintenant par $\mathfrak{R}'$, $\mathfrak{R}''$, ... les variables que j'ai plus particulièrement nommées

variables-indéterminées et je réserverai les lettres x, y, z, ... pour les *variables* proprement dites. Pour abréger l'énoncé des théorèmes et pour réunir en une seule expression les deux cas qui se présentent, celui où nous considérons des variables-indéterminées et celui où nous n'en considérons pas, je conviendrai que lorsqu'il n'y a qu'une variable-indéterminée $\mathfrak{R}$, elle *puisse être* remplacée par l'unité; dans ce cas je *dirai* que cette variable-indéterminée est égale à l'unité.

Demander si une fonction entière est réductible ou non, c'est demander si elle est divisible par une autre fonction entière à coefficients entiers; d'après le théorème de GAUSS dont j'ai fait usage plus haut, je puis même dire par une autre fonction entière à coefficients *rationnels*. Ayant adjoint les variables-indéterminées $\mathfrak{R}$ aux nombres entiers qui font l'objet de nos recherches, il est à la fois naturel et nécessaire d'étendre cette définition de l'irréductibilité.

Si $\mathfrak{R}'$, $\mathfrak{R}''$, ..., $\mathfrak{R}^{(\mu)}$ sont les variables-indéterminées considérées, nous devrons dire qu'une fonction entière de x_0, x_1, ..., x_n, dont les coefficients sont fonctions entières à coefficients entiers de ces variables-indéterminées, est irréductible, lorsqu'elle ne contient aucune autre fonction des variables x_0, x_1, ..., x_n, dont les coefficients soient fonctions entières, à coefficients entiers, des mêmes indéterminées. Pour conserver l'analogie avec le cas où $\mathfrak{R} = 1$, je dirai aussi qu'une fonction entière de x_0, x_1, ..., x_n, dont les coefficients sont fonctions *rationnelles* des variables-indéterminées $\mathfrak{R}'$, $\mathfrak{R}''$, ..., $\mathfrak{R}^{(\mu)}$, est irréductible, lorsqu'elle ne contient aucune autre fonction entière des variables x_0, x_1, ..., x_n, dont les coefficients soient fonctions rationnelles des mêmes variables-indéterminées. Pour fixer les idées je supposerai, une fois pour toutes, que les coefficients de ces fonctions rationnelles soient entiers.

Cette généralisation est légitime; les méthodes des numéros précédents qui permettent de reconnaître, à l'aide d'un nombre fini d'opérations, si une fonction entière contient des diviseurs ou non, sont, en effet, immédiatement applicables. Nous savons trouver les diviseurs de tous les coefficients; car leurs numérateurs et dénominateurs sont fonctions entières à coefficients entiers des variables-indéterminées $\mathfrak{R}'$, ..., $\mathfrak{R}^{(\mu)}$. Nous mettrons donc d'abord la fonction donnée sous la forme d'une fonction entière à coefficients entiers des x_0, x_1, ..., x_n et des $\mathfrak{R}'$, ..., $\mathfrak{R}^{(\mu)}$, divisée par une fonction entière à coefficients entiers des $\mathfrak{R}'$, ..., $\mathfrak{R}^{(\mu)}$, seulement;

nous chercherons ensuite les diviseurs du numérateur et ceux du dénominateur; puis, assignant, *d'une manière arbitraire,* à chaque diviseur du numérateur un nombre quelconque des facteurs du dénominateur, nous ordonnerons chacune des fractions ainsi obtenues par rapport aux variables $x_0, x_1, \ldots, x_n$ dont elles sont fonctions entières, et nous réduirons enfin à leur plus simple expression les fractions qui paraissent comme coefficients et dépendent des variables-indéterminées seulement. L'arbitraire introduit dans cette réduction en facteurs irréductibles, disparaît dès que, chassant tous les dénominateurs, nous retournons dans le domaine réel des fonctions entières à coefficients entiers.

Il convient de désigner tout spécialement, par un nom, l'ensemble des fonctions rationnelles, à coefficients entiers, des variables-indéterminées données, puisque l'irréductibilité en dépend. Nous dirons qu'elles forment *un domaine naturel de rationalité,* le domaine $(\mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)})$. Alors une fonction entière de $x_0, x_1, \ldots, x_n$, sera dite *irréductible dans un domaine* $(\mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)})$ lorsqu'elle ne contient aucune autre fonction entière dont les coefficients fassent partie de ce domaine.

En réalité, c'est l'ensemble des fonctions *entières,* à coefficients entiers, des variables-indéterminées $\mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)}$, qui forme un vrai domaine, que l'on pourrait nommer *domaine d'intégrité.* Mais, comme je l'ai déjà observé dans le premier chapitre, il est commode de se servir des nombres et fonctions rationnelles, et il n'y a aucun inconvénient à s'en servir puisqu'à tout moment on peut chasser les dénominateurs sans rien changer au sens des égalités que l'on considère. C'est pourquoi il convient d'introduire l'idée de *domaine naturel de rationalité,* en même temps que celle de *domaine d'intégrité.*

Remarquons, en terminant, que la convention faite au début de ce numéro, nous permet de comprendre l'idée d'irréductibilité des fonctions entières à coefficients entiers, comme cas particulier, dans l'idée plus générale d'irréductibilité dans un domaine naturel de rationalité $(\mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)})$. Elle répond, en effet, au cas où, symboliquement, $\mathfrak{R}' = 1$ et $\mathfrak{R}'' = \mathfrak{R}''' = \ldots = \mathfrak{R}^{(\mu)} = 0$.

En tenant compte de ces définitions, et des résultats obtenus précédemment, nous pouvons énoncer la proposition fondamentale: *Quel que soit le domaine naturel de rationalité que l'on considère, il est possible de trouver les diviseurs irréductibles d'une fonction entière quelconque, donnée.*

Nous avons ainsi obtenu *la base même* de toutes nos considérations algébriques. Il faut se garder de croire que ces recherches, bien élémentaires il est vrai, ne sont faites que dans le but de systématiser nos connaissances sur la réductibilité des fonctions entières, et qu'elles ne présentent ainsi rien de bien remarquable. Elles sont, au contraire, de la plus haute importance, car elles indiquent déjà la méthode à suivre dans le cas général d'un système de fonctions entières, et il est absolument nécessaire de les placer au début de nos recherches algébriques auxquelles, seules, elles donnent une base à la fois solide et naturelle. Dans la pratique, l'idée d'irréductibilité peut d'ailleurs simplifier considérablement la démonstration de plus d'un théorème.

§ 2.

Résultant de deux fonctions entières.

1. Un domaine naturel de rationalité est supposé connu. Nous partageons ses éléments en trois groupes. Le premier ne contient qu'un élément z, variable ou variable-indéterminée; le second contient des éléments variables $x', x'', \ldots, x^{(\nu)}$; le troisième des éléments indéterminés $\mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)}$.

Considérons deux fonctions *entières* des éléments $z; x', x'', \ldots, x^{(\nu)}$, dont les coefficients soient fonctions rationnelles des éléments $\mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)}$. Après avoir débarassé, s'il y a lieu, ces deux fonctions entières de leur facteur commun, ordonnons-les par rapport à z; soient alors

$$f(z; x', x'', \ldots, x^{(\nu)}) = f_0(x', x'', \ldots, x^{(\nu)})z^m - f_1(x', x'', \ldots, x^{(\nu)})z^{m-1} + \ldots$$
$$\ldots \pm f_m(x', x'', \ldots, x^{(\nu)})$$

$$g(z; x', x'', \ldots, x^{(\nu)}) = g_0(x', x'', \ldots, x^{(\nu)})z^n - g_1(x', x'', \ldots, x^{(\nu)})z^{n-1} + \ldots$$
$$\ldots \pm g_n(x', x'', \ldots, x^{(\nu)});$$

$f_0, f_1, \ldots, f_m$; $g_0, g_1, \ldots, g_n$ désignent des fonctions entières des variables $x', x'', \ldots, x^{(\nu)}$ dont les coefficients sont fonctions rationnelles des indéterminées $\mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)}$.

Les deux fonctions $f(z; x', x'', \ldots, x^{(\nu)})$ et $g(z; x', x'', \ldots, x^{(\nu)})$ n'ont, par hypothèse, aucun diviseur commun tant que les éléments $x', x'', \ldots, x^{(\nu)}$ restent indéterminés. Mais ces éléments sont *variables;* ils peuvent donc prendre des valeurs particulières ou encore être liés par des relations déterminées. Il se pourrait que ces valeurs particulières ou ces relations fussent telles que $f(z; x', x'', \ldots, x^{(\nu)})$ et $g(z; x', x'', \ldots, x^{(\nu)})$ aient précisément un diviseur commun en z. Dans des recherches sur la divisibilité, il importe beaucoup de déterminer celles des valeurs particulières ou des relations pour lesquelles il en est ainsi. C'est pourquoi nous allons nous proposer de rechercher les conditions nécessaires et suffisantes auxquelles doivent satisfaire les variables $x', x'', \ldots, x^{(\nu)}$, pour que les deux fonctions entières $f(z; x', x'', \ldots, x^{(\nu)})$ et $g(z; x', x'', \ldots, x^{(\nu)})$ aient un diviseur commun en z, alors que pour des valeurs indéterminées données à $x' x'', \ldots, x^{(\nu)}$, elles sont supposées sans diviseur commun.

Dans son célèbre Mémoire de 1815, Gauss s'est, le premier, proposé de résoudre un problème semblable, *sans supposer démontrée l'existence des racines des équations algébriques.* Le grand géomètre a donné, dans ce mémoire, la condition nécessaire et suffisante pour qu'une fonction $F(z)$, à coefficients variables, ait avec sa dérivée $F'(z)$ un diviseur commun, $F(z)$ étant supposée sans facteur double pour des valeurs indéterminées de ses coefficients. Nous allons donner la même démonstration dans le cas de deux fonctions entières quelconques $F(z)$ et $G(z)$, à coefficients variables.(1) Ce problème est plus général, et comprend celui que nous nous sommes proposés de résoudre.

Ainsi, en désignant par $\alpha_0, \alpha_1, \ldots, \alpha_m$; $\beta_0, \beta_1, \ldots, \beta_n$, $(m+n+2)$ variables, et par $F(z)$ et $G(z)$ les deux fonctions entières

$$F(z) = \alpha_0 z^m + \alpha_1 z^{m-1} + \ldots + \alpha_m,$$

$$G(z) = \beta_0 z^n + \beta_1 z^{n-1} + \ldots + \beta_n,$$

(1) La première démonstration de ce théorème a été donnée par M. Kronecker, en 1871, dans un Cours professé à l'Université de Berlin.

supposées sans diviseur commun pour des valeurs indéterminées données à $\alpha_0, \alpha_1, \ldots, \alpha_m; \beta_0, \beta_1, \ldots, \beta_n$, *nous cherchons des relations, entre les variables* α *et* β, *qui soient nécessaires et suffisantes pour que* $F(z)$ *et* $G(z)$ *aient un diviseur commun.*

Et cela *sans supposer démontrée l'existence des racines des équations algébriques.* J'ai suffisamment insisté, dans le premier chapitre de ce Mémoire, sur l'importance de cette dernière restriction. D'ailleurs, la méthode de GAUSS doit, d'après M. KRONECKER, servir de type à toutes les recherches d'Algèbre. Il convient donc de la développer avec soin.

A cet effet, nous supposerons d'abord que les variables α et β ne soient pas liées par des relations telles que $F(z)$ et $G(z)$ aient un diviseur commun, puis que les variables α et β soient liées par de telles relations, et nous transformerons successivement ces deux hypothèses en inégalités ou égalités équivalentes.

Considérons d'abord le cas particulier où $\alpha_0 = \beta_0 = 1$.

2. Si $F(z)$ et $G(z)$ n'ont pas de diviseur commun, nous pouvons, à l'aide de l'algorithme du plus grand commun diviseur, déterminer deux fonctions entières de z, $\Phi(z)$ et $\Psi(z)$, vérifiant identiquement l'égalité

$$\Phi(z)F(z) + \Psi(z)G(z) = 1.$$

Les coefficients des deux fonotions $\Phi(z)$ et $\Psi(z)$ sont des fonctions rationnelles des variables $\alpha_1, \alpha_2, \ldots, \alpha_m; \beta_1, \beta_2, \ldots, \beta_n$. Nous pouvons d'ailleurs toujours prendre pour $\Phi(z)$ et $\Psi(z)$ deux fonctions dont le degré, par rapport à z, soit respectivement $(n-1)$ et $(m-1)$; car, puisque

$$[\Phi(z) + h(z)G(z)]F(z) + [\Psi(z) - h(z)F(z)]G(z) = \Phi(z)F(z) + \Psi(z)G(z)$$

nous pouvons toujours choisir la fonction entière $h(z)$ telle que le degré du multiplicateur $\Psi(z)$ soit plus petit que m; celui de $\Phi(z)$ est alors nécessairement plus petit que n.

Comme l'égalité

$$\Phi(z)F(z) + \Psi(z)G(z) = 1$$

et vérifiée identiquement en z, nous pouvons également écrire

$$\Phi(u_k)F(u_k) + \Psi(u_k)G(u_k) = 1 \qquad (k=1, 2, \ldots, m+n)$$

$u_1, u_2, \ldots, u_{m+n}$ désignant $(m+n)$ indéterminées.

Si donc nous formons, à l'aide de ces indéterminées, deux fonctions entières de z

$$\prod_{h=1}^{m}(z-u_h)=P(z) \quad \text{et} \quad \prod_{h=m+1}^{m+n}(z-u_h)=Q(z)$$

nous pouvons écrire

$$\Phi(u_k)[F(u_k)-P(u_k)]+\Psi(u_k)G(u_k)=1 \qquad (k=1,2,\ldots,m)$$

ou encore

$$\prod_{k=1}^{m}\{\Phi(u_k)F(u_k)-\Phi(u_k)P(u_k)+\Psi(u_k)G(u_k)\}=1.$$

Les coefficients de la plus haute puissance de z dans les deux fonctions $F(z)$ et $P(z)$, toutes deux de degré m, sont égaux à l'unité; nous avons donc, en désignant par $\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m$; $\mathfrak{g}_1, \mathfrak{g}_2, \ldots, \mathfrak{g}_n$, les fonctions symétriques élémentaires des indéterminées $u_1, u_2, \ldots, u_m$, d'une part, et $u_{m+1}, u_{m+2}, \ldots, u_{m+n}$, d'autre part,

$$\prod_{k=1}^{m}\{\Phi(u_k)\sum_{h=1}^{m}(-1)^h(\alpha_h-\mathfrak{f}_h)u_k^{m-h}+\Psi(u_k)G(u_k)\}=1.$$

Ce produit est une fonction symétrique entière des indéterminées $u_1, \ldots, u_m$, et par suite une fonction entière des éléments $\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m$. En effectuant la multiplication indiquée, nous obtenons d'ailleurs une fonction dont chaque terme contient au moins un des facteurs $(\alpha_h-\mathfrak{f}_h)$ et que nous pouvons, par suite, considérer comme linéaire et homogène des différences $(\alpha_h-\mathfrak{f}_h)$, à un facteur près

$$\prod_{k=1}^{m}\Psi(u_k)G(u_k).$$

Le produit $\prod_{k=1}^{m}G(u_k)$ est, d'après le théorème fondamental de la théorie des fonctions symétriques, une fonction entière des éléments $\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m$; $\beta_1, \beta_2, \ldots, \beta_n$; et le produit $\prod_{k=1}^{m}\Psi(u_k)$ est, d'après le même théorème, une fonction entière des éléments $\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m$. Si donc nous posons

$$\prod_{k=1}^{m} G(u_k) = R(\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m; \beta_1, \beta_2, \ldots, \beta_n)$$

$$\prod_{k=1}^{m} \Psi(u_k) = S(\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m)$$

et que nous désignions par K une fonction entière des éléments $\mathfrak{f}_1, \ldots, \mathfrak{f}_m$ nous voyons que l'égalité précédente peut être mise sous la forme

$$\sum_{h=1}^{m} (\alpha_h - \mathfrak{f}_h) K_h(\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m)$$

$$+ R(\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m; \beta_1, \beta_2, \ldots, \beta_n) S(\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m) = 1.$$

Nous avons obtenu cette égalité par une simple transformation de l'identité

$$\Phi(z) F(z) + \Psi(z) G(z) = 1.$$

Elle est donc, elle-même, vérifiée identiquement en $u_1, u_2, \ldots, u_m$. Mais les fonctions symétriques élémentaires de m variables indépendantes forment un système de m variables également indépendantes. Il en résulte que l'égalité que nous venons d'établir est vérifiée identiquement en $\mathfrak{f}_1, \ldots, \mathfrak{f}_m$; elle a donc lieu lorsque nous substituons aux indéterminées $\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m$, les valeurs particulières $\alpha_1, \alpha_2, \ldots, \alpha_m$. Ainsi se trouve démontrée, pour des systèmes quelconques $\alpha_1, \alpha_2, \ldots, \alpha_m; \beta_1, \beta_2, \ldots, \beta_n$, vérifiant notre première hypothèse, l'égalité

$$R(\alpha_1, \alpha_2, \ldots, \alpha_m; \beta_1, \beta_2, \ldots, \beta_n) S(\alpha_1, \alpha_2, \ldots, \alpha_m) = 1.$$

Si nous observons que $S(\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m)$ était une fonction *entière* des indéterminées $\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m$, à coefficients rationnels *déterminés* de $\alpha_1, \alpha_2, \ldots, \alpha_m; \beta_1, \beta_2, \ldots, \beta_n$, nous voyons que la valeur de cette fonction est finie lorsqu'on y substitue à $\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m$, les variables $\alpha_1, \alpha_2, \ldots, \alpha_m$. Nous en concluons que la fonction $R(\alpha_1, \alpha_2, \ldots, \alpha_m; \beta_1, \beta_2, \ldots, \beta_n)$ ne saurait être nulle.

Donc, si les variables α et β sont liées par des relations telles, que la fonction $R(\alpha_1, \alpha_2, \ldots, \alpha_m; \beta_1, \beta_2, \ldots, \beta_n)$ soit égale à zéro, les deux fonctions $F(z)$ et $G(z)$ auront nécessairement un diviseur commun en z.

Car si elles n'en avaient pas, nous venons de voir que R serait différent de zéro.

Dans tout ce qui précède nous n'avons considéré que les m indéterminées $u_1, u_2, \ldots, u_m$ qui définissent la fonction $P(z)$; rien ne nous empêche de répéter les mêmes raisonnements en prenant comme point de départ les m indéterminées $u_{m+1}, u_{m+2}, \ldots, u_{m+n}$ qui définissent la fonction $Q(z)$. Nous obtenons alors une fonction entière R_1 définie par l'égalité

$$R_1(\alpha_1, \alpha_2, \ldots, \alpha_m; \beta_1, \beta_2, \ldots, \beta_n) = \prod_{k=m+1}^{m+n} F(u_k)$$

et nous arrivons, comme tout à l'heure, au résultat que si les variables α et β sont liées par des relations telles, que la fonction $R_1(\alpha_1, \alpha_2, \ldots, \alpha_m; \beta_1, \beta_2, \ldots, \beta_n)$ soit égale à zéro, les deux fonctions $F(z)$ et $G(z)$ ont nécessairement un diviseur commun en z.

Posons, pour un instant, $u_{m+i} = v_i$; nous aurons alors

$$\prod_{k=1}^{m} Q(u_k) = \prod_{k=1}^{m}\prod_{h=1}^{n}(u_k - v_h) = (-1)^{mn}\prod_{h=1}^{n}\prod_{k=1}^{m}(v_h - u_k)$$

$$\prod_{k=m+1}^{m+n} P(u_k) = \prod_{h=1}^{n} P(v_h) = \prod_{h=1}^{n}\prod_{k=1}^{m}(v_h - u_k)$$

donc

$$\prod_{k=1}^{m} Q(u_k) = (-1)^{mn}\prod_{k=m+1}^{m+n} P(u_k).$$

Ainsi les deux fonctions R et R_1 sont égales, au signe près, pour des fonctions F et G à coefficients indéterminés. Il est, en effet, manifeste que pour $\alpha_1, \alpha_2, \ldots, \alpha_m; \beta_1, \beta_2, \ldots, \beta_n$ indéterminés, les fonctions P et F et, de même, les fonctions Q et G, sont identiques.

Les deux termes de l'égalité

$$\prod_{k=1}^{m} Q(u_k) = \pm \prod_{k=m+1}^{m+n} P(u_k)$$

sont fonctions symétriques des indéterminées $u_1, u_2, \ldots, u_m$ d'une part et des indéterminées $u_{m+1}, \ldots, u_{m+n}$ de l'autre; cette égalité a d'ailleurs lieu *identiquement* en $u_1, u_2, \ldots, u_m; u_{m+1}, \ldots, u_{m+n}$; donc aussi en

$\mathfrak{f}_1, \ldots, \mathfrak{f}_m; \mathfrak{g}_1, \mathfrak{g}_2, \ldots, \mathfrak{g}_n$; elle a donc également lieu si l'on y substitue à $\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m; \mathfrak{g}_1, \mathfrak{g}_2, \ldots, \mathfrak{g}_n$ les variables $\alpha_1, \alpha_2, \ldots, \alpha_m; \beta_1, \beta_2, \ldots, \beta_n$ liées par les relations considérées, ce qui démontre l'égalité, au signe près, des deux fonctions $R(\alpha_1, \alpha_2, \ldots, \alpha_m; \beta_1, \beta_2, \ldots, \beta_n)$ et $R_1(\alpha_1, \alpha_2, \ldots, \alpha_m; \beta_1, \beta_2, \ldots, \beta_n)$.

Cette remarque nous permet de donner une méthode pour trouver, dans chaque cas particulier, la fonction $R(\alpha_1, \alpha_2, \ldots, \alpha_m; \beta_1, \beta_2, \ldots, \beta_n)$. En effet, si

$$H(z) = \prod_{k=1}^{m+n} (z - u_k)$$

l'expression

$$\sum_{k=1}^{m+n} \frac{H(z)}{(z - u_k) H'(u_k)}$$

est une fonction de z, qui, pour $z = u_k$, se réduit à l'unité. Elle représente donc la fonction de degré $(m + n - 1)$

$$\Phi(z) F(z) + \Psi(z) G(z)$$

qui est *identiquement* égale à l'unité, et nous pouvons écrire

$$\sum_{k=1}^{m+n} \frac{H(z)}{(z - u_k) H'(u_k)} = 1$$

ou encore, puisque $H(z) = P(z)Q(z)$

$$\sum_{k=1}^{m} \frac{P(z)Q(z)}{z - u_k} \frac{1}{P'(u_k)Q(u_k)} + \sum_{k=m+1}^{m+n} \frac{P(z)Q(z)}{z - u_k} \frac{1}{P(u_k)Q'(u_k)}.$$

En chassant le dénominateur,

$$\prod_{k=1}^{m} Q(u_k) = \pm \prod_{k=m+1}^{m+n} P(u_k) = R(\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m; \mathfrak{g}_1, \mathfrak{g}_2, \ldots, \mathfrak{g}_n)$$

il vient,

$$R(\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m; \mathfrak{g}_1, \mathfrak{g}_2, \ldots, \mathfrak{g}_n)$$

$$= \sum_{k=1}^{m} \frac{P(z)Q(z)Q(u_1)Q(u_2) \ldots Q(u_{k-1})Q(u_{k+1}) \ldots Q(u_m)}{(z - u_k)P'(u_k)}$$

$$\pm \sum_{k=m+1}^{m+n} \frac{P(z)Q(z)P(u_{m+1})P(u_{m+2}) \ldots P(u_{k-1})P(u_{k+1}) \ldots P(u_{m+n})}{(z - u_k)Q'(u_k)}.$$

Mais $\frac{P(z)}{z-u_k}$ et $\frac{Q(z)}{z-u_k}$ sont des fonctions entières de z et de u_k que nous désignerons par $P_1(z;\ u_k)$ et $Q_1(z;\ u_k)$; les deux produits

$$Q(u_1)Q(u_2)\ \ldots\ Q(u_{k-1})Q(u_{k+1})\ \ldots\ Q(u_m)$$

et

$$\pm\, P(u_{m+1})P(u_{m+2})\ \ldots\ P(u_{k-1})P(u_{k+1})\ \ldots\ P(u_{m+n})$$

sont des fonctions entières de u_k; nous les désignerons par $Q^*(u_k)$ et $P^*(u_k)$. Alors l'expression $P_1(z;\ u_k)Q^*(u_k)$ sera une fonction entière de u_k; à l'aide de l'équation $P(u_k) = 0$ $(k = 1,\ 2,\ \ldots,\ m)$, nous la réduirons au degré $(m-1)$; elle peut donc être mise sous la forme

$$q_1u_k^{m-1} + q_2u_k^{m-2} + \ldots + q_m;$$

de même, à l'aide de l'équation $Q(u_k) = 0$ $(k = m+1,\ m+2,\ \ldots,\ m+n)$, l'expression $Q_1(z;\ u_k)P^*(u_k)$ peut être mise sous la forme

$$p_1u_k^{n-1} + p_2u_k^{n-2} + \ldots + p_n;$$

les coefficients $p_1,\ p_2,\ \ldots,\ p_n;\ q_1,\ q_2,\ \ldots,\ q_m$, désignent des fonctions entières de z.

Nous obtenons ainsi l'égalité,

$$R(\mathfrak{f}_1,\ \mathfrak{f}_2,\ \ldots,\ \mathfrak{f}_m;\ \mathfrak{g}_1,\ \mathfrak{g}_2,\ \ldots,\ \mathfrak{g}_n)$$

$$= Q(z)\sum_{k=1}^{m}\frac{q_1u_k^{m-1} + q_2u_k^{m-2} + \ldots + q_m}{P'(u_k)} + P(x)\sum_{k=m+1}^{m+n}\frac{p_1u_k^{n-1} + p_2u_k^{n-2} + \ldots + p_n}{Q'(u_k)}.$$

Les formules d'Euler

$$\sum_{k=1}^{m}\frac{u_k^{m-i}}{P'(u_k)} = \sum_{k=m+1}^{m+n}\frac{u_k^{n-i}}{Q'(u_k)} = \begin{cases} 1, \text{ pour } i = 1 \\ 0, \text{ pour } i > 1 \end{cases}$$

nous permettent de réduire cette égalité à la suivante, identique en $\mathfrak{f}_1,\ \mathfrak{f}_2,\ \ldots,\ \mathfrak{f}_m;\ \mathfrak{g}_1,\ \mathfrak{g}_2,\ \ldots,\ \mathfrak{g}_n$,

$$R(\mathfrak{f}_1,\ \mathfrak{f}_2,\ \ldots,\ \mathfrak{f}_m;\ \mathfrak{g}_1,\ \mathfrak{g}_2,\ \ldots,\ \mathfrak{g}_n) = q_1(z)Q(z) + p_1(z)P(z).$$

Si donc on nous proposait, dans un cas particulier quelconque, de former la fonction $R(\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_m;\ \beta_1,\ \beta_2,\ \ldots,\ \beta_n)$ correspondant à deux fonctions données $F(z)$ et $R(z)$, nous formerions à l'aide des indéterminées

$u_1, u_2, \ldots, u_{m+n}$ les deux fonctions auxiliaires $P(z)$ et $Q(z)$, et la méthode précédente nous permettrait de déterminer deux fonctions $p_1(z)$ et $q_1(z)$ telles que $p_1(z)P(z) + q_1(z)Q(z)$ se réduise à une fonction entière des indéterminées $\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m; \mathfrak{g}_1, \mathfrak{g}_2, \ldots, \mathfrak{g}_n$. Si dans cette fonction, nous substituons $\alpha_1, \alpha_2, \ldots, \alpha_m; \beta_1, \beta_2, \ldots, \beta_n$, à $\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m; \mathfrak{g}_1, \mathfrak{g}_2, \ldots, \mathfrak{g}_n$, nous obtenons la fonction cherchée,

$$R(\alpha_1, \alpha_2, \ldots, \alpha_m; \beta_1, \beta_2, \ldots, \beta_n).$$

Nous pouvons résumer les recherches précédentes en disant que l'unique condition

$$R(\alpha_1, \alpha_2, \ldots, \alpha_m; \beta_1, \beta_2, \ldots, \beta_n) = 0$$

est *suffisante,* pour que les deux fonctions $F(z)$ et $G(z)$ aient un diviseur commun.

3. L'algorithme du plus grand commun diviseur suffit pour nous donner la condition *nécessaire.*

Comme $P(z)$ et $Q(z)$ n'ont, par hypothèse, aucun diviseur commun (puisque leurs coefficients $\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m$ et $\mathfrak{g}_1, \mathfrak{g}_2, \ldots, \mathfrak{g}_n$ sont indéterminés), nous savons trouver deux fonctions entières de z, $\varphi(z)$ et $\psi(z)$, à coefficients rationnels en $\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m; \mathfrak{g}_1, \mathfrak{g}_2, \ldots, \mathfrak{g}_n$, telles que

$$\varphi(z)P(z) + \psi(z)Q(z) = 1.$$

Réduisons au même dénominateur les fonctions $\varphi(z)$ et $\psi(z)$, et chassons ce dénominateur. L'égalité précédente devient alors

$$p(z)P(z) + q(z)Q(z) = T(\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m; \mathfrak{g}_1, \mathfrak{g}_2, \ldots, \mathfrak{g}_n)$$

où les coefficients de $p(z)$, $q(z)$, et T lui-même sont fonctions entières, à coefficients entiers, de $\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m; \mathfrak{g}_1, \mathfrak{g}_2, \ldots, \mathfrak{g}_n$. Si nous réduisons les degrés de $\varphi(z)$ et $\psi(z)$ à $(n-1)$ et $(m-1)$, il est facile de voir que les deux multiplicateurs $\varphi(z)$ et $\psi(z)$ sont déterminés univoquement; il en résulte que les trois fonctions $p(z)$, $q(z)$ et T sont, au signe près, également déterminées d'une manière univoque, si nous convenons de débarasser T et les coefficients de $p(z)$ et $q(z)$ des facteurs qu'ils pourraient avoir tous en commun. L'existence et l'univocité, au signe près, des fonctions entières $p(z)$, $q(z)$, T, est ainsi démontrée; elle repose sur la possibilité de trouver les diviseurs d'une fonction entière quelconque.

Ceci posé, supposons que $F(z)$ et $G(z)$ aient un diviseur commun; il faudra alors que ce diviseur soit contenu dans la fonction T que l'on obtient en substituant à $\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m; \mathfrak{g}_1, \mathfrak{g}_2, \ldots, \mathfrak{g}_n$, les coefficients $\alpha_1, \alpha_2, \ldots, \alpha_m; \beta_1, \beta_2, \ldots, \beta_n$ des deux fonctions $F(z)$ et $G(z)$; car l'égalité précédente est identique en $\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m; \mathfrak{g}_1, \mathfrak{g}_2, \ldots, \mathfrak{g}_n$. Les coefficients des plus hautes puissances de $F(z)$ et de $G(z)$ sont égaux à l'unité; un diviseur commun à $F(z)$ et à $G(z)$ dépend donc nécessairement de z, et, par suite, $T(\alpha_1, \ldots, \alpha_m; \beta_1, \ldots, \beta_n)$ qui est indépendant de z, est égal à zéro.

Nous avons ainsi trouvé *une condition nécessaire* pour que les deux fonctions $F(z)$ et $G(z)$ aient un diviseur commun.

4. Il est maintenant naturel de rechercher si les deux fonctions

$$R(\alpha_1, \alpha_2, \ldots, \alpha_m; \beta_1, \beta_2, \ldots, \beta_n) \text{ et } T(\alpha_1, \alpha_2, \ldots, \alpha_m; \beta_1, \beta_2, \ldots, \beta_n)$$

sont indépendantes ou non, et, si elles ne le sont pas, de chercher à trouver les relations qui les lient l'une à l'autre.

Dans ce but, nous démontrerons d'abord que dans le *domaine d'intégrité* $(\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m; \mathfrak{g}_1, \mathfrak{g}_2, \ldots, \mathfrak{g}_n)$, la fonction R est irréductible. Cela est facile. Nous avons, en effet, *identiquement* en $u_1, u_2, \ldots, u_m; v_1, v_2, \ldots, v_n$,

$$R(\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m; \mathfrak{g}_1, \mathfrak{g}_2, \ldots, \mathfrak{g}_n) = \prod_{(h,k)} (u_h - v_k). \qquad \binom{h=1, 2, \ldots, m}{k=1, 2, \ldots, n}$$

Supposons donc que R soit réductible dans le domaine d'intégrité considéré; l'un de ses facteurs contiendra alors nécessairement une des différences du double produit qui est égal à R, par exemple $u_h - v_k$, et si nous désignons ce facteur par R_1, nous avons identiquement en $u_1, u_2, \ldots, u_m; v_1, v_2, \ldots, v_n$,

$$R_1(\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m; \mathfrak{g}_1, \mathfrak{g}_2, \ldots, \mathfrak{g}_n) \equiv 0 \pmod{u_h - v_k}$$

et par suite, à cause de l'identité en $u_1, u_2, \ldots, u_m$,

$$R_1(\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m; \mathfrak{g}_1, \mathfrak{g}_2, \ldots, \mathfrak{g}_n) \equiv 0 \pmod{u_i - v_k}. \qquad (i=1, 2, \ldots, m)$$

Comme les m fonctions linéaires $(u_i - v_k)$, $(i = 1, 2, \ldots, m)$, n'ont aucun diviseur commun, nous aurons donc, toujours identiquement en $u_1, u_2, \ldots, u_m; v_1, v_2, \ldots, v_n$,

$$R_1(\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m; \mathfrak{g}_1, \mathfrak{g}_2, \ldots, \mathfrak{g}_n) \equiv 0 \ [\mathrm{mod} \prod_{i=1}^{m} (u_i - v_k)]$$

et par suite, à cause de l'identité en $v_1, v_2, \ldots, v_n$, la même congruence pour $k = 1, 2, \ldots, n$, ou encore, comme les n modules $\prod_{i=1}^{m}(u_i - v_k)$, $(k = 1, 2, \ldots, n)$ n'ont aucun diviseur commun,

$$R_1(\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m; \mathfrak{g}_1, \mathfrak{g}_2, \ldots, \mathfrak{g}_n) \equiv 0 \ [\mathrm{mod} \prod_{(i,k)} (u_i - v_k)]. \quad \binom{i=1,2,\ldots,m}{k=1,2,\ldots,n}$$

Si donc la fonction R_1 contient un facteur linéaire $(u_h - v_k)$ de la résultante $R(\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m; \mathfrak{g}_1, \mathfrak{g}_2, \ldots, \mathfrak{g}_n)$, elle contient aussi nécessairement le double produit qui est identique à cette résultante elle-même. L'irréductibilité de R, dans le domaine considéré, est ainsi démontrée.

Ceci posé, comparons les deux fonctions $R(\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m; \mathfrak{g}_1, \mathfrak{g}_2, \ldots, \mathfrak{g}_n)$ et $T(\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m; \mathfrak{g}_1, \mathfrak{g}_2, \ldots, \mathfrak{g}_n)$.

Nous avions obtenu les deux égalités

$$p_1(z)P(z) + q_1(z)Q(z) = R$$
$$p(z)P(z) + q(z)Q(z) = T.$$

Nous en tirons, par soustraction,

$$[p_1(z) - p(z)]P(z) + [q_1(z) - q(z)]Q(z) = R - T$$

ou encore, [$q_1(z)$ est différent de zéro]

$$q_1(z)[p_1(z) - p(z)]P(z) + [q_1(z) - q(z)][R - p_1(z)P(z)] = q_1(z)(R - T).$$

Nous voyons donc que la différence $q_1(z)T - q(z)R$, dont le degré, par rapport à z, est plus petit que m, est divisible par $P(z)$ dont le degré, par rapport à z, est égal à m; ce qui n'est possible que si

$$q_1(z)T - q(z)R = 0.$$

Il faut donc que la fonction $q(z)$ soit contenue dans le produit $q_1(z)T$, et, par suite, que $q(z)$ soit un diviseur de $q_1(z)$; car si $q(z)$ contenait un facteur indépendant de z qui fût également contenu dans T, comme le coefficient de la plus haute puissance de $P(z)$ est l'unité, ce facteur serait

aussi contenu dans $p(z)$, et $p(z)$, $q(z)$, T, auraient un facteur commun contrairement à ce que nous avons dit dans le numéro précédent.

Soit donc

$$q_1(z) = t(z)q(z);$$

remplaçons, dans l'égalité précédente, $q_1(z)$ par sa valeur, et divisons par la fonction $q(z)$ qui est différente de zéro; il vient

$$t(z)T = R.$$

Ainsi T est contenue dans R; mais R est irréductible; donc

$$T = R.$$

Cette même égalité, démontrée dans le domaine $(\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m; \mathfrak{g}_1, \mathfrak{g}_2, \ldots, \mathfrak{g}_n)$ a évidemment encore lieu lorsque l'on substitue aux indéterminées $\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m; \mathfrak{g}_1, \mathfrak{g}_2, \ldots, \mathfrak{g}_n$, les variables $\alpha_1, \alpha_2, \ldots, \alpha_m; \beta_1, \beta_2, \ldots, \beta_n$, quelles que soient d'ailleurs les relations qui lient ces variables.

La condition nécessaire que nous avons trouvée, et la condition suffisante sont donc identiques, et nous pouvons dire:

»La condition nécessaire et suffisante à laquelle doivent satisfaire les variables x', x'', $\ldots$, $x^{(\nu)}$, pour que les deux fonctions entières $f(z; x', x'', \ldots, x^{(\nu)})$ et $g(z; x' x'', \ldots, x^{(\nu)})$ de la page 21 aient un diviseur commun en z, est, dans le cas particulier où $f_0 = g_0 = 1$,

$$R(f_1, f_2, \ldots, f_m; g_1, g_2, \ldots, g_n) = 0.$$

Cette fonction R est le *résultant* des deux fonctions $f(z)$ et $g(z)$; d'après ce qui précède, nous savons le former, quels que soient les coefficients de $f(z)$ et de $g(z)$. Remarquons, en passant, qu'en réalité c'est $R = 0$ qui est l'équation résultante des deux équations $f(z) = 0$ et $g(z) = 0$.«

5. J'ai, dans ce qui précède, défini le résultant de deux fonctions entières, et, comme une fonction entière *déterminée* des coefficients des deux fonctions entières données, et, comme une fonction entière facile à déterminer dans chaque cas particulier, à l'aide de l'algorithme du plus grand commun diviseur appliqué aux deux fonctions entières données. J'ai ensuite montré que les deux fonctions, ainsi définies, étaient identiques. Il me reste à ramener, au cas particulier considéré, le cas général où les

deux fonctions $f_0(x', x'', \ldots, x^{(\nu)})$ et $g_0(x', x'', \ldots, x^{(\nu)})$ ne sont pas égales à l'unité. Il suffit, de nouveau, de considérer les deux fonctions $F(z)$ et $G(z)$ dans lesquelles les coefficients α_0 et β_0 ne sont pas égaux à l'unité.

Soient

$$F_1(z) = \frac{1}{\alpha_0} F(z) \text{ et } G_1(z) = \frac{1}{\beta_0} G(z);$$

le résultant des deux fonctions $F_1(z)$ et $G_1(z)$ est une fonction entière de $\frac{\alpha_1}{\alpha_0}, \frac{\alpha_2}{\alpha_0}, \ldots, \frac{\alpha_m}{\alpha_0}, \frac{\beta_1}{\beta_0}, \frac{\beta_2}{\beta_0}, \ldots, \frac{\beta_n}{\alpha_0}$. Il est d'ailleurs égal au produit

$$\prod_{k=1}^{m} G_1(u_k)$$

dans lequel on a remplacé les fonctions symétriques élémentaires de $u_1, u_2, \ldots, u_m$ par les coefficients $\frac{\alpha_1}{\alpha_0}, \frac{\alpha_2}{\alpha_0}, \ldots, \frac{\alpha_m}{\alpha_0}$. Si donc nous multiplions ce produit par $\alpha_0^n \beta_0^m$, ce qui revient à multiplier le produit

$$\prod_{k=1}^{m} G(u_k)$$

par α_0^n, nous obtenons une fonction entière de $\alpha_0, \alpha_1, \ldots, \alpha_m; \beta_0, \beta_1, \ldots, \beta_n$; d'ailleurs

$$\mathfrak{f}_0^n \prod_{k=1}^{m} Q(u_k) = \mathfrak{f}_0^n \mathfrak{g}_0^m \sum_{k=1}^{m} \prod_{h=1}^{n} (u_k - v_h) = \mathfrak{g}_0^m \prod_{h=1}^{n} P(v_h).$$

Il convient donc de considérer cette fonction entière, comme *le résultant* des deux fonctions $F(z)$ et $G(z)$.

Le résultant de $P(z)$ et de $Q(z)$ est irréductible. Nous savons, en effet, que le double produit

$$\prod_{k=1}^{m} \prod_{h=1}^{n} (u_k - v_h)$$

est irréductible dans le domaine $(\mathfrak{f}_0, \mathfrak{f}_1, \ldots, \mathfrak{f}_m; \mathfrak{g}_0, \ldots, \mathfrak{g}_n)$; si donc le résultant de $P(z)$ et de $Q(z)$ était réductible, il aurait tout au plus un facteur indépendant de z, $\mathfrak{f}_0$ ou $\mathfrak{g}_0$. Mais dans le produit

$$\mathfrak{f}_0^n \prod_{k=1}^{m} Q(u_k)$$

le terme indépendant de $u_1, u_2, \ldots, u_n$, est égal à $\mathfrak{f}_0^n \mathfrak{g}_n^m$; et dans le produit

$$\mathfrak{g}_0^m \prod_{h=1}^{n} P(v_h)$$

il est égal à $\mathfrak{g}_0^m \mathfrak{f}_m^n$. Ni $\mathfrak{f}_0$, ni $\mathfrak{g}_0$ ne sont donc contenus dans le résultant des deux fonctions $P(z)$ et $Q(z)$; ce résultant est donc bien irréductible.

Le problème proposé peut ainsi être considéré, comme entièrement résolu.

§ 3.

Domaine général de rationalité.

1. Considérons une fonction entière de x, de degré n, irréductible dans une domaine naturel de rationalité $(\Re', \Re'', \ldots, \Re^{(\mu)})$. Egalons cette fonction à zéro; l'équation ainsi obtenue est dite irréductible, et ses n racines $\xi_1, \xi_2, \ldots, \xi_n$ sont dites *fonctions algébriques conjuguées* de $\Re', \Re'', \ldots, \Re^{(\mu)}$; dans le cas particulier où le domaine se réduit à l'unité, c'est à dire où les coefficients sont des nombres entiers, les racines $\xi_1, \xi_2, \ldots, \xi_n$ sont dites *nombres algébriques conjugués.*

C'est ici que nous supposerons connue la démonstration de GAUSS sur l'existence des racines d'une équation algébrique, telle qu'elle a été interprétée par M. KRONECKER, qui, après avoir ramené le cas général à celui des racines réelles, *sépare* tout d'abord les intervalles dans lesquels une équation peut être vérifiée approximativement. (1) Il est alors parfaitement rigoureux, pour abréger le langage, de dire qu'une équation a n racines. Cette introduction en algèbre d'un symbole qui lui est étranger, a, comme je l'ai exposé dans le premier chapitre de ce mémoire, au moins dans l'état actuel de la science, ses avantages et ses inconvénients. Pour faire saisir, en partie du moins, les uns et les autres, je reprendrai dans le chapitre suivant, à l'aide des systèmes de diviseurs, la question importante que j'aborderai tout à l'heure, dans le paragraphe

(1) Comparez page 4.

4 de ce chapitre, à l'aide des fonctions algébriques, et je montrerai comment on peut la résoudre sans l'emploi de ces symboles. Mais comme il m'a été impossible de démontrer de la même manière la décomposition générale des systèmes de diviseurs, dont la question traitée dans le paragraphe 4 n'est qu'un cas particulier, j'ai préféré introduire, dès maintenant, les éléments auxiliaires, dont j'aurais parfaitement pu me passer dans tout ce chapitre. Je ne les ai pas introduits, dès le début de ce chapitre, parce que quelques-uns des résultats obtenus jusqu'ici sont nécessaires pour la démonstration de la séparation des racines possibles d'une équation algébrique donnée, et de l'existence d'un nombre rationnel vérifiant cette équation avec une approximation aussi grande que l'on veut.

Ainsi nous parlerons de fonctions algébriques, de nombre algébriques; mais, encore une fois, il est bien entendu que ces fonctions algébriques, ces nombres algébriques, n'ont aucune existence par eux-mêmes, que nous y adjoindrons toujours l'équation $f(x; \mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)}) = 0$ qui les définit, f étant une fonction entière, que c'est cette équation qui a un sens algébrique, que c'est son adjonction qui seule nous permet d'introduire, pour abréger, l'idée approximative de fonction algébrique, au même titre que celle de fonction rationnelle.

2. Dans un grand nombre de recherches les éléments du domaine de rationalité sont liés par une équation algébrique. Nous *dirons* alors que, dans ces recherches, on considère comme connue une fonction algébrique déterminée ou encore que nous *adjoignons* au domaine naturel de rationalité $(\mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)})$ une fonction algébrique $\mathfrak{G}$ de ces indéterminées. Le nouveau domaine $(\mathfrak{G}, \mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)})$ comprend toutes les fonctions rationnelles de $\mathfrak{G}, \mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)}$. Ces fonctions rationnelles sont, toutes, des fonctions algébriques de $\mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)}$. En effet, si $\mathfrak{G}$ est racine de $F(\mathfrak{G}) = 0$ et si $R(\mathfrak{G}) = \mathfrak{G}_1$ désigne une fonction rationnelle quelconque de $\mathfrak{G}$, $\mathfrak{G}_1$ sera racine de l'équation

$$\Pi(z - \mathfrak{G}_1) = 0$$

où le produit est étendu à toutes les racines de $F(\mathfrak{G}) = 0$. Ce produit est fonction symétrique des racines de l'équation $F(\mathfrak{G}) = 0$, donc fonction rationnelle des coefficients de cette équation. $\mathfrak{G}_1$ et $\mathfrak{G}$, et, par suite, toutes les fonctions du domaine $(\mathfrak{G}, \mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)})$ sont donc fonctions algébriques des mêmes indéterminées.

Parmi les fonctions algébriques comprises dans le domaine

$$(\mathfrak{G},\ \mathfrak{R}',\ \mathfrak{R}'',\ \ldots,\ \mathfrak{R}^{(\mu)})$$

celles qui sont d'un *ordre* donné k, c'est à dire celles qui vérifient une équation dont le degré est k, forment un *genre d'ordre k*. $\mathfrak{G}$ étant d'ordre n, il y a certainement un genre d'ordre n. Ce genre *dérive* du domaine naturel $(\mathfrak{R}',\ \mathfrak{R}'',\ \ldots,\ \mathfrak{R}^{(\mu)})$.

Les fonctions algébriques conjuguées déterminent des genres qui s'ils sont différents, sont dits *genres conjuguées.*

Le nombre k est nécessairement un diviseur du nombre n. Soit, en effet,

$$F(\mathfrak{G};\ \mathfrak{R}',\ \mathfrak{R}'',\ \ldots,\ \mathfrak{R}^{(\mu)}) = 0$$

une équation irréductible de degré n, définissant les fonctions conjuguées $\mathfrak{G}_1,\ \mathfrak{G}_2,\ \ldots,\ \mathfrak{G}_n$; et soit

$$\mathfrak{g} = \Phi(\mathfrak{G}_k,\ \mathfrak{R}',\ \ldots,\ \mathfrak{R}^{(\mu)})$$

une fonction rationnelle de $\mathfrak{G}_k,\ \mathfrak{R}',\ \mathfrak{R}'',\ \ldots,\ \mathfrak{R}^{(\mu)}$. Le produit

$$\prod_{k=1}^{n} [\mathfrak{g} - \Phi(\mathfrak{G}_k)]$$

est une fonction entière de $\mathfrak{g}$ dont les coefficients sont fonctions rationnelles de $\mathfrak{R}',\ \mathfrak{R}'',\ \ldots,\ \mathfrak{R}^{(\mu)}$. Cette fonction entière $G(\mathfrak{g};\ \mathfrak{R}',\ \mathfrak{R}'',\ \ldots,\ \mathfrak{R}^{(\mu)})$ peut être réductible; soit $H(\mathfrak{g};\ \mathfrak{R}',\ \mathfrak{R}'',\ \ldots,\ \mathfrak{R}^{(\mu)})$ un de ses facteurs irréductibles. Comme la fonction entière $H[\Phi(\mathfrak{G}_k);\ \mathfrak{R}',\ \mathfrak{R}'',\ \ldots,\ \mathfrak{R}^{(\mu)}]$ s'annule pour une des n racines $\mathfrak{G}_k$ de l'équation irréductible $F(\mathfrak{G}) = 0$, elle s'annule pour toutes les racines de cette équation. Ainsi

$$H[\Phi(\mathfrak{G}_k);\ \mathfrak{R}',\ \mathfrak{R}'',\ \ldots,\ \mathfrak{R}^{(\mu)}] = 0$$

pour $k = 1, 2, \ldots, n$. Cette même relation ayant lieu pour tous les facteurs irréductibles de $G(\mathfrak{g};\ \mathfrak{R}',\ \mathfrak{R}'',\ \ldots,\ \mathfrak{R}^{(\mu)})$, ces facteurs irréductibles sont identiques, et nous avons

$$G(\mathfrak{g};\ \mathfrak{R}',\ \mathfrak{R}'',\ \ldots,\ \mathfrak{R}^{(\mu)}) = H^{\nu}(\mathfrak{g};\ \mathfrak{R}',\ \mathfrak{R}'',\ \ldots,\ \mathfrak{R}^{(\mu)}).$$

Il en résulte que l'ordre k de $\mathfrak{g}$ est égal à un diviseur de n; $n = k.\nu$.

Pour voir comment se groupent les fonctions algébriques $\mathfrak{G}$, si nous considérons les fonctions algébriques conjuguées $\mathfrak{g}_i$ comme connues, posons

$$\mathfrak{g}_{\lambda k+i} = \mathfrak{g}_i \qquad \begin{pmatrix} \lambda = 1, 2, \ldots, (\nu-1) \\ i = 1, 2, \ldots, k \end{pmatrix}$$

et désignons par $\Psi(\mathfrak{G}, \mathfrak{g}_i)$ le plus grand commun diviseur de $F(\mathfrak{G})$ et de $\varphi(\mathfrak{G}) - \mathfrak{g}_i$. Nous aurons alors

$$\Psi(\mathfrak{G}, \mathfrak{g}_i) = \prod_{\lambda=0}^{\nu-1} (\mathfrak{G} - \mathfrak{G}_{\lambda k+i}) \qquad (i = 1, 2, \ldots, k)$$

d'où

$$F(\mathfrak{G}) = \prod_{i=1}^{k} \Psi(\mathfrak{G}, \mathfrak{g}_i).$$

Ainsi la fonction $F(\mathfrak{G})$, irréductible dans le domaine naturel de rationalité, devient réductible si nous adjoignons à ce domaine les racines de l'équation $H(\mathfrak{g}; \mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)}) = 0$. Ses n facteurs linéaires se partagent en k groupes contenant chacun $\frac{n}{k}$ éléments. Afin de mettre en évidence cette dépendance de $\mathfrak{G}$ et de $\mathfrak{g}$, nous dirons que le genre $\mathfrak{g}$ est contenu dans le genre $\mathfrak{G}$, et que le genre $\mathfrak{G}$ contient le genre $\mathfrak{g}$. Lorsque deux genres se contiennent réciproquement, ils sont identiques. Ainsi toutes les fonctions du domaine $(\mathfrak{G}, \mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)})$ font ou bien partie du genre $\mathfrak{G}$, ou elles sont contenues dans ce genre. Les fonctions rationnelles de $\mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)}$, pouvant être considérées comme des fonctions algébriques d'ordre *un*, font elles-mêmes partie du domaine $(\mathfrak{G}, \mathfrak{R}', \ldots, \mathfrak{R}^{(\mu)})$ de sorte que le domaine naturel de rationalité $(\mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)})$ est contenu dans le domaine $(\mathfrak{G}; \mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)})$ qu'il a engendré par adjonction de la fonction algébrique $\mathfrak{G}$.

L'adjonction d'une racine d'une fonction entière égalée à zéro, à un domaine $(\mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)})$ ne donne naissance qu'à des genres dérivés du domaine considéré, même si les coefficients de la fonction entière font eux-mêmes partie d'un genre dérivé de ce domaine. En effet, dans un domaine déterminé, une fonction algébrique d'une fonction algébrique est une fonction algébrique; car, si $F(x; \mathfrak{R}', \ldots, \mathfrak{R}^{(\mu)}) = 0$ et $G(y; x, \mathfrak{R}', \ldots, \mathfrak{R}^{(\mu)}) = 0$ et que ξ_i $(i = 1, 2, \ldots)$ désignent les racines de $F = 0$, le produit $\prod_{(i)} G(y; \xi_i, \mathfrak{R}', \ldots, \mathfrak{R}^{(\mu)})$ étendu à toutes les racines ξ_i, est une fonction

symétrique de ces racines, et, par suite, une fonction entière de y, dont les coefficients sont fonctions rationnelles de $\mathfrak{R}'$, ..., $\mathfrak{R}^{(\mu)}$.

Ainsi en répétant plusieurs fois l'opération auxiliaire qui définit les nombres et les fonctions algébriques, nous n'obtenons rien de nouveau. L'idée de genre suffit pour nous rendre compte des domaines qui sont alors engendrés par le domaine naturel de rationalité. Suffit-elle également pour nous rendre compte de ce que devient ce domaine naturel de rationalité, si nous lui adjoignons un nombre quelconque de fonctions algébriques de ses éléments, ou est-il nécessaire d'introduire, dans nos recherches, une idée plus générale? C'est ce que nous allons étudier maintenant.

3. Soient $\rho^{(1)}$, $\rho^{(2)}$, ..., $\rho^{(\nu)}$, ν fonctions algébriques des variables indéterminées $\mathfrak{R}'$, $\mathfrak{R}''$, ..., $\mathfrak{R}^{(\mu)}$, définies par les relations,

$$f_1(\rho^{(1)}) = 0;\ f_2(\rho^{(2)}) = 0;\ \ldots,\ f_\nu(\rho^{(\nu)}) = 0;$$

et u_1, u_2, ..., u_ν, ν variables auxiliaires. Considérons le produit

$$\Pi(z - u_1\rho^{(1)} - u_2\rho^{(2)} - \ldots - u_\nu\rho^{(\nu)})$$

étendu à toutes les valeurs conjuguées de $\rho^{(1)}$, de $\rho^{(2)}$, ... et de $\rho^{(\nu)}$. Ce produit est une fonction symétrique des racines de chacune des équations $f_1(\rho^{(1)}) = 0$, $f_2(\rho^{(2)}) = 0$, ..., $f_\nu(\rho^{(\nu)}) = 0$; c'est donc une fonction de z dont les coefficients sont fonctions rationnelles des variables indéterminées $\mathfrak{R}'$, $\mathfrak{R}''$, ..., $\mathfrak{R}^{(\mu)}$, et fonctions entières des variables auxiliaires u_1, u_2, ..., u_ν. Soit $H(z;\ u_1,\ u_2,\ \ldots,\ u_\nu;\ \mathfrak{R}',\ \ldots,\ \mathfrak{R}^{(\mu)})$ un de ses facteurs irréductibles. Nous aurons évidemment

$$H(z;\ u_1,\ u_2,\ \ldots,\ u_\nu) = \prod_{(h)}(z - u_1\rho_h^{(1)} - u_2\rho_h^{(2)} - \ldots - u_\nu\rho_h^{(\nu)})$$

le produit n'étant étendu qu'à un certain nombre des valeurs conjuguées de $\rho^{(1)}$, de $\rho^{(2)}$, ... et de $\rho^{(\nu)}$. Mais alors, si v_1, v_2, ..., v_ν désignent ν nouvelles variables auxiliaires, nous avons

$$H(z;\ u_1 + v_1,\ u_2 + v_2,\ \ldots,\ u_\nu + v_\nu)$$

$$= \prod_{(h)}(z - u_1\rho_h^{(1)} - \ldots - u_\nu\rho_h^{(\nu)} - v_1\rho_h^{(1)} - \ldots - v_\nu\rho_h^{(\nu)})$$

et

$$H(z - v_1\rho_1^{(1)} - v_2\rho_1^{(2)} - \ldots - v_\nu\rho_1^{(\nu)};\ u_1,\ u_2,\ \ldots,\ u_\nu)$$

$$= \prod_{(h)} (z - u_1\rho_h^{(1)} - \ldots - u_\nu\rho_h^{(\nu)} - v_1\rho_1^{(1)} - \ldots - v_\nu\rho_1^{(\nu)}).$$

Ces deux fonctions ont un diviseur commun,

$$z - u_1\rho_1^{(1)} - u_2\rho_1^{(2)} - \ldots - u_\nu\rho_1^{(\nu)} - v_1\rho_1^{(1)} - v_2\rho_1^{(2)} - \ldots - v_\nu\rho_1^{(\nu)}.$$

En général ils n'en ont point d'autre; car de l'équation

$$z - u_1\rho_h^{(1)} - u_2\rho_h^{(2)} - \ldots - u_\nu\rho_h^{(\nu)} - v_1\rho_h^{(1)} - v_2\rho_h^{(2)} - \ldots - v_\nu\rho_h^{(\nu)}$$

$$= z - u_1\rho_k^{(1)} - u_2\rho_k^{(2)} - \ldots - u_\nu\rho_k^{(\nu)} - v_1\rho_1^{(1)} - v_2\rho_1^{(2)} - \ldots - v_\nu\rho_1^{(\nu)},$$

il résulterait

$$v_1\rho_h^{(1)} + v_2\rho_h^{(2)} + \ldots + v_\nu\rho_h^{(\nu)} = v_1\rho_1^{(1)} + v_2\rho_1^{(2)} + \ldots + v_\nu\rho_1^{(\nu)}$$

et, par suite, le discriminant de la fonction *irréductible,*

$$H(z;\ v_1,\ v_2,\ \ldots,\ v_\nu)$$

serait nul. Si donc nous donnons au système de variables $v_1, v_2, \ldots, v_\nu$, une valeur quelconque $a_1, a_2, \ldots, a_\nu$, différente de la variété $(\nu - 1)^{\text{ième}}$ qui seule peut annuler le discriminant de $H(z;\ v_1,\ v_2,\ \ldots,\ v_\nu)$, l'expression $z - u_1\rho_1^{(1)} - \ldots - u_\nu\rho_1^{(\nu)} - a_1\rho_1^{(1)} - \ldots - a_\nu\rho_1^{(\nu)}$ est le plus grand commun diviseur des deux fonctions $H(z;\ u_1 + a_1,\ \ldots,\ u_\nu + a_\nu)$ et $H(z - a_1\rho_1^{(1)} - \ldots - a_\nu\rho_1^{(\nu)};\ u_1,\ u_2,\ \ldots,\ u_\nu)$. Mais alors l'expression

$$u_1\rho_1^{(1)} + u_2\rho_1^{(2)} + \ldots + u_\nu\rho_1^{(\nu)} + a_1\rho_1^{(1)} + a_2\rho_1^{(2)} + \ldots + a_\nu\rho_1^{(\nu)}$$

est fonction rationnelle de $a_1\rho_1^{(1)} + a_2\rho_1^{(2)} + \ldots + a_\nu\rho_1^{(\nu)}$, $u_1, u_2, \ldots, u_\nu$ et, par suite, $u_1\rho_1^{(1)} + u_2\rho_1^{(2)} + \ldots + u_\nu\rho_1^{(\nu)}$ est fonction rationnelle de $a_1\rho_1^{(1)} + a_2\rho_1^{(2)} + \ldots + a_\nu\rho_1^{(\nu)}$, $u_1, u_2, \ldots, u_\nu$. Ce que nous venons de dire de la fonction algébrique ρ_1, a lieu de même pour chacune de ses conjuguées. Nous pouvons donc dire que

$$u_1\rho^{(1)} + u_2\rho^{(2)} + \ldots + u_\nu\rho^{(\nu)}$$

est fonction rationnelle de $a_1\rho^{(1)} + \ldots + a_\nu\rho^{(\nu)};\ u_1,\ u_2,\ \ldots,\ u_\nu$. En donnant à $u_1, u_2, \ldots, u_\nu$ des valeurs convenables, il en résulte que

chacune des fonctions $\rho^{(1)}, \rho^{(2)}, \ldots, \rho^{(\nu)}$ est fonction rationnelle de $a_1\rho^{(1)} + a_2\rho^{(2)} + \ldots + a_\nu\rho^{(\nu)}$. D'autre part, $a_1\rho^{(1)} + a_2\rho^{(2)} + \ldots + a_\nu\rho^{(\nu)}$ est manifestement fonction rationnelle de $\rho^{(1)}, \rho^{(2)}, \ldots, \rho^{(\nu)}$. Le genre $(\rho^{(1)}, \rho^{(2)}, \ldots, \rho^{(\nu)}; \mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)})$ est, par suite, identique au genre $(a_1\rho^{(1)} + a_2\rho^{(2)} + \ldots + a_\nu\rho^{(\nu)}; \mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)})$.

La question posée est ainsi résolue; l'adjonction d'un nombre quelconque de fonctions algébriques aux indéterminées et aux entiers qui composent le domaine naturel de rationalité, est identique à celle d'une seule fonction algébrique à ce même domaine. C'est pourquoi nous nommons un domaine de la forme

$$(\mathfrak{G}, \mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)})$$

domaine général de rationalité.

Le domaine général de rationalité embrasse le domaine naturel correspondant. Dorénavant lorsque nous parlerons d'un domaine de rationalité, nous entendrons par là, indistinctement un domaine général ou naturel de rationalité; ainsi dans le domaine $(\mathfrak{G}; \mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)})$ il ne sera pas indispensable que $\mathfrak{G}$ figure vraiment. Lorsqu'il sera nécessaire de distinguer entre les deux cas, nous ajouterons l'adjectif naturel ou engendré suivant que $\mathfrak{G}$ ne figure pas, ou figure, dans le domaine

$$(\mathfrak{G}; \mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)}).$$

4. On pourrait enfin supposer que les variables-indéterminées soient liées, non par les relations particulières

$$f_k(\rho^{(k)}; \mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)}) = 0 \qquad (k = 1, 2, \ldots, \nu)$$

qui définissent ν fonctions algébriques $\rho^{(1)}, \rho^{(2)}, \ldots, \rho^{(\nu)}$, mais par un nombre quelconque d'équations algébriques entre les variables indéterminées $\rho^{(1)}, \rho^{(2)}, \ldots, \rho^{(\nu)}, \mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)}$, c'est à dire entre un nombre quelconque de variables-indéterminées.

Je démontrerai plus tard que le domaine ainsi formé ne donne, lui aussi, naissance à rien de nouveau. C'est dans la démonstration de ce théorème que consiste précisément le problème général de l'élimination, dans le cas particulier où le domaine de rationalité est égal à l'unité. Les premières recherches sur la divisibilité nous amènent ainsi à étudier

le problème général de l'élimination. Il suffit, pour le moment, d'avoir réduit l'adjonction d'un nombre quelconque de fonctions algébriques à l'adjonction d'une seule fonction algébrique, et d'avoir ainsi introduit l'idée de domaine général de rationalité dans nos recherches d'Algèbre.

§ 4.

Réductibilité des fonctions entières dans un domaine général de rationalité.

1. L'idée d'irréductibilité est relative. Elle dépend du domaine de rationalité que nous fixons au début de nos recherches. Il est donc naturel de nous demander si nous pouvons l'étendre à un domaine *général* de rationalité.

Rien n'est moins évident. Car la méthode que nous avons suivie pour reconnaître si, dans un domaine naturel de rationalité, une fonction entière a des facteurs ou non, n'est plus applicable.

A la vérité, nous pourrions donner une définition logique de l'irréductibilité. Mais il nous faut une définition algébrique comme nous l'avons fait remarquer dans le premier chapitre.

Nous devons donc, tout d'abord, donner une nouvelle méthode qui permette, à l'aide d'un nombre fini d'opérations, de *reconnaître* si une fonction entière de plusieurs variables, dont les coefficients font partie d'un domaine général de rationalité $(\rho; \mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)})$, peut, ou non, être mise sous la forme d'un produit de fonctions entières de ces variables, dont les coefficients fassent, eux aussi, partie du domaine $(\rho; \mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)})$, et qui, dans le premier cas, donne le moyen de trouver ces facteurs.

Ordonnons par rapport à l'une des variables, z. Si le coefficient A de la plus haute puissance de z est différent de l'unité, nous décomposerons la fonction considérée en deux facteurs dont l'un est A et l'autre une fonction de z dont les coefficients font partie du domaine $(\rho; \mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)})$, le coefficient de la plus haute puissance étant égal à l'unité. Deux cas peuvent alors se présenter. Ou bien A contient au moins une nouvelle variable indépendante z', et alors nous pouvons, en ordonnant A par

rapport à z', répéter sur A, qui contient une variable de moins, les mêmes raisonnements que sur toute la fonction considérée. Ou bien A ne contient que ρ et les variables-indéterminées et alors il ne serait d'aucune utilité de décomposer A. Nous pouvons donc supposer, sans restriction aucune, que le coefficient de la plus haute puissance de z est égal à l'unité.

Attachons-nous d'abord, pour plus de clarté, au cas où il n'y a qu'une seule variable z. Il est toujours permis de supposer que la fonction donnée $F(z)$ ne contienne pas de facteurs multiples; car, si elle en contenait nous considérerions non pas cette fonction, mais la suivante,

$$\frac{F(z)}{\mathrm{Dv}[F(z),\ F'(z)]}$$

en convenant, une fois pour toutes, de représenter par $\mathrm{Dv}[\varphi(x),\ \psi(x)]$ le plus grand commun diviseur des deux fonctions $\varphi(x)$ et $\psi(x)$. Nous savons toujours, par un nombre fini d'opérations rationnelles, former cette fonction qui ne contient que les facteurs simples de $F(z)$ et qui les contient tous.

Remarquons ensuite que dans un certain nombre de recherches les coefficients de la fonction entière donnée font simplement partie d'un domaine naturel de rationalité $(\mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)})$ et que c'est cependant le domaine général $(\rho; \mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)})$ que l'on considère comme connu. Nous avons alors à faire une recherche analogue à la précédente. Les deux cas ont ceci de commun que dans tous deux nous cherchons à savoir si la fonction donnée contient ou non un facteur dans un domaine déterminé $(\rho; \mathfrak{R}', \ldots, \mathfrak{R}^{(\mu)})$. Pour n'avoir pas à distinguer entre eux, nous considérerons, non pas la fonction $F(z; \rho, \mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)})$ où ρ pourrait ne figurer qu'en apparence dans les coefficients des différentes puissances de z, mais la fonction

$$F(z + u\rho; \rho, \mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)})$$

où u désigne une indéterminée. Nous sommes alors certain que ρ figure dans les coefficients des différentes puissances de la variable z; quant à l'indéterminée u nous savons que son adjonction ne peut en rien changer la réductibilité d'une fonction quelconque; d'autre part, si nous donnons une méthode pour trouver les facteurs contenus dans la fonction $F(z + u\rho; \rho, \mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)})$, considérée comme fonction de $(z + u\rho)$,

il est bien évident que, u étant une indéterminée, nous aurons, en même temps, les facteurs cherchés, contenus en $F(z;\ \rho,\ \mathfrak{R}',\ \mathfrak{R}'',\ \ldots,\ \mathfrak{R}^{(\mu)})$.

2. Ceci posé, soient $\rho_1,\ \rho_2,\ \ldots,\ \rho_\lambda$, les λ racines de l'équation $f(\rho) = 0$, qui définit ρ. Formons le produit

$$\prod_{k=1}^{\lambda} F(z + u\rho_k;\ \rho_k,\ \mathfrak{R}',\ \mathfrak{R}'',\ \ldots,\ \mathfrak{R}^{(\mu)});$$

cette expression est symétrique dans les racines de $f(\rho) = 0$; c'est donc une fonction entière de z, dont les coefficients font partie du domaine $(\mathfrak{R}',\ \mathfrak{R}'',\ \ldots,\ \mathfrak{R}^{(\mu)})$. Nous savons trouver les facteurs irréductibles d'une fonction entière, dans un domaine naturel de rationalité; nous pouvons donc écrire, en sous-entendant les variables-indéterminées $\mathfrak{R}',\ \mathfrak{R}'',\ \ldots,\ \mathfrak{R}^{(\mu)}$,

$$\prod_{k=1}^{\lambda} F(z + u\rho_k;\ \rho_k) = V_1^{\mu_1}(z)V_2^{\mu_2}(z)\ \ldots\ V_n^{\mu_n}(z)$$

où $V_h(z)$, $(h = 1,\ 2,\ \ldots,\ n)$ désigne une fonction entière de z, irréductible dans le domaine $(\mathfrak{R}',\ \mathfrak{R}'',\ \ldots,\ \mathfrak{R}^{(\mu)})$, et contient en outre l'indéterminée u. Les μ_h sont des nombres entiers. Pour nous rendre compte de la grandeur de ces entiers, prenons, dans l'égalité précédente, la dérivée, par rapport à z, des termes de droite et de gauche.

Nous obtenons, à droite,

$$V_1^{\mu_1-1}(z)V_2^{\mu_2-1}(z)\ \ldots\ V_n^{\mu_n-1}(z)\sum_{i=1}^{n}[\mu_i V_1(z)V_2(z)\ \ldots\ V_{i-1}(z)V_{i+1}(z)\ \ldots\ V_n(z)].$$

Si donc l'un seulement des entiers μ, était plus grand que l'unité, la dérivée du terme de droite et, par suite, celle du terme de gauche, c'est à dire celle du produit considéré, aurait un facteur commun avec ce produit lui-même. Cette dérivée étant égale à

$$\sum_{k=1}^{\lambda}\left(\frac{F'(z + u\rho_k;\ \rho_k)}{F(z + u\rho_k;\ \rho_k)}\cdot\prod_{h=1}^{\lambda} F(z + u\rho_h;\ \rho_h)\right)$$

il faudrait donc que l'un des facteurs du produit, $F(z + u\rho_1;\ \rho_1)$ par exemple, et

$$F'(z + u\rho_1;\ \rho_1)F(z + u\rho_2;\ \rho_2)F(z + u\rho_3;\ \rho_3)\ \ldots\ F(z + u\rho_\lambda;\ \rho_\lambda)$$

eussent un facteur commun; comme nous avons eu soin de débarasser, tout d'abord, la fonction $F(z)$ de ses facteurs multiples, il faudrait donc aussi que $F(z + u\rho_1; \rho_1)$ et $F(z + u\rho_k; \rho_k)$, par exemple, pour $k > 1$, et, par suite, en posant $z + u\rho_1 = y$, que $F(y; \rho_1)$ et $F[y + u(\rho_k - \rho_1); \rho_k]$ eussent un facteur commun.

En développant la dernière fonction suivant les puissances de u, on a

$$F[y + u(\rho_k - \rho_1); \rho_k] = F(y; \rho_k) + u(\rho_k - \rho_1)F'(y; \rho_k) + \ldots + u^n(\rho_k - \rho_1)^n.$$

Mais u est une indéterminée; il faudrait donc que $F(y; \rho_1)$ et $(\rho_k - \rho_1)^n$ qui est indépendant de y, eussent un diviseur commun, contrairement à l'hypothèse $A = 1$.

Nous avons ainsi montré qu'aucun des entiers μ n'est plus grand que *un*, et nous pouvons maintenant écrire,

$$\prod_{k=1}^{\lambda} F(z + u\rho_k; \rho_k) = V_1(z)V_2(z) \ldots V_n(z).$$

La fonction entière de z, $F(z + u\rho_1, \rho_1)$ a d'ailleurs, manifestement, un diviseur commun avec l'une des fonctions $V_h(z)$, avec $V_1(z)$, par exemple. Si nous désignons par $\theta_1(z; \rho_1)$ le plus grand commun diviseur de ces deux fonctions, déterminé de manière que le coefficient de la plus haute puissance de z soit égal à l'unité, et par $\varphi(z; \rho_1)$, $\psi(z; \rho_1)$, $\Phi(z; \rho_1)$, $\Psi(z; \rho_1)$, des fonctions entières de z, nous pouvons donc écrire

$$V_1(z) = \varphi(z; \rho_1)\theta_1(z; \rho_1)$$

$$F(z + u\rho_1; \rho_1) = \psi(z; \rho_1)\theta_1(z; \rho_1)$$

$$\theta_1(z; \rho_1) = \Phi(z; \rho_1)V_1(z) + \Psi(z; \rho_1)F(z + u\rho_1; \rho_1)$$

ou, plus simplement, d'après la convention faite au début de ce paragraphe

$$\theta_1(z; \rho_1) = \mathrm{Dv}[V_1(z); F'(z + u\rho_1; \rho_1)].$$

Mais toute fonction rationnelle de ρ qui s'annule pour une racine ρ_1 de l'équation irréductible $f(\rho; \mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)}) = 0$ s'annule également, d'après un théorème bien connu, pour toutes les racines ρ_k de cette

équation. Les trois égalités précédentes subsistent donc si nous changeons ρ_1 en ρ_k, et nous avons

$$\theta_1(z;\ \rho_k) = \mathrm{Dv}[V_1(z);\ F(z + u\rho_k;\ \rho_k)]. \qquad (k=1, 2, \ldots, \lambda)$$

Deux quelconques des fonctions $\theta_1(z;\ \rho_h)$ et $\theta_1(z;\ \rho_k)$ sont d'ailleurs premières entre elles; car elles sont respectivement contenues dans les deux fonctions $F(z + u\rho_h;\ \rho_h)$ et $F(z + u\rho_k;\ \rho_k)$ que nous savons être sans diviseur commun. Si donc nous considérons le produit

$$\prod_{k=1}^{\lambda} \theta_1(z;\ \rho_k)$$

qui est une fonction entière de z, dont les coefficients font partie du domaine naturel de rationalité $(\Re', \Re'', \ldots, \Re^{(\mu)})$, nous voyons que ce produit est un facteur de la fonction entière $V_1(z)$ dont les coefficients font partie du même domaine, et nous avons

$$V_1(z) \equiv 0 \ [\mathrm{mod} \prod_{k=1}^{\lambda} \theta_1(z;\ \rho_k)].$$

D'autre part, de l'égalité

$$\theta_1(z;\ \rho_k) = \Phi(z;\ \rho_k) V_1(z) + \Psi(z;\ \rho_k) F(z + u\rho_k;\ \rho_k)$$

qui a lieu pour $k = 1, 2, \ldots, \lambda$, nous déduisons la congruence

$$\prod_{k=1}^{\lambda} \theta_1(z;\ \rho_k) \equiv \prod_{k=1}^{\lambda} \Psi(z;\ \rho_k) \prod_{k=1}^{\lambda} F(z + u\rho_k;\ \rho_k) \ [\mathrm{mod}\, V_1(z)]$$

et comme $\prod_{k=1}^{\lambda} F(z + u\rho_k;\ \rho_k)$ est égal au produit $\prod_{h=1}^{n} V_h(z)$, nous avons aussi

$$\prod_{k=1}^{\lambda} \theta_1(z;\ \rho_k) \equiv 0 \ [\mathrm{mod}\, V_1(z)].$$

Des deux congruences démontrées résulte l'égalité

$$V_1(z) = \prod_{k=1}^{\lambda} \theta_1(z;\ \rho_k).$$

Nous avons donc décomposé la fonction $V_1(z)$, irréductible dans le domaine naturel de rationalité $(\Re', \Re'', \ldots, \Re^{(\mu)})$, en λ facteurs, en adjoignant à ce domaine une fonction algébrique ρ, d'ordre λ, et ses conjuguées.

Si

$$\theta_h(z;\ \rho_i) = \mathrm{Dv}[V_h(z);\ F(z + u\rho_i;\ \rho_i)]$$

nous obtenons, de même, l'égalité

$$V_h(z) = \prod_{k=1}^{\lambda} \theta_h(z;\ \rho_k).$$

Comme ceci a lieu pour $h = 1, 2, \ldots, n$, nous avons aussi

$$\prod_{k=1}^{\lambda} F(z + u\rho_k;\ \rho_k) = \prod_{h=1}^{n} V_h(z) = \prod_{k=1}^{\lambda}\prod_{h=1}^{n} \theta_h(z;\ \rho_k).$$

Considérons maintenant le produit

$$\prod_{h=1}^{n} \theta_h(z;\ \rho_k).$$

Comme

$$\theta_h(z;\ \rho_k) = \Phi_h(z;\ \rho_k)V_h(z) + \Psi_h(z;\ \rho_k)F(z + u\rho_k;\ \rho_k)$$

et que

$$\prod_{h=1}^{n} V_h(z) = \prod_{k=1}^{\lambda} F(z + u\rho_k;\ \rho_k)$$

il est évident que nous avons la congruence

$$\prod_{h=1}^{n} \theta_h(z;\ \rho_k) \equiv 0 \ [\mathrm{mod}\ F(z + u\rho_k;\ \rho_k)].$$

Ecrivons

$$\prod_{h=1}^{n} \theta_h(z;\ \rho_k) = Q(z;\ \rho_k)F(z + u\rho_k;\ \rho_k);$$

il en résulte immédiatement,

$$\prod_{k=1}^{\lambda}\prod_{h=1}^{n} \theta_h(z;\ \rho_k) = \prod_{k=1}^{\lambda} Q(z;\ \rho_k)\prod_{k=1}^{\lambda} F(z + u\rho_k;\ \rho_k)$$

d'où, à cause de l'égalité que nous venons de démontrer,

$$\prod_{k=1}^{\lambda} Q(z;\ \rho_k) = 1.$$

Chacune des fonctions entières de z, $Q(z;\ \rho_k)$, est donc indépendante de z et comme le coefficient de la plus haute puissance de z est égal à l'unité dans toutes les fonctions considérées, et, par suite, aussi dans $Q(z;\ \rho_k)$, nous pouvons écrire :

$$Q(z;\ \rho_k) = 1. \qquad (k=1, 2, \ldots, \lambda)$$

Ainsi

$$\prod_{h=1}^{n} \theta_h(z;\ \rho_k) = F(z + u\rho_k;\ \rho_k).$$

Chacune des fonctions θ_h contient l'indéterminée u. D'après le théorème fondamental sur la réductibilité des fonctions de plusieurs variables dans un domaine naturel de rationalité, nous savons que θ_h est fonction entière de cette indéterminée u, puisque $F(z + u\rho_k;\ \rho_k)$ est elle-même fonction entière de u. En développant les deux termes de l'égalité précédente, suivant les puissances de u, nous obtenons donc, enfin, une décomposition de la fonction $F(z;\ \rho_k)$ dans le domaine général de rationalité $(\rho_k;\ \mathfrak{R}',\ \mathfrak{R}'',\ \ldots,\ \mathfrak{R}^{(\mu)})$.

Nous avons ainsi un premier exemple de l'emploi des indéterminées en Algèbre. Si l'on se proposait simplement d'assurer la présence de ρ_k dans les coefficients de $F(z;\ \rho_k)$ on pourrait aussi poser $z = x + a\rho_k$ et donner à a une valeur quelconque différente de celles qui annulent le résultant de $F(x + a\rho_h;\ \rho_h)$ et de $F(x + a\rho_k;\ \rho_k)$, pris par rapport à x. En effet, nous ne nous sommes servis de l'indétermination de u que pour montrer que $F(z + u\rho_h;\ \rho_h)$ et $F(z + u\rho_k;\ \rho_k)$ ne pouvaient avoir de diviseurs communs par rapport à z. Et, d'autre part, nous avons démontré que la condition nécessaire et suffisante pour que deux fonctions qui, en général, sont sans diviseur commun, aient un diviseur commun pour des valeurs particulières données à leurs coefficients, est que le résultant de ces deux fonctions s'annule pour les valeurs particulières considérées.

Nous obtiendrions ainsi

$$F(x + a\rho_k;\ \rho_k) = \prod_{h=1}^{n} \theta_h(x;\ \rho_k)$$

donc aussi

$$F(z;\ \rho_k) = \prod_{h=1}^{n} \theta_h(z - a\rho_k;\ \rho_k)$$

et, par suite, la décomposition cherchée.

Cette décomposition ne peut d'ailleurs être poussée plus loin. Car si $\theta_1(z;\ \rho_k)$, par exemple, contenait une fonction $\eta_1(z;\ \rho_k)$ et si nous avions

$$\theta_1(z;\ \rho_k) = \eta_1(z;\ \rho_k)\zeta_1(z;\ \rho_k)$$

nous aurions la même égalité pour $k = 1, 2, \ldots, \lambda$, puisque $\rho_1, \rho_2, \ldots, \rho_\lambda$ sont les λ racines d'une équation irréductible dans un domaine naturel de rationalité. Nous aurions donc aussi

$$V_1(z) = \prod_{k=1}^{\lambda} \eta_1(z;\ \rho_k) \cdot \prod_{k=1}^{\lambda} \zeta_1(z;\ \rho_k)$$

et comme chacun de ces produits est une fonction entière de z dont les coefficients font partie du domaine naturel $(\mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)})$, la fonction $V_1(z)$ ne serait pas irréductible dans ce domaine contrairement à la définition de cette fonction.

Enfin la décomposition précédente est univoque. Il est facile de s'en assurer à l'aide de l'algorithme d'Euclide, par un raisonnement tout à fait identique à celui du paragraphe 1 de ce chapitre.

3. La décomposition d'une fonction de plusieurs variables en ses facteurs irréductibles, dans un domaine général de rationalité, ne présente plus maintenant aucune espèce de difficultés. En effet, rien n'est changé, dans ce qui précède, si nous considérons plusieurs des variables-indéterminées $\mathfrak{R}$ dont ρ ne dépend pas, comme si elles étaient des variables quelconques, à condition toutefois que F en soit fonction *entière*. Le produit

$$\prod_{k=1}^{\lambda} F(z + u\rho_k;\ z_1, z_2, \ldots, z_\nu;\ \rho_k;\ \mathfrak{R}', \mathfrak{R}'', \ldots)$$

où F est une fonction *entière* des variables $z, z_1, z_2, \ldots, z_\nu$, dont les coefficients sont fonctions rationnelles des variables-indéterminées $\mathfrak{R}', \mathfrak{R}'', \ldots$ et de la fonction algébrique ρ de ces variables-indéterminées, est également une fonction entière de $z, z_1, \ldots, z_\nu$ dont les coefficients font partie d'un domaine naturel de rationalité. Mais nous avons démontré que, dans un tel domaine, la décomposition d'une fonction entière de plusieurs variables indépendantes est identique à celle de la même fonction, par rapport à l'une des variables seulement. Dans le cas que nous

considérons, les fonctions θ_h sont donc entières, non seulement en z, mais aussi en $z_1, z_2, \ldots, z_\nu$.

Le problème que nous nous étions proposé est ainsi résolu. L'adjonction d'une fonction algébrique ρ à un domaine naturel de rationalité rend parfois réductible une fonction entière de z, irréductible dans le domaine naturel considéré.

Désignons par ζ les racines de cette fonction égalée à zéro. Il est intéressant de remarquer qu'il existe entre ρ et ζ une complète réciprocité. Soient, en effet, $F(z)$ une fonction entière de degré n et $G(r)$ une fonction entière de degré k, toutes deux irréductibles dans le domaine considéré. Supposons que par adjonction d'une racine ρ de l'équation $G(r) = 0$, la fonction $F(z)$ devienne réductible et qu'un de ses facteurs soit $f(z; \rho)$. Nous pouvons réduire à $(k - 1)$ le degré de cette fonction par rapport à ρ, à l'aide de l'équation $G(r) = 0$ qui est vérifiée pour $r = \rho$. L'égalité $f(\zeta, \rho) = 0$ nous montre alors que la fonction $f(\zeta, r)$ dont le degré, par rapport à r, est plus petit que k, est égale à zéro pour l'une au moins des racines de l'équation irréductible $G(r) = 0$. L'adjonction de ζ au domaine de rationalité rend donc réductible la fonction irréductible $G(r)$. La réciprocité de ζ et de ρ est ainsi démontrée.

Voici donc l'idée d'irréductibilité étendue aux fonctions entières dont les coefficients font partie d'un domaine général de rationalité. L'étude des fonctions entières quelconques est ramenée à celle des fonctions entières irréductibles quelles que soient les fonctions algébriques des variables indéterminées que nous supposions connues.

Un premier pas est ainsi fait dans la voie de la décomposition des fonctions entières. Il peut être continué dans deux directions différentes. Ou bien l'on peut se proposer d'élargir encore le domaine général de rationalité, comme nous l'avons indiqué à la fin du paragraphe précédent, et si l'on y parvient d'étendre, si possible, au domaine obtenu l'idée d'irréductibilité. Ou bien l'on peut rechercher si plusieurs fonctions que nous embrassons en un système après les avoir débarassées de leurs facteurs communs dans un domaine général de rationalité, ne peuvent avoir encore un élément arithmétique commun, et si l'on ne peut ainsi étendre l'idée même de décomposition en facteurs. Cette double recherche sera l'objet des chapitres suivants.

Chapitre III.

Introduction des systèmes de diviseurs en Algèbre.

§ 1.

Définitions.

1. Un système de fonctions d'une, de deux ou de trois variables, égalées à zéro, est susceptible d'une interprétation géométrique.

Une fonction entière d'une variable, $\Phi(x)$ égalée à zéro et interprétée sur une droite y définit un nombre fini de points; si la fonction entière $\Phi(x)$ est débarassée de ses facteurs doubles, ces points seront distincts. Nous savons alors que toute fonction $F(x)$ qui, égalée à zéro, définit, entre autres points, ces points distincts, *contient* la fonction $\Phi(x)$, et nous observons ainsi une correspondance directe entre l'idée de *contenir,* se rapportant aux fonctions entières d'une variable et celle de système de points, sur une droite, faisant partie d'un autre système de points sur la même droite, se rapportant à ces mêmes fonctions entières d'une variable, égalées à zéro.

Une fonction de deux variables égalée à zéro et interprétée dans un plan y définit une courbe. Considérons deux courbes planes $\Phi(x, y) = 0$ et $\Psi(x, y) = 0$. Deux cas peuvent se présenter suivant que ces deux courbes ont des courbes communes ou n'en ont pas. Si elles ont des courbes communes C, ces courbes seront représentées par le plus grand commun diviseur $\theta(x, y)$ de $\Phi(x, y)$ et de $\Psi(x, y)$, égalé à zéro, et lorsque les courbes C font partie des courbes définies par une fonction entière $F(x, y)$ égalée à zéro, nous savons que $F(x, y)$ *contient* le plus grand commun diviseur $\theta(x, y)$. Ainsi, ici encore, nous observons une correspondance directe entre l'idée de *contenir* se rapportant aux fonctions entières de deux variables, à leur plus grand commun diviseur, et celle de système de courbes, dans un plan, faisant partie d'un autre système de courbes situées dans le même plan, se rapportant à ces mêmes fonc-

tions entières de deux variables, égalées à zéro. Si elles n'ont pas de courbes communes C, elles peuvent cependant avoir un nombre fini de points communs P. Si ces points sont distincts, on démontre que toute fonction entière de x et de y, $f(x, y)$, qui s'annule pour tous ces points P, est fonction linéaire et homogène de $\Phi(x, y)$ et $\Psi(x, y)$, à coefficients fonctions entières de x et de y. Quoique nous ne donnions la démonstration de ce théorème que dans le chapitre suivant, nous pouvons cependant le supposer connu, dès à présent, parce qu'il s'agit ici simplement de légitimer l'introduction des systèmes de diviseurs en Algèbre, et non pas de démontrer quoi que ce soit. Ce théorème nous montre une correspondance directe entre être fonction homogène et linéaire de deux fonctions entières $\Phi(x, y)$, $\Psi(x, y)$ sans diviseurs communs, et celle de représenter un système de courbes et de points dont font partie les points communs aux deux courbes $\Phi(x, y) = 0$ et $\Psi(x, y) = 0$. C'est pourquoi nous dirons, par analogie avec le cas précédent, que la fonction entière $f(x, y)$ *contient le système* des deux fonctions $\Phi(x, y)$, $\Psi(x, y)$, que *ce système est contenu* dans $f(x, y)$, ou encore est un *système de diviseurs* de $f(x, y)$.

Il en est de même pour les fonctions entières de trois variables; dans l'étude des formes géométriques définies par ces fonctions égalées à zéro, il faut distinguer deux cas. Ou bien les formes communes à trois fonctions de trois variables égalées à zéro sont des surfaces et alors ces surfaces sont représentées par le plus grand commun diviseur des trois fonctions considérées, égalé à zéro; toute fonction qui *contient* ce plus grand commun diviseur, représente, si nous l'égalons à zéro, entre autres, ces surfaces; nous avons donc, de nouveau, dans ce cas, la même correspondance que pour les fonctions d'une et de deux variables. Ou bien, les formes communes aux trois fonctions considérées égalées à zéro, sont des courbes et des points et alors toute fonction qui, égalée à zéro, représente entre autres ces courbes et ces points est fonction homogène et linéaire des trois fonctions considérées. Nous dirons, de nouveau par analogie, qu'elle *contient le système des trois fonctions considérées.* Mais tandis que pour les fonctions de deux variables, aux courbes communes correspondaient les diviseurs, et, aux points isolés communs, les systèmes de diviseurs des fonctions considérées, ainsi à chaque élément géométrique, courbe et point, une idée analytique différente, les points et les courbes sont encore confondues pour les fonctions de trois variables. Pour distinguer

les deux cas qui peuvent se présenter, celui où des fonctions de trois variables, sans diviseur commun, égalées à zéro définissent des courbes et des points, et celui où elles ne definissent que des points, nous dirons, dans le premier cas, que le système de diviseurs est de *rang deux,* et, dans le second cas, qu'il est de *rang trois.* Le rang d'un système ne dépend donc en rien du nombre d'éléments de ce système. Un diviseur de *rang un* d'un système de fonctions entières, est un diviseur de ces fonctions, dans le sens habituel du mot.

Nous pouvons ainsi continuer, et considérer des fonctions d'un nombre quelconque n de variables. Nous dirons alors qu'une fonction entière *contient* un système de fonctions entières lorsqu'elle est exprimable par une fonction linéaire et homogène de ces fonctions entières dont les coefficients soient également fonctions entières des n variables considérées. Comme dans le cas de trois variables, nous distinguerons entre des systèmes de rang un, deux, trois, et ainsi de suite jusqu'à n suivant que les formes géométriques représentées par les fonctions données, égalées à zéro, sont de variété $(n-1)^{\text{ième}}$, $(n-2)^{\text{ième}}$, $(n-3)^{\text{ième}}$, et ainsi de suite jusqu'à zéro; dans ce dernier cas elles représentent des points isolés situés dans la variété $n^{\text{ième}}$ donnée. Nous dirons souvent système de diviseurs au lieu de système de fonctions à cause de l'analogie qu'offre un système de fonctions contenu dans une fonction entière avec un facteur, *un diviseur* de cette fonction entière.

2. La définition que nous venons de donner est indépendante de toute interprétation géométrique, sauf toutefois l'idée de *rang* que nous ne pourrons préciser d'une manière arithmétique que dans la théorie générale de l'élimination. Ce qui précède avait simplement pour but de nous faire voir comment on pouvait être amené à donner précisément cette définition de *contenant* et de *contenu* de préférence à toute autre.

Cependant cette définition n'est pas encore complète. Nous n'avons parlé que de variables comme éléments des fonctions entières considérées et, en effet, la géométrie ne peut pas nous donner autre chose. D'après les principes développés dans le chapitre premier de ce Mémoire, il nous reste à tenir compte des *nombres entiers.* C'est pourquoi, étendant encore les définitions précédentes et les faisant concorder avec les recherches arithmétiques que nous avons en vue, nous dirons enfin:

1° *Un système de fonctions ou système de diviseurs est l'ensemble d'un*

certain nombre de fonctions faisant partie d'un domaine d'intégrité que nous fixons à l'avance. Chacune de ces fonctions est un élément du système.

2° *Une fonction faisant partie d'un domaine d'intégrité donné contient un système de diviseurs lorsqu'elle peut être représentée par une fonction homogène et linéaire des éléments du système dont les coefficients fassent également partie du domaine d'intégrité considéré.*

Ainsi dire que, dans le domaine d'intégrité $[\mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(n)}]$, la fonction F contient le système $(f_1, f_2, \ldots, f_k)$, c'est dire que l'on peut mettre F sous la forme

$$F = \varphi_1 f_1 + \varphi_2 f_2 + \ldots + \varphi_k f_k$$

$\varphi_1, \varphi_2, \ldots, \varphi_k$ désignant comme $F, f_1, f_2, \ldots, f_k$, des fonctions faisant partie du domaine d'intégrité considéré et n'étant pas toutes nulles. Dans cette dernière égalité, ce qui importe, ce sont manifestement les fonctions $f_1, f_2, \ldots, f_k$, les éléments du système, et non pas les multiplicateurs $\varphi_1, \varphi_2, \ldots, \varphi_k$. Pour bien mettre ce fait en évidence, M. KRONECKER se sert d'une notation analogue à celle dont GAUSS a fait usage dans les *Disquisitiones arithmeticæ* et il écrit au lieu de l'égalité précédente, simplement

$$F \equiv 0 \ (\mathrm{modd}\, f_1, f_2, \ldots, f_k)$$

ce que nous énoncerons en disant que F est congru à zéro, suivant le système de fonctions, ou le système de diviseurs, $(f_1, f_2, \ldots, f_k)$; ou encore, pour ne pas nous répéter trop souvent et conserver l'analogie avec le cas particulier où l'on considère la congruence $F \equiv 0 \pmod f$, que F est congru à zéro suivant le *système de modules* $(f_1, f_2, \ldots, f_k)$. Ainsi lorsqu'une fonction faisant partie d'un domaine d'intégrité contient un système de modules faisant partie du même domaine, elle est congrue à zéro suivant ce système de modules et réciproquement.

Enfin, rien ne nous empêche d'étendre encore l'idée de *contenir* à un système de fonctions faisant partie d'un domaine d'intégrité donné. Nous dirons que

3° *Un système de diviseurs contient un autre système de diviseurs lorsque chaque fonction du premier système contient le second système;*

4° *Lorsque deux systèmes se contiennent réciproquement ils sont équivalents,*

et nous écrirons, lorsqu'un système $(F_1, F_2, \ldots, F_h)$ en contient un autre $(f_1, f_2, \ldots, f_k)$,

$$(F_1, F_2, \ldots, F_h) \equiv 0 \pmod{f_1, f_2, \ldots, f_k}$$

et lorsque les deux systèmes $(F_1, F_2, \ldots, F_h)$ et $(f_1, f_2, \ldots, f_k)$ sont équivalents,

$$(F_1, F_2, \ldots, F_h) \sim (f_1, f_2, \ldots, f_k).$$

Cette équivalence représente donc l'ensemble des deux congruences

$$(F_1, F_2, \ldots, F_h) \equiv 0 \pmod{f_1, f_2, \ldots, f_k}$$
$$(f_1, f_2, \ldots, f_k) \equiv 0 \pmod{F_1, F_2, \ldots, F_h}$$

ou encore des $(h + k)$ congruences,

$$F_m \equiv 0 \pmod{f_1, f_2, \ldots, f_k} \qquad (m = 1, 2, \ldots, h)$$
$$f_n \equiv 0 \pmod{F_1, F_2, \ldots, F_h}. \qquad (n = 1, 2, \ldots, k)$$

Nous pouvons nous servir du symbole de l'équivalence comme de celui de l'égalité; car il est manifeste que si $a \sim b$ on a aussi $b \sim a$ et que si $a \sim b$ et $b \sim c$ on a aussi $a \sim c$.

Tout ce que nous venons de dire a lieu quel que soit le domaine d'intégrité donné. Rien ne nous empêche, par exemple, de faire déjà les mêmes raisonnements sur le domaine [1], c'est à dire sur les nombres entiers. Cependant, pour l'objet que nous avons en vue, ils ne deviennent indispensables que lorsque nous considérons un domaine d'intégrité contenant au moins une variable $\mathfrak{R}$. Cela tient à ce que dans le cas où un système est composé de nombres entiérs seulement, tout nombre qui peut être mis sous la forme d'une fonction homogène et linéaire des éléments du système est manifestement un multiple de leur plus grand commun diviseur et que, par suite, tout le système est ainsi entièrement remplacé par ce plus grand commun diviseur. Remarquons en passant que cette réduction à la divisibilité telle qu'elle est conçue généralement, que nous obtenons ainsi dans un cas particulier, légitime aussi l'introduction des systèmes de diviseurs en Algèbre.

3. La même réduction aurait lieu si nous considérions exclusivement les fonctions d'une variable. Mais ce ne serait point dans la nature des choses. Dans l'arithmétique plus générale que nous obtenons en considérant, dès le début, les fonctions entières à coefficients entiers d'une et de plusieurs variables indépendantes il est indispensable de ne pas laisser de côté les nombres entiers eux-mêmes. Aussi le domaine d'intégrité $[\mathfrak{R}]$ contient-il non seulement les fonctions entières à coefficients entiers de la variable $\mathfrak{R}$, mais encore tous les nombres entiers; on peut considérer ces derniers comme fonctions entières à coefficients entiers de $\mathfrak{R}$, ne contenant que la puissance zéro de cette variable. Et alors il est bien évident que tous les entiers qui peuvent être exprimés en fonction linéaire et homogène d'une série de fonctions entières à coefficients entiers font en quelque sorte partie d'une même famille, car ils ont un caractère commun, et ce caractère ne peut pas être, comme tout à l'heure, simplement donné par le plus grand commun diviseur des fonctions considérées. Ainsi déjà dans un domaine d'intégrité $[\mathfrak{R}]$, les développements précédents sont indispensables.

Un exemple bien simple éclaircira, peut être, ce que ces considérations générales pourraient avoir laissé d'obscur.

Les deux fonctions

$$f_n = x^{n-1} + x^{n-2} + \ldots + x + 1$$

et

$$f_{m,n} = x^{(m-1)n} + x^{(m-2)n} + \ldots + x^n + 1$$

où m et n désignent des entiers quelconques, sont premières entre elles. La recherche de leur plus grand commun diviseur nous donne, en effet,

$$f_{m,n} = f_n \cdot \sum_{k=2}^{m} (k-1)(x^{(m-k)n+1} - x^{(m-k)n}) + m.$$

Nous pouvons donc écrire

$$m \equiv 0 \pmod{\text{dd}} f_{m,n},\ f_n)$$

et

$$f_{m,n} \equiv 0 \pmod{\text{dd}} f_n,\ m);$$

il est d'ailleurs manifeste que

$$f_n \equiv 0 \ (\mathrm{modd}\, f_{m,n},\ f_n)$$

et que

$$f_n \equiv 0 \ (\mathrm{modd}\, f_n,\ m).$$

Nous avons donc deux systèmes équivalents

$$(f_{m,n},\ f_n) \quad \text{et} \quad (f_n,\ m)$$

et, en effet, chacun de ces systèmes contient bien l'autre, ainsi que l'on s'en assure à l'aide des quatre congruences précédentes.

L'équivalence

$$(f_{m,n},\ f_n) \sim (f_n,\ m)$$

nous montre clairement que les deux fonctions $f_{m,n}$ et f_n, quoiqu'étant premières entre elles, ont cependant quelque chose en commun et le nombre m est un des éléments qui caractérise leur liaison.

L'équivalence précédente nous amène à une remarque bien simple à l'aide de laquelle on pourrait caractériser, dès le début de l'arithmétique, un genre de liaison comme celui des deux fonctions $f_{m,n}$ et f_n. Introduire en Arithmétique les fonctions d'une variable, à coefficients entiers, c'est considérer toutes les valeurs que prennent ces fonctions lorsque la variable parcourt successivement toute l'échelle des nombres entiers. Pour comparer entre elles deux fonctions d'une variable, il faut donc comparer deux suites d'entiers, les deux suites que l'on obtient en donnant successivement à la variable toutes les valeurs entières possibles et écrivant les entiers correspondants auxquels se réduisent les deux fonctions entières considérées. Il peut alors se présenter plusieurs cas. Ainsi lorsque les entiers correspondants restent toujours sans diviseur commun, le système des deux fonctions est équivalent à l'unité car le plus grand commun diviseur des deux fonctions ne peut, dans ce cas, être différent de l'unité. Au contraire, lorsque l'on rencontre un nombre infini d'entiers correspondants, ayant des diviseurs communs, tous facteurs d'un nombre déterminé m, ce nombre caractérise certainement, en partie du moins, une liaison entre les deux fonctions considérées. C'est ce qui arrive dans l'exemple précédent. Il est inutile d'insister ici sur cette interprétation que l'on pourrait, sans doute, rendre facilement rigoureuse.

Je voudrais enfin faire une remarque, d'ailleurs bien évidente, sur l'introduction des systèmes de diviseurs en Algèbre. Si, au lieu de dire qu'une fonction contient un système $(f_1, f_2, \ldots, f_k)$ lorsqu'elle peut être mise sous la forme d'une fonction linéaire et homogène de $f_1, f_2, \ldots, f_k$, nous disions qu'elle contient le système $(f_1, f_2, \ldots, f_k)$ lorsqu'elle peut être mise sous la forme d'une fonction homogène de $f_1, f_2, \ldots, f_k$, d'une dimension donnée quelconque, nous n'obtiendrions rien de nouveau; nous ne ferions que nous limiter dans nos recherches, sans pouvoir en tirer aucun profit. Et nous devons considérer un ensemble *homogène;* car, dans le cas contraire, nous aurions un système dans lequel l'un des éléments devrait être égal à l'unité. Mais alors ce système serait contenu dans l'unité et, par suite, dans tous les nombres; il ne servirait donc à rien de l'introduire dans nos recherches.

4. Après avoir défini l'équivalence des systèmes de fonctions, il faut encore nous entendre sur la manière dont nous voulons *composer* ces systèmes; je dirais *multiplier,* si ici la notion d'égalité n'était pas remplacée par celle d'équivalence.

Il convient de nommer *système composé* de deux systèmes donnés, le système dont les éléments sont obtenus en multipliant, de toutes les manières possibles, les éléments de l'un des systèmes donnés par ceux de l'autre; car le système ainsi formé est, par rapport aux systèmes donnés, ce que le produit de deux fonctions est par rapport à ses facteurs. Nous écrirons donc, par exemple,

$$(a, b)(c, d) \sim (ac, bc, ad, bd).$$

La méthode à suivre pour résoudre le problème de la composition de deux et, par suite, de plusieurs systèmes en un seul étant ainsi fixée par définition, le problème inverse s'impose, celui de donner une méthode pour *décomposer* en plusieurs systèmes plus simples, un système quelconque donné. C'est ce problème qui fera l'objet de toutes les recherches contenues dans la seconde moitié de ce Mémoire.

La première recherche se rapportant à la divisibilité des fonctions entières est celle du plus grand commun diviseur de deux fonctions. Pour suivre une voie analogue à celle du chapitre précédent nous devrons donc, tout d'abord, chercher à voir ce qu'il faut entendre par plus grand commun diviseur de deux systèmes de fonctions.

Désignons par $(f_1, f_2, \ldots, f_m)$ et $(f_{m+1}, f_{m+2}, \ldots, f_n)$ deux systèmes donnés et formons le système

$$(f_1, f_2, \ldots, f_n).$$

Il est contenu dans chacun des systèmes donnés, car il est contenu dans chacun de leurs éléments. De plus, si un système quelconque $(\varphi_1, \varphi_2, \ldots)$ est contenu dans les deux systèmes donnés, nous avons, par définition,

$$f_k \equiv 0 \,(\mathrm{modd}\, \varphi_1, \varphi_2, \ldots) \qquad (k=1,2,\ldots,m; m+1, m+2, \ldots, n)$$

et, par suite,

$$(f_1, f_2, \ldots, f_n) \equiv 0 \,(\mathrm{modd}\, \varphi_1, \varphi_2, \ldots).$$

Nous voyons donc aussi que tout système $(\varphi_1, \varphi_2, \ldots)$ contenu dans les deux systèmes $(f_1, f_2, \ldots, f_m)$ et $(f_{m+1}, f_{m+2}, \ldots, f_n)$ est également contenu dans leur diviseur commun $(f_1, f_2, \ldots, f_n)$. C'est pourquoi nous dirons que $(f_1, f_2, \ldots, f_n)$ est *le plus grand commun diviseur* des deux systèmes $(f_1, f_2, \ldots, f_m)$ et $(f_{m+1}, f_{m+2}, \ldots, f_n)$.

Le symbole de M. KRONECKER présente ainsi un grand avantage; il permet de former immédiatement le plus grand commun diviseur de deux systèmes, en juxtaposant leurs éléments, c'est à dire en écrivant les éléments du second système à la suite de ceux du premier et en réunissant tous ces éléments en un seul système. Et cet avantage n'est contrebalancé par aucun désavantage; car il est parfaitement indifférent que nous ayons, dans le système ainsi formé, un plus grand nombre d'éléments que dans les systèmes donnés; le nombre d'éléments d'un système ne complique, en effet, en rien nos recherches; la nature des systèmes ne dépend pas du nombre d'éléments qui les composent.

Remarquons d'ailleurs que rien ne sera changé dans un système de modules, si nous ajoutons à ses éléments une fonction linéaire et homogène de quelques-uns d'entre eux; car, si

$$f_{n+1} \equiv 0 \,(\mathrm{modd}\, f_1, f_2, \ldots, f_k) \qquad (k \leqq n)$$

nous avons, par définition,

$$(f_1, f_2, \ldots, f_{n+1}) \sim (f_1, f_2, \ldots, f_n);$$

nous pouvons donc ajouter aux éléments $f_1, f_2, \ldots, f_n$, l'élément f_{n+1}, ou retrancher des éléments $f_1, f_2, \ldots, f_{n+1}$, ce même élément f_{n+1}.

Ce que nous venons de dire du plus grand commun diviseur de deux systèmes, s'étend immédiatement au plus grand commun diviseur d'un nombre quelconque de systèmes.

Si $f_0 = g_1 f_1 + f_2$, on a

$$(f_0, f_1) \sim (f_0, f_1, f_2) \sim (f_1, f_2).$$

Ainsi $(15, 25) \sim (15, 25, 25 - 15) \sim (15, 10 + 15, 10) \sim (15, 10) \sim (15, 10, 15 - 10) \sim (10 + 5, 10, 5) \sim (10, 5) \sim 5$.

Une remarque intéressante et bien facile à vérifier, est que le procédé de réduction d'un système, dont nous venons de donner un exemple, nous donne, appliqué aux nombres et répété un nombre suffisant de fois, précisément l'algorithme d'EUCLIDE.

Nous pouvons résumer les recherches de ce paragraphe en disant que nous arrivons à la même généralisation de l'idée de *contenant* et de *contenu*, que nous nous placions au point de vue de la géométrie ou à celui de l'arithmétique, à condition, toutefois, de tenir compte, dans le premier cas, de la nature des coefficients des fonctions entières considérées. Dans le second cas, cette condition est inutile; il est, en outre, d'autant plus important qu'il se rapporte directement à la fonction elle-même, et non pas à cette fonction égalée à zéro. L'exemple du système $(f_{m,n}, f_n)$, que nous avons donné, nous montre que la géométrie est certainement insuffisante dans nos théories algébriques: Le système $(f_{m,n} = 0, f_n = 0)$ n'est en effet susceptible d'aucune interprétation géométrique.

§ 2.

Résultant pris suivant un module déterminé.

Nous allons maintenant aborder un tout autre ordre de questions et étudier l'algorithme du plus grand commun diviseur, en ne considérant les fonctions entières d'une variable x, que suivant un module

$\Psi(\mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)})$; $\mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)}$, désignant les éléments d'un domaine d'intégrité donné. Nous développerons cette théorie plus que cela ne serait nécessaire pour résoudre les problèmes proposés dans les paragraphes suivants, parce qu'elle fait partie de la théorie élémentaire des congruences, et permet de simplifier considérablement plusieurs recherches arithmétiques.

Supposons d'abord que le domaine d'intégrité soit $[1]$, et que le module soit simplement un nombre premier p.

Soient alors deux fonctions entières à coefficients entiers $f_1(x)$ et $f_2(x)$ non congrues à zéro suivant le module p; nous réduisons leurs coefficients à leur plus petit reste, suivant ce module. Si alors a_2 est le coefficient de la plus haute puissance de x, dans $f_2(x)$, on peut toujours déterminer un nombre α_2 tel que la congruence $a_2\alpha_2 \equiv 1 \pmod p$ soit vérifiée. En divisant $f_1(x)$ par $\alpha_2 f_2(x)$ nous obtenons comme quotient une fonction entière à coefficients entiers que nous nommons $g_2(x)$, après avoir réduit ses coefficients suivant le module p; nous réduisons egalement, suivant ce même module, les coefficients du reste de la division, et nous obtenons alors une fonction entière que nous désignons par $-f_3(x)$. Nous établissons ainsi la congruence

$$f_1(x) - \alpha_2 g_2(x) f_2(x) + f_3(x) \equiv 0 \pmod p.$$

En opérant, de même, avec $f_2(x)$ et $f_3(x)$, etc., nous obtenons une suite de congruences,

$$f_{k-1}(x) - \alpha_k g_k(x) f_k(x) + f_{k+1}(x) \equiv 0 \pmod p \qquad (k=2,3,\ldots,\nu-1)$$

et enfin

$$f_{\nu-1}(x) - \alpha_\nu g_\nu(x) f_\nu(x) \equiv 0 \pmod p$$

où $f_\nu(x)$ est une fonction entière de x, à coefficients entiers, qui peut se réduire à un nombre.

Ces congruences sont tout à fait analogues aux égalités de l'algorithme d'Euclide; elles n'en diffèrent qu'en ce que le signe d'égalité y est remplacé par celui de congruence. Nous en tirons donc immédiatement les trois congruences caractéristiques

$$f_1 \equiv \theta_1 f_\nu \pmod p$$
$$f_2 \equiv \theta_2 f_\nu \pmod p$$
$$f_\nu \equiv \varphi_1 f_1 + \varphi_2 f_2 \pmod p$$

que nous pouvons aussi écrire

$$f_1 \equiv 0 \,(\mathrm{modd}\, f_\nu,\ p)$$

$$f_2 \equiv 0 \,(\mathrm{modd}\, f_\nu,\ p)$$

$$f_\nu \equiv 0 \,(\mathrm{modd}\, f_1,\ f_2,\ p).$$

Les deux premières congruences nous donnent

$$(f_1,\ f_2) \equiv 0 \,(\mathrm{modd}\, f_\nu,\ p).$$

Le système (f_1, f_2) contient donc le système (f_ν, p). Ici encore on aperçoit clairement l'analogie avec la divisibilité par f_ν, de f_1 et de f_2, divisibilité que nous pouvons déduire des deux premières égalités caractéristiques de l'algorithme d'Euclide

$$f_1 = \theta_1 f_\nu; \qquad f_2 = \theta_2 f_\nu.$$

De la troisième égalité de cet algorithme nous avons déduit une des deux méthodes qui permettent de former le résultant R de deux fonctions entières, et nous avons démontré que la condition

$$R(f_1,\ f_2) = 0$$

était nécessaire et suffisante pour que les deux fonctions f_1 et f_2 aient un diviseur commun, dans le cas où $f_\nu = 1$. Nous allons généraliser ce théorème.

Le résultant de deux fonctions étant une fonction homogène et linéaire de ces deux fonctions, nous avons

$$R(f_1,\ f_2) \equiv 0 \,(\mathrm{modd}\, f_1,\ f_2)$$

et, par suite, d'après une remarque faite plus haut,

$$[f_1,\ f_2,\ R(f_1,\ f_2)] \sim (f_1,\ f_2).$$

Ceci posé, supposons que la congruence $R(f_1, f_2) \equiv 0 \pmod p$ n'ait pas lieu. Si p désigne un nombre premier, R et p n'auront alors aucun diviseur commun, et nous aurons, par suite, $(R, p) \sim 1$. Il en résulte immédiatement

$$(f_1,\ f_2,\ R,\ p) \sim (f_1,\ f_2,\ 1) \sim 1.$$

Mais $(f_1, f_2, R) \sim (f_1, f_2)$; donc $(f_1, f_2, p) \sim 1$. Comme (f_1, f_2, p) est le plus grand commun diviseur des deux systèmes (f_1, p) et (f_2, p), nous avons enfin l'équivalence

$$\mathrm{Dv}[(f_1, p), (f_2, p)] \sim 1.$$

Ainsi, si la congruence $R(f_1, f_2) \equiv 0 \pmod{p}$ n'a pas lieu, les deux systèmes n'ont aucun diviseur commun.

Le résultat que nous venons d'obtenir nous montre que si les deux systèmes considérés ont un diviseur commun, il faut que le résultant $R(f_1, f_2)$ soit congru à zéro, suivant le module p.

En voici un exemple: Le système $(x + 3, 7)$ est contenu dans le système $(x^2 + x + 1, 7)$. On a, en effet,

$$(x^2 + x + 1, 7) \sim (x + 3, 7)(x - 2, 7).$$

Le résultant des deux fonctions $(x^2 + x + 1)$ et $(x + 3)$ est d'ailleurs égal à 7; on a donc bien $R \equiv 0 \pmod{7}$.

Réciproquement, si les deux systèmes (f_1, p) et (f_2, p), où nous désignerons par α et β les coefficients des deux fonctions entières $f_1(x)$ et $f_2(x)$, n'ont point de diviseur commun, la congruence $R(f_1, f_2) \equiv 0 \pmod{p}$ ne saurait avoir lieu. En effet, dans cette hypothèse, comme

$$\mathrm{Dv}[(f_1, p), (f_2, p)] \sim (f_1, f_2, p)$$

nous avons l'équivalence

$$(f_1, f_2, p) \sim 1$$

ou encore la congruence

$$\varphi_1(x) f_1(x) + \varphi_2(x) f_2(x) \equiv 1 \pmod{p}.$$

Cette congruence est vérifiée identiquement, par rapport à x; nous pouvons donc écrire, en désignant par u_k une indéterminée,

$$\varphi_1(u_k) f_1(u_k) + \varphi_2(u_k) f_2(u_k) \equiv 1 \pmod{p}.$$

Nous prendrons pour k toutes les valeurs entières depuis 1 jusqu'à $(m + n)$

si m et n indiquent les degrés de $f_1(x)$ et de $f_2(x)$, par rapport à x. Si alors, nous définissons $P_1(x)$ et $P_2(x)$ par les congruences

$$P_1(x) \equiv \prod_{h=1}^{m} (x - u_h) \pmod{p}$$

$$P_2(x) \equiv \prod_{h=m+1}^{m+n} (x - u_h) \pmod{p}$$

nous obtenons facilement la congruence

$$\prod_{k=1}^{m} \{\varphi_1(u_k) f_1(u_k) - \varphi_1(u_k) P_1(u_k) + \varphi_2(u_k) f_2(u_k)\} \equiv 1 \pmod{p};$$

le raisonnement est tout à fait celui du paragraphe 2 du chapitre précédent. Si $\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m$ désignent les fonctions symétriques élémentaires de $u_1, u_2, \ldots, u_m$ et $\mathfrak{g}_1, \mathfrak{g}_2, \ldots, \mathfrak{g}_n$ celles de $u_{m+1}, u_{m+2}, \ldots, u_{m+n}$, la congruence précédente peut être mise sous la forme

$$\prod_{k=1}^{m} \left| \varphi_1(u_k) \sum_{h=1}^{m} (-1)^h (\alpha_h - \mathfrak{f}_h) u_k^{m-h} + \varphi_2(u_k) f_2(u_k) \right| \equiv 1 \pmod{p}$$

ou encore, en posant, comme dans le paragraphe cité,

$$\prod_{k=1}^{m} f_2(u_k) = R(\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m; \beta_1, \beta_2, \ldots, \beta_n)$$

et

$$\prod_{k=1}^{m} \varphi_2(u_k) = S(\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m),$$

$$R(\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m; \beta_1, \beta_2, \ldots, \beta_n) S(\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m) \equiv 1 \text{ (modd } p, \alpha_1 - \mathfrak{f}_1, \ldots, \alpha_m - \mathfrak{f}_m).$$

Cette congruence est vérifiée identiquement en $u_1, u_2, \ldots, u_m$, donc en $\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m$; elle a donc lieu pour $\mathfrak{f}_1 = \alpha_1, \mathfrak{f}_2 = \alpha_2, \ldots, \mathfrak{f}_m = \alpha_m$ et comme la valeur de $S(\alpha_1, \alpha_2, \ldots, \alpha_m)$ est finie, il est impossible que la congruence

$$R(\alpha_1, \alpha_2, \ldots, \alpha_m; \beta_1, \beta_2, \ldots, \beta_n) \equiv 0 \pmod{p}$$

soit vérifiée. On démontre, comme dans le paragraphe cité, l'identité des deux fonctions R que nous venons de définir; on peut alors énoncer le théorème suivant:

»*La condition* $R(f_1, f_2) \equiv 0 \pmod{p}$ *est nécessaire et suffisante pour que les deux systèmes* (f_1, p) *et* (f_2, p) *aient un diviseur commun, et cela quelle que soit la nature particulière des deux fonctions entières de* x, $f_1(x)$ *et* $f_2(x)$, *que nous considérons.*«

Dans le cas particulier où le résultant des deux fonctions $f_1(x)$ et $f_2(x)$ est précisément égal au nombre premier p, nous avons aussi

$$p \equiv 0 \,(\mathrm{modd}\, f_1, f_2).$$

Mais alors, au lieu de $f_\nu \equiv 0 \,(\mathrm{modd}\, f_1, f_2, p)$, nous pouvons écrire simplement $f_\nu \equiv 0 \,(\mathrm{modd}\, f_1, f_2)$, et comme

$$(f_1, f_2) \equiv 0 \,(\mathrm{modd}\, f_\nu, p)$$

nous obtenons l'équivalence

$$(f_1, f_2) \sim (f_\nu, p).$$

Le cas plus général où le module ne se réduit pas à un nombre premier p, mais est une fonction irréductible $\Psi(\mathfrak{R}')$ d'une variable-indéterminée $\mathfrak{R}'$, dont les coefficients font partie du domaine naturel de rationalité $(\mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)})$, le coefficient de la plus haute puissance étant égal à l'unité, peut être traité de la même manière, lorsque les coefficients de la plus haute puissance de chacune des deux fonctions de x, $f_1(x)$ et $f_2(x)$, sont congrus à l'unité, suivant le module $\Psi(\mathfrak{R}')$. Mais il ne faut pas oublier que nous privilégions ainsi l'une des variables-indéterminées du domaine d'intégrité donné; nous pouvons donc seulement dire que le système (f_1, f_2) contient le système (f_ν, Ψ) *relativement* à l'une des indéterminées $\mathfrak{R}'$ du domaine d'intégrité. Dans ce même sens restreint nous pouvons également énoncer le théorème:

»La congruence $R(f_1, f_2) \equiv 0 \pmod{\Psi}$, où R désigne le résultant des deux fonctions entières f_1 et f_2, pris par rapport à x, est nécessaire et suffisante pour que les deux systèmes (f_1, Ψ) et (f_2, Ψ) aient un diviseur commun.«

§ 3.

Application des systèmes de modules à la décomposition d'une fonction entière dans un domaine général de rationalité.

1. L'emploi des systèmes de modules nous permet d'effectuer, plus facilement, la décomposition d'une fonction entière dont les coefficients font partie d'un domaine *général* de rationalité, sans introduire dans nos recherches l'idée de nombre et fonction algébrique. C'est ce que je vais essayer de faire voir dans ce paragraphe.

En reprenant ainsi, sous une autre forme, les recherches du dernier paragraphe du chapitre précédent et en montrant comment elles se traduisent à l'aide des nouveaux symboles, mon but est, surtout, de mettre en évidence, par un exemple, d'une part le rôle important que jouent actuellement dans les recherches d'Algèbre, les fonctions algébriques, les grandes simplifications que l'emploi de ces fonctions peut apporter dans le mécanisme d'une démonstration, et, d'autre part, la méthode à suivre pour éviter précisément l'emploi de ces fonctions. La complication de cette méthode n'est qu'apparente et ne porte *que* sur le mécanisme de la démonstration; loin de rendre la démonstration elle-même plus difficile, elle nous fait, au contraire, apercevoir plus clairement le lien entre les hypothèses que nous faisons et le résultat qui en découle, entre notre point de départ et notre point d'arrivée; et *seule,* elle mérite le nom de méthode algébrique, car, seule, elle se meut dans le domaine particulier à l'Algèbre.

Je commencerai par formuler, à l'aide de notre nouvelle terminologie, le problème proposé d'une manière qui diffère un peu de celle du chapitre précédent. Dans ce problème, les éléments d'un domaine de rationalité $(\mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)})$ sont supposés liés par *une* relation algébrique $\Psi(\mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)}) = 0$. Nous pouvons supposer que la fonction entière Ψ soit irréductible, car nous savons décomposer, en ses facteurs irréductibles, toute fonction faisant partie d'un domaine naturel de rationalité.

Il s'agit de décomposer, si possible, une fonction entière de z, $F(z)$ dont les coefficients font partie du domaine $(\Re', \Re'', \ldots, \Re^{(\mu)})$ ainsi limité par la relation $\Psi = 0$, c'est à dire de mettre $F(z)$ sous la forme d'un produit de deux ou plusieurs fonctions de z dont les coefficients fassent également partie du domaine $(\Re', \Re'', \ldots, \Re^{(\mu)})$ limité par la même relation $\Psi = 0$.

Dire que $F(z)$ contient une fonction $F_1(z)$, tandis que $\Re', \Re'', \ldots, \Re^{(\mu)}$, sont liés par l'équation $\Psi = 0$, c'est donc dire que $F(z)$ est congru au produit de $F_1(z)$ et d'une autre fonction entière de z, suivant le module Ψ, ou, en d'autres termes, c'est dire que $F(z)$ est congru à zéro suivant le système de modules $[F_1(z), \Psi]$. La divisibilité des fonctions entières, dans un domaine général de rationalité, revient ainsi à la décomposition des fonctions entières à coefficients faisant partie d'un domaine naturel de rationalité, en systèmes de diviseurs dont l'un des éléments, commun à tous les systèmes, est connu et ne renferme pas la variable indépendante z, ou encore, à décomposer dans un domaine naturel de rationalité, un système donné $[F(z), \Psi]$ en d'autres systèmes contenant chacun l'élément Ψ. C'est ce problème de la décomposition des systèmes dans un cas très-particulier, que je veux étudier dans ce paragraphe.

A cet effet, je suivrai une voie analogue à celle du dernier paragraphe du chapitre précédent, et, conservant les mêmes notations, je démontrerai d'abord que les entiers désignés par μ_i (page 43) sont nécessairement égaux à l'unité, ou, ce qui revient au même, que le résultant, par rapport à z, du résultant, par rapport à $\Re'$, des deux fonctions F et Ψ, et de la dérivée, par rapport à z, de ce résultant, diffère nécessairement de zéro. Je rappelle que, dans la fonction F, le coefficient de la plus haute puissance de z et, dans la fonction Ψ, le coefficient de la plus haute puissance de $\Re'$, sont supposés égaux à l'unité, et que, de plus, $F(z)$ peut toujours sans restriction aucune, être supposée fonction entière de z *et* de $\Re'$ sans diviseur commun avec sa dérivée prise par rapport à z, $F'(z)$, tandis que Ψ est fonction entière de $\Re'$ seulement,

$$\Psi(\Re') = \Re'^n + \psi_1 \Re'^{n-1} + \ldots + \psi_n;$$

les coefficients de F et de Ψ sont fonctions rationnelles des variables-indéterminées $\Re'', \Re''', \ldots, \Re^{(\mu)}$.

Soit $S = R(z;\ \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)})$ le résultant, par rapport à $\mathfrak{R}'$, des deux fonctions

$$F(z + t\mathfrak{R}';\ \mathfrak{R}', \ldots, \mathfrak{R}^{(\mu)}) \text{ et } \Psi(\mathfrak{R}';\ \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)})$$

t étant une indéterminée. D'après ce que j'ai exposé sur le résultant de deux fonctions entières, si $\mathfrak{g}_1, \mathfrak{g}_2, \ldots, \mathfrak{g}_n$ désignent les fonctions symétriques élémentaires des indéterminées $v_1, v_2, \ldots, v_n$, et si la fonction symétrique de ces indéterminées

$$\prod_{k=1}^{n} F(z + tv_k;\ v_k,\ \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)})$$

transformée en une fonction entière de $\mathfrak{g}_1, \mathfrak{g}_2, \ldots, \mathfrak{g}_n$, est égale à

$$\Phi(z,\ t,\ \mathfrak{g}_1,\ \mathfrak{g}_2, \ldots, \mathfrak{g}_n;\ \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)}),$$

on a

$$S = \Phi(z,\ t,\ \psi_1,\ \psi_2, \ldots, \psi_n;\ \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)});$$

et, si la fonction symétrique de $v_1, v_2, \ldots, v_n$,

$$\sum_{k=1}^{n} \frac{F'(z + tv_k;\ v_k)}{F(z + tv_k;\ v_k)} \prod_{h=1}^{n} F(z + tv_h;\ v_h)$$

transformée en une fonction entière de $z, t, \mathfrak{g}_1, \mathfrak{g}_2, \ldots, \mathfrak{g}_n$, est égale à

$$\Phi_1(z,\ t,\ \mathfrak{g}_1,\ \mathfrak{g}_2, \ldots, \mathfrak{g}_n)$$

on a aussi

$$\frac{\partial S}{\partial z} = \Phi_1(z,\ t,\ \psi_1,\ \psi_2, \ldots, \psi_n).$$

Pour abréger je n'ai plus écrit les éléments $\mathfrak{R}''$, $\mathfrak{R}'''$, ..., $\mathfrak{R}^{(\mu)}$, qui ne seront pas transformés dans le courant de la démonstration.

Formons maintenant le résultant, par rapport à z, des deux fonctions S et $\frac{\partial S}{\partial z}$. Il est égal à

$$T(t,\ \psi_1,\ \psi_2, \ldots, \psi_n)$$

si nous désignons par $T(t, g_1, g_2, \ldots, g_n)$ le résultant, par rapport à z, des deux fonctions

$$\Phi(z, t, g_1, g_2, \ldots, g_n) \text{ et } \Phi_1(z, t, g_1, g_2, \ldots, g_n).$$

Ce qu'il faut démontrer, c'est que $T(t, g_1, g_2, \ldots, g_n)$ est différent de zéro. En appliquant plusieurs fois les identités

$$R(ab, c) = R(a, c)R(b, c)$$

$$R(a + b, b) = R(a, b)$$

qui découlent immédiatement de la définition même du résultant de deux fonctions entières, nous pouvons écrire

$$T(t; g_1, g_2, \ldots, g_n) = R\left\{\prod_{h=1}^{n} F(z + tv_h, v_h); \sum_{i=1}^{n} \frac{F'(z + tv_i, v_i)}{F(z + tv_i, v_i)} \prod_{k=1}^{n} F(z + tv_k, v_k)\right\}$$

$$= \prod_{h=1}^{n} R\left\{F(z + tv_h, v_h)); \sum_{i=1}^{n} \frac{F'(z + tv_i, v_i)}{F(z + tv_i, v_i)} \prod_{k=1}^{n} F(z + tv_k, v_k)\right\}$$

$$= \prod_{h=1}^{n} R\left\{F(z + tv_h, v_h); \frac{F'(z + tv_h, v_h)}{F(z + tv_h, v_h)} \prod_{k=1}^{n} F(z + tv_k, v_k)\right\}$$

$$= \prod_{h=1}^{n} R\{F(z + tv_h, v_h); F'(z + tv_h, v_h)\} \prod_{h=1}^{n} R\left\{F(z + tv_h, v_h); \prod_{(k)} F(z + tv_k, v_k)\right\}$$

$$(k = 1, 2, \ldots (h-1), (h+1), \ldots, n)$$

$$= \prod_{h=1}^{n} R\{F(z + tv_h, v_h); F'(z + tv_h, v_h)\} \prod_{(h,k)} R\{F(z + tv_h, v_h); F(z + tv_k, v_k)\}.$$

$$\begin{pmatrix} h = 1, 2, \ldots, n \\ k = 1, 2, \ldots, (h-1), (h+1), \ldots, n \end{pmatrix}$$

Il suffit donc de démontrer que chacun des deux produits

$$\prod_{h=1}^{n} R\{F(z + tv_h, v_h); F'(z + tv_h, v_h)\}$$

et

$$\prod_{(h,k)} R\{F(z + tv_h, v_h); F(z + tv_k, v_k)\} \quad \begin{pmatrix} h = 1, 2, \ldots, n \\ k = 1, 2, \ldots, (h-1), (h+1), \ldots, n \end{pmatrix}$$

est différent de zéro lorsqu'on y remplace les fonctions symétriques élémentaires $g_1, g_2, \ldots, g_n$, par les coefficients $\phi_1, \phi_2, \ldots, \phi_n$ de la fonction $\Psi(\Re')$.

Comme, par hypothèse, les deux fonctions $F(z, \mathfrak{R}')$ et $\frac{\partial F(z, \mathfrak{R}')}{\partial z}$ n'ont point de diviseur commun et comme t est une indéterminée, les deux fonctions $F(x, \mathfrak{R}')$ et $F'(x, \mathfrak{R}')$, où $x = z + t\mathfrak{R}'$, n'auront également pas de diviseur commun; nous pouvons donc appliquer à ces deux fonctions les raisonnements du paragraphe 2 du chapitre précédent, et, en conservant les mêmes notations, établir l'égalité,

$$\prod_{k=1}^{m}\{\Phi(u_k, \mathfrak{R}')F(u_k, \mathfrak{R}') - \Phi(u_k, \mathfrak{R}')P(u_k, \mathfrak{R}') + \Psi(u_k, \mathfrak{R}')F'(u_k, \mathfrak{R}')\} = 1.$$

Cette égalité a lieu pour $\mathfrak{R}' = v_1, v_2, \ldots, v_n$; nous avons donc aussi

$$\prod_{(h,k)}\{\Phi(u_k, v_h)F(u_k, v_h) - \Phi(u_k, v_h)P(u_k, v_h) + \Psi(u_k, v_h)F'(u_k, v_h)\} = 1 \qquad \binom{h=1, 2, \ldots, n}{k=1, 2, \ldots, m}$$

et, par suite, en posant,

$$F(x, v_h) = x^m - \alpha_1^{(h)}x^{m-1} + \alpha_2^{(h)}x^{m-2} - \ldots + (-1)^m\alpha_m^{(h)} \qquad (h=1, 2, \ldots, n)$$

$$P(x, v_h) = x^m - \mathfrak{f}_1^{(h)}x^{m-1} + \mathfrak{f}_2^{(h)}x^{m-2} - \ldots + (-1)^m\mathfrak{f}_m^{(h)}, \qquad (h=1, 2, \ldots, n)$$

$$\prod_{(h,k)}\{\Psi(u_h, v_h)F'(u_h, v_h)\} \equiv 1$$

$$[\mathrm{modd}\,(\alpha_1^{(1)} - \mathfrak{f}_1^{(1)}), (\alpha_2^{(1)} - \mathfrak{f}_2^{(1)}), \ldots, (\alpha_m^{(1)} - \mathfrak{f}_m^{(1)}), (\alpha_1^{(2)} - \mathfrak{f}_1^{(2)}), \ldots, (\alpha_m^{(n)} - \mathfrak{f}_m^{(n)})].$$

Soient maintenant

$$\prod_{k=1}^{m}F'(u_k, v_h) = R(v_h; \mathfrak{f}_1^{(h)}, \mathfrak{f}_2^{(h)}, \ldots, \mathfrak{f}_m^{(h)})$$

et

$$\prod_{k=1}^{m}\Psi(u_k, v_h) = S(v_h; \mathfrak{f}_1^{(h)}, \mathfrak{f}_2^{(h)}, \ldots, \mathfrak{f}_m^{(h)});$$

nous savons alors que $R(v_h; \alpha_1^{(h)}, \alpha_2^{(h)}, \ldots, \alpha_m^{(h)})$ est bien le résultant des deux fonctions $F(x, v_h)$ et $F'(x, v_h)$. En désignant les fonctions entières de $\mathfrak{g}_1, \mathfrak{g}_2, \ldots, \mathfrak{g}_n$

$$\prod_{h=1}^{n}R(v_h, \mathfrak{f}_1^{(h)}, \mathfrak{f}_2^{(h)}, \ldots, \mathfrak{f}_m^{(h)}) \text{ et } \prod_{h=1}^{n}S(v_h, \mathfrak{f}_1^{(h)}, \mathfrak{f}_2^{(h)}, \ldots, \mathfrak{f}_m^{(h)})$$

respectivement par

$$U(g_1, g_2, \ldots, g_n, f_1^{(1)}, f_2^{(1)}, \ldots, f_m^{(1)}, f_1^{(2)}, \ldots, f_m^{(n)})$$

et

$$V(g_1, g_2, \ldots, g_n, f_1^{(1)}, f_2^{(1)}, \ldots, f_m^{(1)}, f_1^{(2)}, \ldots, f_m^{(n)}),$$

et en substituant ces expressions dans la congruence précédente, nous avons aussi,

$$U(g_1, g_2, \ldots, g_n, f_1^{(1)}, f_2^{(1)}, \ldots, f_m^{(n)})\, V(g_1, g_2, \ldots, g_n, f_1^{(1)}, f_2^{(1)}, \ldots, f_m^{(n)}) \equiv 1$$
$$[\mathrm{modd}\,(\alpha_1^{(1)} - f_1^{(1)}),\ (\alpha_2^{(1)} - f_2^{(1)}),\ \ldots,\ (\alpha_m^{(n)} - f_m^{(n)})].$$

Si dans cette congruence nous substituons aux indéterminées $f_1^{(1)}, f_2^{(1)}, \ldots, f_m^{(n)}$, les coefficients $\alpha_1^{(1)}, \alpha_2^{(1)}, \ldots, \alpha_m^{(n)}$ des fonctions $F(x, v_1), F(x, v_2), \ldots, F(x, v_n)$ considérées comme fonctions de x seulement, elle aura toujours lieu. D'ailleurs, comme pour $i = 1, 2, \ldots, m$, les deux fonctions

$$U(g_1, g_2, \ldots, g_n, \alpha_1^{(1)}, \ldots, \alpha_m^{(n)}) \text{ et } V(g_1, g_2, \ldots g_n, \alpha_1^{(1)}, \ldots, \alpha_m^{(n)})$$

sont fonctions symétriques de $\alpha_i^{(1)}, \alpha_i^{(2)}, \ldots, \alpha_i^{(n)}$, ces deux fonctions peuvent être transformées en fonctions entières de $g_1, g_2, \ldots, g_n$ ne contenant plus explicitement les indéterminées $v_1, v_2, \ldots, v_n$. La congruence que nous venons d'écrire est vérifiée identiquement en $g_1, g_2, \ldots, g_n$; elle est donc encore vérifiée si, après la transformation indiquée, nous substituons aux indéterminées $g_1, g_2, \ldots, g_n$ les coefficients $\psi_1, \psi_2, \ldots, \psi_n$ de la fonction $\Psi(\mathfrak{R}')$.

Nous avons donc enfin

$$U(\psi_1, \psi_2, \ldots, \psi_n, \alpha_1^{(1)}, \alpha_2^{(1)}, \ldots, \alpha_m^{(n)})\, V(\psi_1, \psi_2, \ldots, \psi_n, \alpha_1^{(1)}, \alpha_2^{(1)}, \ldots, \alpha_m^{(n)}) = 1$$

et comme la fonction entière $V(\psi_1, \psi_2, \ldots, \psi_n, \alpha_1^{(1)}, \alpha_2^{(1)}, \ldots, \alpha_m^{(n)})$ ne peut être infinie, la fonction $U(\psi_1, \psi_2, \ldots, \psi_n, \alpha_1^{(1)}, \alpha_2^{(1)}, \ldots, \alpha_m^{(n)})$ est certainement différente de zéro.

Mais la fonction $U(\psi_1, \psi_2, \ldots, \psi_n, \alpha_1^{(1)}, \alpha_2^{(1)}, \ldots, \alpha_m^{(n)})$ représente précisément le premier des deux facteurs de la fonction $T(t; \psi_1, \ldots, \psi_n)$ que nous considérons; ainsi, nous avons démontré que le produit

$$\prod_{h=1}^{n} R\{F(z + tv_h, v_h);\ F'(z + tv_h, v_h)\}$$

est nécessairement différent de zéro lorsqu'on y remplace les fonctions symétriques élémentaires $g_1, g_2, \ldots, g_n$ par les coefficients $\psi_1, \psi_2, \ldots, \psi_n$ de la fonction $\Psi(\mathfrak{R}')$.

2. Pour démontrer que le double produit

$$\prod_{(h,k)} R\{F(z + tv_h, v_h);\ F(z + tv_k, v_k)\} \qquad \binom{h,k=1,2,\ldots,n}{h \gtrless k}$$

est également différent de zéro on a besoin du théorème auxiliaire suivant.

»Les deux formes

$$\varphi = \prod_{h=1}^{n} \{a_0^{(h)} + a_1^{(h)} t + \ldots + a_m^{(h)} t^m\} = \sum_{k=0}^{mn} f_k t^k$$

et

$$\Phi = \prod_{h=1}^{n} \{a_0^{(h)} + a_1^{(h)} t_h + \ldots + a_m^{(h)} t_h^m\}$$

où $t, t_1, t_2, \ldots, t_n$ désignent des indéterminées et les $a_i^{(h)}$ des quantités quelconques, sont liées par une équation algébrique

$$\Phi^\nu - F_1 \Phi^{\nu-1} + F_2 \Phi^{\nu-2} - \ldots \pm F_\nu = 0$$

dans laquelle F_k $(k = 1, 2, \ldots, \nu)$ est une fonction homogène des seules quantités $f_0, f_1, \ldots, f_{mn}$ de dimension $k^{\text{ième}}$.»

Voici comment on démontre simplement ce théorème: (1)

Soient $v_1, v_2, \ldots, v_{mn}$, mn indéterminées. Posons

$$\mathfrak{f}_0 \prod_{(i)} (1 + v_i t) = \mathfrak{f}_0 + \mathfrak{f}_1 t + \mathfrak{f}_2 t^2 + \ldots + \mathfrak{f}_{mn} t^{mn} \qquad (i=1,2,\ldots,mn)$$

et

$$\mathfrak{g}_0 \prod_{(k_h)} (1 + v_{k_h} t) = \mathfrak{g}_0^{(h)} + \mathfrak{g}_1^{(h)} t + \mathfrak{g}_2^{(h)} t^2 + \ldots + \mathfrak{g}_m^{(h)} t^m \qquad [k_{h+1} = mh+1, mh+2, \ldots, m(h+1)]$$

pour $h = 1, 2, \ldots, n$, et considérons l'expression

$$G_0 = \prod_{(h)} \{\mathfrak{g}_0^{(h)} + \mathfrak{g}_1^{(h)} t_h + \mathfrak{g}_2^{(h)} t_h^2 + \ldots + \mathfrak{g}_m^{(h)} t_h^m\} \qquad (h=1,2,\ldots,n)$$

---

(1) Comparez KRONECKER, Sitzungsberichte der Berliner Akademie, 26 Juillet 1883.

que nous pouvons aussi mettre sous la forme

$$G_0 = \sum_{(k_1, k_2, \ldots, k_n)} \mathfrak{g}_{k_1}^{(1)} \mathfrak{g}_{k_2}^{(2)} \ldots \mathfrak{g}_{k_n}^{(n)} u_{k_1, k_2, \ldots, k_n}. \qquad \left(\begin{smallmatrix} k_{h+1} = mh+1, mh+2, \ldots, m(h+1) \\ h = 0, 1, 2, \ldots, (n-1) \end{smallmatrix}\right)$$

En examinant les coefficients $\mathfrak{g}_{k_1}^{(1)} \mathfrak{g}_{k_2}^{(2)} \ldots \mathfrak{g}_{k_n}^{(n)}$ de cette forme, nous voyons de suite qu'ils sont fonctions entières des indéterminées $v_1, v_2, \ldots, v_{mn}$ et ne sont que *linéaires* par rapport à chacune de ces indéterminées. Si nous permutons $v_1, v_2, \ldots, v_{mn}$ de toutes les manières possibles la fonction G_0 se change en un certain nombre de fonctions différentes que nous désignerons par $G_1, G_2, \ldots, G_{\nu-1}$; chacune de ces fonctions a, comme coefficients, des fonctions entières de $v_1, v_2, \ldots, v_{mn}$, linéaires par rapport à v_1, à $v_2, \ldots,$ à v_{mn}; si donc nous développons le produit $\prod_{r=0}^{\nu-1} (G - G_r)$ et si

$$\prod_{(r)} (G - G_r) = G^\nu - \mathfrak{F}_1 G^{\nu-1} + \mathfrak{F}_2 G^{\nu-2} - \ldots \pm \mathfrak{F}_\nu, \qquad [r = 0, 1, 2, \ldots, (\nu-1)]$$

la fonction *symétrique* $\mathfrak{F}_k$ sera une fonction homogène entière à coefficients entiers des indéterminées $\mathfrak{f}_0, \mathfrak{f}_1, \ldots, \mathfrak{f}_{mn}$, et sa dimension sera égale à k. Nous aurons ainsi

$$G_0^\nu - \mathfrak{F}_1 G_0^{\nu-1} + \mathfrak{F}_2 G_0^{\nu-2} - \ldots \pm \mathfrak{F}_\nu = 0$$

et comme cette relation a lieu identiquement en $v_1, v_2, \ldots, v_{mn}$, elle a encore lieu lorsque l'on substitue aux indéterminées $\mathfrak{g}_0^{(h)}, \mathfrak{g}_1^{(h)}, \ldots, \mathfrak{g}_m^{(h)}$, les quantités données $a_0^{(h)}, a_1^{(h)}, \ldots, a_m^{(h)}$, ce qui change G_0 en Φ; mais alors il faut aussi substituer à $\mathfrak{f}_0, \mathfrak{f}_1, \ldots, \mathfrak{f}_{mn}$ les quantités $f_0, f_1, \ldots, f_{mn}$, et le théorème est démontré.

3. Supposons maintenant que lorsqu'on remplace les indéterminées $\mathfrak{g}_1, \mathfrak{g}_2, \ldots, \mathfrak{g}_n$ par $\psi_1, \psi_2, \ldots, \psi_n$, le double produit

$$\prod_{(h,k)} R\{F(z + tv_h, v_h);\ F(z + tv_k, v_k)\} \qquad \left(\begin{smallmatrix} h, k = 1, 2, \ldots, n \\ h \gtrless k \end{smallmatrix}\right)$$

soit nul. Il en serait alors de même du double produit

$$\prod_{(h,k)} R_x\{F(x, v_h);\ F[x + t(v_k - v_h), v_k]\} \qquad \left(\begin{smallmatrix} h, k = 1, 2, \ldots, n \\ h \gtrless k \end{smallmatrix}\right)$$

dans lequel nous avons posé $x = z + tv_h$, le résultant étant formé par rapport à x. Mais alors, après avoir remplacé les indéterminées

$\mathfrak{g}_1, \mathfrak{g}_2, \ldots, \mathfrak{g}_n$, par les quantités données $\psi_1, \psi_2, \ldots, \psi_n$, nous aurions aussi l'égalité

$$\prod_{(h,k)} R_x\{F(x, v_h);\ F(x, v_k) + t(v_k - v_h)F'(x, v_k) + \ldots + t^m(v_k - v_h)^m\} = 0 \qquad \begin{pmatrix} h,k=1,2,\ldots,n \\ h \gtrless k \end{pmatrix}$$

ou encore, en introduisant, comme dans la première partie de notre démonstration, pour $h = 1, 2, \ldots, n$, les fonctions auxiliaires

$$P(x, v_h) = \prod_{i=1}^{m}(x - u_i^{(h)}) = x^m - \mathfrak{f}_1^{(h)}x^{m-1} + \mathfrak{f}_2^{(h)}x^{m-2} - \ldots \pm \mathfrak{f}_m^{(h)},$$

$$\prod_{(h,i,k)}\{F(u_i^{(h)}, v_k) + t(v_k - v_h)F'(u_i^{(h)}, v_k) + \ldots + t^m(v_k - v_h)^m\} = 0 \qquad \begin{pmatrix} i=1,2,\ldots,m \\ h,k=1,2,\ldots,n \\ h \gtrless k \end{pmatrix}$$

à condition de remplacer, pour $h = 1, 2, \ldots, n$, dans la fonction entière de $\mathfrak{f}_1^{(h)}, \mathfrak{f}_2^{(h)}, \ldots, \mathfrak{f}_m^{(h)}$ qui représente le terme de gauche de cette égalité, les indéterminées $\mathfrak{f}_1^{(h)}, \mathfrak{f}_2^{(h)}, \ldots, \mathfrak{f}_m^{(h)}$, par les coefficients $\alpha_1^{(h)}, \alpha_2^{(h)}, \ldots, \alpha_m^{(h)}$, de $F(x, v_h)$ considérée comme fonction de x seulement, puis, après avoir transformé la fonction symétrique de $v_1, v_2, \ldots, v_n$, ainsi obtenue, en une fonction entière de $\mathfrak{g}_1, \mathfrak{g}_2, \ldots, \mathfrak{g}_n$, de remplacer les indéterminées $\mathfrak{g}_1, \mathfrak{g}_2, \ldots, \mathfrak{g}_n$ par les quantités données $\psi_1, \psi_2, \ldots, \psi_n$.

Ordonnons ce produit par rapport à l'indéterminée t; tous les coefficients seront nuls. D'après le théorème auxiliaire que nous venons de démontrer, une puissance entière du produit

$$\prod_{(h,i,k)}\{F(u_i^{(h)}, v_k) + t_{h,k}(v_k - v_h)F'(u_i^{(h)}, v_k) + \ldots + t_{h,k}^m(v_k - v_h)^m\} \qquad \begin{pmatrix} i=1,2,\ldots,m \\ h,k=1,2,\ldots,n \\ h \gtrless k \end{pmatrix}$$

sera également nulle; donc aussi ce produit lui-même.

Posons, pour abréger,

$$t_{h,k}(v_k - v_h) = w'_{h,k}$$

et introduisons de nouvelles indéterminées $w_{h,k}$ comme coefficients des expressions $F(u_i^{(h)}, v_k)$; nous aurons alors

$$\prod_{(h,i,k)}\{w_{h,k}F(u_i^{(h)}, v_k) + w'_{h,k}F'(u_i^{(h)}, v_k) + \ldots + w'^m_{h,k}\} = L = 0 \qquad \begin{pmatrix} i=1,2,\ldots,m \\ h,k=1,2,\ldots,n \\ h \gtrless k \end{pmatrix}$$

ou encore, en écrivant

$$L - \prod_{(h,i,k)} \{w_{h,k} F(u_i^{(h)}, v_k) + w'_{h,k} F'(u_i^{(h)}, v_k)\} = l \qquad \left(\begin{smallmatrix} i = 1, 2, \ldots, m \\ h, k = 1, 2, \ldots, n \\ h \gtrless k \end{smallmatrix}\right)$$

$$\prod_{(h,i,k)} \{w_{h,k} F(u_i^{(h)}, v_k) + w'_{h,k} F'(u_i^{(h)}, v_k)\} + l = 0. \qquad \left(\begin{smallmatrix} i = 1, 2, \ldots, m \\ h, k = 1, 2, \ldots, n \\ h \gtrless k \end{smallmatrix}\right)$$

Comme l est une fonction entière de $\phi_1, \phi_2, \ldots, \phi_n$, ne contenant plus les indéterminées auxiliaires u et v, et que chacun des termes de l contient au moins une des indéterminées $w'_{h,k}$ à une puissance plus élevée que la première, il faut que nous ayons séparément

$$\prod_{(h,i,k)} \{w_{h,k} F(u_i^{(h)}, v_k) + w'_{h,k} F'(u_i^{(h)}, v_k)\} = 0 \quad \text{et} \quad l = 0. \qquad \left(\begin{smallmatrix} i = 1, 2, \ldots, m \\ h, k = 1, 2, \ldots, n \\ h \gtrless k \end{smallmatrix}\right)$$

Ainsi, nous avons démontré que si le double produit

$$\prod_{(h,k)} R\{F(z + tv_h, v_h); F(z + tv_k, v_k)\}$$

est nul, pour t indéterminée, les deux dernières égalités sont vérifiées identiquement dans les indéterminées

$$w_{h,k} \quad \text{et} \quad w'_{h,k}. \qquad \left(\begin{smallmatrix} h, k = 1, 2, \ldots, n \\ h \gtrless k \end{smallmatrix}\right)$$

Mais, d'autre part, il est facile de donner à ces indéterminées $w_{h,k}$ et $w'_{h,k}$ des valeurs particulières pour lesquelles la dernière égalité n'est pas vérifiée. Nous avons, en effet, vu tout à l'heure que le produit

$$\prod_{k=1}^{n} R\{F(x, v_k), F'(x, v_k)\}$$

était différent de zéro. Comme l'égalité

$$R_z\{F(z); F'(z)\} = F_1(z) F(z) + F_2(z) F'(z)$$

que l'on peut établir quelle que soit $F(z)$, est vérifiée identiquement en z, nous pouvons aussi dire que le produit

$$\prod_{k=1}^{n} \{F_1(u_i^{(h)}, v_k) F(u_i^{(h)}, v_k) + F_2(u_i^{(h)}, v_k) F'(u_i^{(h)}, v_k)\}$$

et, par suite, que le triple produit

$$\prod_{(h,i,k)} \{F_1(u_i^{(h)}, v_k) F(u_i^{(h)}, v_k) + F_2(u_i^{(h)}, v_k) F'(u_i^{(h)}, v_k)\} \qquad \begin{pmatrix} i = 1, 2, \ldots, m \\ h, k = 1, 2, \ldots, n \\ h \gtrless k \end{pmatrix}$$

est différent de zéro.

Si donc nous remplaçons les indéterminées $w_{h,k}$ et $w'_{h,k}$ par les fonctions $F_1(u_i^{(h)}, v_k)$ et $F_2(u_i^{(h)}, v_k)$, la fonction symétrique des u et des v,

$$\prod_{(h,i,k)} \{w_{h,k} F(u_i^{(h)}, v_k) + w'_{h,k} F'(u_i^{(h)}, v_k)\}$$

dans laquelle on remplace les fonctions symétriques élémentaires de $u_1^{(h)}, u_2^{(h)}, \ldots, u_m^{(h)}$ par les coefficients de $F(x, v_h)$, considérée comme fonction de x seulement, puis $g_1, g_2, \ldots, g_n$ par $\psi_1, \psi_2, \ldots, \psi_n$, est différente de zéro. Elle ne saurait donc être nulle pour des $w_{h,k}$ et $w'_{h,k}$ indéterminées, et, par suite, le second facteur du résultant

$$T(t, \psi_1, \psi_2, \ldots, \psi_n)$$

n'est pas nul non plus.

Cette recherche est nouvelle. Elle offre un exemple frappant de l'avantage qu'il y a à se servir de méthodes naturelles, sans introduire aucun élément étranger au domaine dans lequel on se meut. C'est, en effet, l'impossibilité dans laquelle je me suis trouvé, de démontrer que le résultant $T(t, \psi_1, \psi_2, \ldots, \psi_n)$ est différent de zéro, sans supposer l'existence des racines des équations algébriques, et à l'aide de la généralisation des idées de contenant et de contenu donnée au début de ce chapitre, qui a amené M. KRONECKER à généraliser d'avantage encore les idées de contenant et de contenu(1) en découvrant le théorème *auxiliaire*(2) nécessaire à notre démonstration, théorème qui, en réalité, est *fondamental* en Algèbre.

4. Il est maintenant facile de décomposer, dans un domaine naturel de rationalité, un système donné $[F(z), \Psi]$ en d'autres systèmes contenant chacun l'élément Ψ.

---

(1) Sitzungsberichte der Berliner Akademie. Séance du 26 Juillet 1883.

(2) Page 71 de ce Mémoire.

En effet,(1) nous venons de voir que le résultant

$$\Phi(z;\ t,\ \psi_1,\ \psi_2,\ \ldots,\ \psi_n)$$

qui est entièrement équivalent au système donné, n'a point de facteurs doubles pour t indéterminée; nous pouvons donc toujours remplacer t par une quantité a telle que

$$\Phi(z;\ a,\ \psi_1,\ \psi_2,\ \ldots,\ \psi_n)$$

n'ait point de facteurs doubles. Décomposons cette fonction entière de z en ses facteurs irréductibles, dans le domaine naturel de rationalité $(\mathfrak{R}'', \mathfrak{R}''', \ldots, \mathfrak{R}^{(\nu)})$ et soit

$$\Phi(z) = V_1(z)V_2(z)\ \ldots\ V_\nu(z).$$

Comme $\Phi(z)$ est congru à zéro suivant le système de modules $[F(z),\ \Psi]$ nous avons manifestement l'équivalence

$$[F(z),\ \Psi] \sim [F(z),\ \Psi,\ \prod_{k=1}^{\nu} V_k(z)].$$

D'autre part, si nous composons les deux systèmes

$$[F(z),\ \Psi,\ \prod_{k=1}^{\nu-1} V_k(z)] \quad \text{et} \quad [F(z),\ \Psi,\ V_\nu(z)]$$

il vient

$$[F(z),\ \Psi,\ \prod_{k=1}^{\nu-1} V_k(z)][F(z),\ \Psi,\ V_\nu(z)]$$

$$\sim [F(z),\ \Psi,\ F(z)\prod_{k=1}^{\nu-1} V_k(z),\ \Psi\prod_{k=1}^{\nu-1} V_k(z),\ F(z)V_\nu(z),\ \Psi V_\nu(z),\ \Psi F(z),\ \Phi(z)]$$

ou, comme

$$(V_i,\ V_k) \sim 1 \qquad (i, k = 1, 2, \ldots, \nu;\ i \gtrless k)$$

$$[F(z),\ \Psi,\ \prod_{k=1}^{\nu=1} V_k(z)][F(z),\ \Psi,\ V_\nu(z)] \sim [F(z),\ \Psi,\ \Phi(z)].$$

---

(1) Cette dernière partie de la démonstration a été donnée par M. KRONECKER dans son Cours de 1883.

Ainsi nous avons démontré l'équivalence

$$[F(z),\ \Psi] \sim [F(z),\ \Psi,\ \prod_{k=1}^{\nu-1} V_k(z)][F(z),\ \Psi,\ V_\nu(z)]$$

en isolant, en quelque sorte, le facteur $V_\nu(z)$ des autres facteurs irréductibles de $\Phi(z)$.

Nous obtenons de même

$$[F(z),\ \Psi,\ \prod_{k=1}^{\nu-1} V_k(z)] \sim [F(z),\ \Psi,\ \prod_{k=1}^{\nu-2} V_k(z)][F(z),\ \Psi,\ V_{\nu-1}(z)]$$

en isolant le facteur $V_{\nu-1}(z)$, et en répétant la même opération ν fois, nous avons enfin

$$[F(z),\ \Psi] \sim \prod_{k=1}^{\nu} [F(z),\ \Psi,\ V_k(z)].$$

Formons maintenant le plus grand commun diviseur, suivant le module Ψ, des deux fonctions $F(z)$ et $V_k(z)$. D'après ce que nous avons montré dans le paragraphe précédent nous aurons à la fois, en désignant par $D_k(z)$ ce plus grand commun diviseur, les trois congruences,

$$D_k(z) \equiv 0 \ [\mathrm{modd}\, F(z),\ V_k(z),\ \Psi]$$

$$V_k(z) \equiv 0 \ [\mathrm{modd}\, \Psi,\ D_k(z)]$$

$$F(z) \equiv 0 \ [\mathrm{modd}\, \Psi,\ D_k(z)]$$

d'où il résulte que l'équivalence

$$[\Psi,\ D_k(z)] \sim [F(z),\ V_k(z),\ \Psi]$$

est vérifiée. Mais nous venons de voir que

$$[F(z),\ \Psi] \sim \prod_{k=1}^{\nu} [F(z),\ V_k(z),\ \Psi];$$

donc nous avons démontré l'équivalence

$$[F(z),\ \Psi] \sim \prod_{k=1}^{\nu} [\Psi,\ D_k(z)].$$

Les fonctions entières $D_k(z)$ sont premières entre elles; car si $D_h(z)$ et $D_k(z)$ avaient un diviseur commun, il en serait de même de $V_h(z)$ et $V_k(z)$ contrairement à l'hypothèse. En effectuant la composition indiquée dans le terme de droite de l'équivalence précédente, et en tenant compte de la relation

$$[D_i(z),\ D_k(z)] \sim 1 \qquad (i, k = 1, 2, \ldots, \nu;\ i \gtrless k)$$

nous avons successivement

$$[\Psi, D_1(z)][\Psi, D_2(z)] \sim [\Psi, \Psi D_1(z), \Psi D_2(z), D_1(z) D_2(z)] \sim [\Psi, D_1(z) D_2(z)]$$

$$[\Psi, D_1(z) D_2(z)][\Psi, D_3(z)] \sim [\Psi, \Psi D_1(z) D_2(z), \Psi D_3(z), D_1(z) D_2(z) D_3(z)]$$
$$\sim [\Psi, D_1(z) D_2(z) D_3(z)]$$

. . . . . .

$$[\Psi, \prod_{k=1}^{\nu-1} D_k(z)][\Psi, D_\nu(z)] \sim [\Psi, \Psi \prod_{k=1}^{\nu-1} D_k(z), \Psi D_\nu(z), \prod_{k=1}^{\nu} D_k(z)] \sim [\Psi, \prod_{k=1}^{\nu} D_k(z)]$$

ce qui nous donne

$$\prod_{k=1}^{\nu} [\Psi, D_k(z)] \sim [\Psi, \prod_{k=1}^{\nu} D_k(z)]$$

et, par suite,

$$[\Psi, \prod_{k=1}^{\nu} D_k(z)] \sim [F(z), \Psi].$$

Nous avons ainsi trouvé la décomposition du système donné $[F(z), \Psi]$. Il est facile d'en déduire celle de la fonction $F(z)$ dans le domaine général de rationalité considéré. En effet, de l'équivalence précédente nous déduisons la congruence

$$F(z) \equiv 0 \ [\mathrm{modd}\ \Psi, \prod_{k=1}^{\nu} D_k(z)]$$

ou encore l'égalité

$$F(z) = P(z)\Psi + Q(z) \prod_{k=1}^{\nu} D_k(z).$$

Mais $\Psi(\mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)}) = 0$ caractérise notre domaine général de rationalité. Nous avons donc, dans ce domaine,

$$F(z) = Q(z)\prod_{k=1}^{\nu} D_k(z).$$

D'autre part, le produit $\prod_{k=1}^{\nu} D_k$ est congru à zéro suivant le système de modules $[F(z), \Psi]$; comme $\Psi = 0$, il en résulte l'égalité

$$\prod_{k=1}^{\nu} D_k(z) = q(z)F(z).$$

Ainsi $Q(z)q(z) = 1$; $Q(z)$ et $q(z)$ sont donc indépendants de z, et comme le coefficient de la plus haute puissance de z, dans $F(z)$, est supposé égal à l'unité, $Q = 1$. Chacune des fonctions $D_k(z)$ est d'ailleurs irréductible dans le domaine considéré; en effet si nous avions

$$D_k(z) \equiv \eta_k(z)\zeta_k(z) \pmod{\Psi}$$

comme

$$V_k(z) \equiv 0 \ [\text{modd } \Psi, \ D_k(z)]$$

il en résulterait

$$V_k(z) \equiv a_k(z)\eta_k(z)\zeta_k(z) \pmod{\Psi}$$

et la fonction $V_k(z)$ serait elle-même réductible, contrairement à l'hypothèse.

Le problème proposé est ainsi résolu sans l'emploi des nombres et fonctions algébriques.

Chapitre IV.

Décomposition des systèmes de diviseurs.

§ 1.

Cas particulier de deux variables.

1. Nous venons de voir comment, dans un cas très-particulier, on peut décomposer les systèmes de diviseurs en systèmes plus simples. Nous

allons maintenant chercher à étudier la décomposition des systèmes de diviseurs dans le cas général. A cet effet, et pour nous rendre compte de la méthode à suivre, nous commencerons par considérer le cas le plus simple, celui d'un système de deux fonctions de deux variables.

Soient donc $F(x, y)$ et $G(x, y)$ deux fonctions entières des variables x et y dont les coefficients fassent partie d'un domaine de rationalité $(\Re, \Re', \ldots, \Re^{(n)})$. Si $F(x, y)$ et $G(x, y)$ ont un diviseur commun $H(x, y)$ et si $F(x, y) = H(x, y)\Phi(x, y)$; $G(x, y) = H(x, y)\Psi(x, y)$ nous pouvons remplacer le système $[F(x, y), G(x, y)]$ par le produit *équivalent* $H(x, y)[\Phi(x, y), \Psi(x, y)]$. Nous savons former le plus grand commun diviseur de deux fonctions entières; si donc $H(x, y)$ désigne le plus grand commun diviseur des deux fonctions $F(x, y)$ et $G(x, y)$, il ne nous reste plus qu'à décomposer un système dont les deux éléments n'ont aucun diviseur commun.

Remarquons que les systèmes (ξ, η) communs à $F(x, y) = 0$ et $G(x, y) = 0$, sont d'abord ceux pour lesquels la fonction $H(x, y)$ s'annule; ils forment une variété d'ordre un; ce sont ensuite ceux qui annulent à la fois $\Phi(x, y)$ et $\Psi(x, y)$; ils sont isolés. En déterminant le facteur $H(x, y)$ du système $[F(x, y), G(x, y)]$ nous avons donc déterminé la variété d'ordre un, commune aux deux fonctions $F(x, y)$ et $G(x, y)$ égalées à zéro; pour parvenir à une nouvelle décomposition du système considéré, il est donc naturel de commencer par chercher les systèmes isolés (ξ, η) communs aux deux fonctions $\Phi(x, y)$ et $\Psi(x, y)$ égalées à zéro. Je montrerai à la fin de ce paragraphe qu'en trouvant ces systèmes isolés on obtient vraiment une décomposition du système $[\Phi(x, y), \Psi(x, y)]$ en systèmes plus simples.

La première partie de cette recherche n'est pas nouvelle. Mais il me semble nécessaire de la donner ici en insistant sur les points susceptibles de généralisation afin de bien faire comprendre sur quoi repose la solution du problème dans le cas général que j'exposerai plus loin. Comme c'est ce cas général qui est l'objet de nos recherches, je laisserai, à dessein, de côté, tout ce qui ne s'y rapporte pas directement.

Pour trouver les solutions communes aux deux équations $\Phi(x, y) = 0$, $\Psi(x, y) = 0$ nous chercherons à transformer le système $(\Phi = 0, \Psi = 0)$ en un système entièrement équivalent ne contenant qu'une seule équation. S'il est possible d'effectuer cette transformation, le problème ne présentera

plus aucune difficulté, à condition que nous supposions connu le théorème de GAUSS sur la séparation des racines d'une équation algébrique.

Le problème ainsi posé, on est directement amené à reprendre les recherches que j'ai exposées, dans le chapitre premier de ce Mémoire, sur le résultant de deux fonctions entières. Comme, pour des valeurs indéterminées de y, $\Phi(x, y)$ et $\Psi(x, y)$ n'ont pas de diviseur commun, on sait que l'on peut trouver des fonctions entières de x et de y, Φ_1 et Ψ_1, vérifiant l'égalité

$$\Phi(x, y)\Psi_1(x, y) + \Psi(x, y)\Phi_1(x, y) = R_1(y),$$

dans laquelle le résultant $R_1(y)$ est une fonction entière de y qui n'a aucun diviseur commun avec Φ_1 et Ψ_1 et qui n'est pas identiquement nul en y.

Lorsque les coefficients des plus hautes puissances de x, dans Φ et Ψ ne dépendent pas de y, j'ai démontré que l'égalité $R_1(y) = 0$ est la condition nécessaire et suffisante pour que les deux fonctions Φ et Ψ aient un diviseur commun en x. Il n'en est pas de même lorsque, dans Φ ou Ψ, le coefficient de la plus haute puissance de x dépend de y; en effet, pour des valeurs particulières données à y, le degré de $\Psi(x, y)$ par exemple, par rapport à x, peut alors s'abaisser d'une unité; si donc $R_1(y) = 0$, c'est à dire, si

$$\Phi(x)\Psi_1(x) + \Psi(x)\Phi_1(x) = 0$$

on ne peut plus, en supposant l'existence des racines, conclure immédiatement que $\Phi(x)$ et $\Psi(x)$ ont un diviseur commun; car la relation

$$\Psi_1(x) \equiv 0 \ [\mathrm{mod}\ \Psi(x)]$$

qui était impossible dans le cas où le coefficient de la plus haute puissance de x, dans $\Psi(x)$ ne dépendait pas de y, est possible maintenant.

Ainsi pour pouvoir appliquer à des fonctions de deux variables le théorème fondamental sur leur résultant, il nous faut tout d'abord transformer ces fonctions en d'autres qui leur soient équivalentes et dont le degré par rapport à chacune des variables soit égal à la dimension.

Une simple transformation linéaire nous fournit ce résultat. Soit λ la dimension de $\Phi(x, y)$ et μ celle de $\Psi(x, y)$. Désignons par $\varphi_0(x, y)$ l'ensemble des termes de $\Phi(x, y)$ qui sont de dimension λ, et par

$\psi_0(x, y)$ l'ensemble des termes de $\Psi(x, y)$ qui sont de dimension μ. Si nous posons

$$x = \alpha x' + \beta y'$$
$$y = \gamma x' + \delta y',$$

comme une substitution linéaire des variables ne change pas la dimension d'une fonction de ces variables, les termes de plus haute dimension en x' et y' seront, après la substitution,

$$\varphi_0(\alpha x' + \beta y', \gamma x' + \delta y') = \varphi_0(\alpha, \gamma) x'^{\lambda} + \varphi_0(\beta, \delta) y'^{\lambda} + \ldots$$

et

$$\psi_0(\alpha x' + \beta y', \gamma x' + \delta y') = \psi_0(\alpha, \gamma) x'^{\mu} + \psi_0(\beta, \delta) y'^{\mu} + \ldots$$

Il suffit donc de choisir les systèmes de nombres (α, γ) et (β, δ) tels que φ_0 et ψ_0 soient différents de zéro lorsqu'on y remplace (x, y) par l'un et l'autre de ces systèmes, pour avoir transformé $\Phi(x, y)$ et $\Psi(x, y)$ en deux fonctions de x' et de y' dont le degré par rapport à chacune des variables est respectivement égal à λ et à μ. Ces fonctions égalées à zéro sont entièrement équivalentes à $\Phi(x, y) = 0$, $\Psi(x, y) = 0$. Ce n'est donc pas une restriction que de supposer que $\Phi(x, y)$ et $\Psi(x, y)$ sont déjà les fonctions transformées. Dans cette hypothèse nous pouvons appliquer le théorème fondamental sur le résultant de deux fonctions entières.

Formons d'abord le résultant, par rapport à x, des deux fonctions $\Phi(x, y)$ et $\Psi(x, y)$; soit

$$R_1(y) = \prod_{(k)} (y - y_k)$$

ce résultant. Les deux fonctions de x,

$$\Phi(x, y_k), \qquad \Psi(x, y_k)$$

ont, d'après ce que nous avons démontré, un diviseur commun; il y aura donc sûrement pour $y = y_k$, une valeur de x, $x = \xi$, pour laquelle les deux fonctions $\Phi(x, y)$ et $\Psi(x, y)$ s'annuleront simultanément. Inversement, si pour une valeur particulière de y, $y = \eta$, on peut trouver une valeur de x, $x = \xi$, telle que les deux égalités

$$\Phi(\xi, \eta) = 0, \qquad \Psi(\xi, \eta) = 0$$

soient vérifiées simultanément, $\Phi(x, y)$ et $\Psi(x, y)$ ont, pour $y = \eta$, un diviseur commun; le résultant de ces deux fonctions, par rapport à x, $R_1(y)$, s'annule donc pour $y = \eta$, ce qui montre que η est nécessairement égale à l'une des racines y_k de l'équation $R_1(y) = 0$.

Formons ensuite le résultant, par rapport à y, des deux fonctions $\Phi(x, y)$ et $\Psi(x, y)$; soit

$$R_2(x) = \prod_{(k)} (x - x_k)$$

ce résultant. Comme $R_2(x) = 0$ est la condition nécessaire et suffisante pour que $\Phi(x, y)$ et $\Psi(x, y)$, considérées comme des fonctions de y, aient un diviseur commun, il y aura sûrement, pour $x = x_k$, une valeur de y, $y = \eta$, pour laquelle $\Phi(x_k, y)$ et $\Psi(x_k, y)$ s'annuleront simultanément; et si pour $x = \xi$ on peut trouver une valeur de y, $y = \eta$, telle que les deux égalités

$$\Phi(\xi, \eta) = 0, \qquad \Psi(\xi, \eta) = 0$$

soient vérifiées simultanément, ξ sera nécessairement égale à l'une des racines x_k de l'équation $R_2(x) = 0$.

Le théorème fondamental sur le résultant de deux fonctions entières, appliqué aux deux fonctions $\Phi(x, y)$ et $\Psi(x, y)$ nous montre donc que les systèmes (ξ, η) pour lesquels on a simultanément

$$\Phi(\xi, \eta) = 0 \quad \text{et} \quad \Psi(\xi, \eta) = 0$$

sont tous compris parmi ceux que l'on peut former à l'aide des racines des deux équations

$$R_1(y) = 0 \quad \text{et} \quad R_2(x) = 0.$$

Mais nous ne voyons pas encore comment se groupent les racines de ces deux équations, pour former les systèmes (ξ, η). C'est pourquoi nous introduisons dans nos recherches une quantité *indéterminée* u.

Posons

$$z = ux + y$$

ou encore, pour conserver la symétrie entre x et y

$$z = ux + vy; \qquad v = 1$$

et

$$\Phi(x,\ z - ux) = \varphi(x,\ z,\ u)$$
$$\Psi(x,\ z - ux) = \psi(x,\ z,\ u).$$

Dans les deux fonctions de x et de z, φ et ψ, le coefficient de la plus haute puissance de z, ne dépend, comme dans Φ et Ψ, que des éléments du domaine de rationalité, et le coefficient de la plus haute puissance de x que de ces mêmes éléments et de l'indéterminée u; ils ne peuvent donc jamais s'annuler pour des valeurs particulières données aux variables x ou z, ce qui nous permet d'appliquer au système

$$\varphi(x,\ z,\ u) = 0, \qquad \psi(x,\ z,\ u) = 0$$

le même raisonnement que tout à l'heure. Formons donc le résultant, par rapport à x des deux fonctions φ et ψ, et désignons par

$$R(z,\ u) = c \prod_{(k)} (z - \zeta_k)$$

ce résultant, divisé, s'il y a lieu, par une fonction entière de u, afin que le coefficient de la plus haute puissance de z ne dépende plus que des éléments du domaine de rationalité. Nous pouvons alors toujours déterminer une valeur de x, $x = \xi'$, telle que

$$\varphi(\xi',\ \zeta_k) = 0 \quad \text{et} \quad \psi(\xi',\ \zeta_k) = 0.$$

Comme inversement, toutes les valeurs de z pour lesquelles φ et ψ s'annulent simultanément, sont racines de l'équation $R(z) = 0$, nous voyons également que

$$x = \xi' \quad \text{et} \quad u\xi' + vy = \zeta_k$$

représentent *tous* les systèmes vérifiant les deux équations

$$\varphi(x,\ ux + vy) = 0 \quad \text{et} \quad \psi(x,\ ux + vy) = 0$$

ou encore que

$$x = \xi' \quad \text{et} \quad y = \zeta_k - u\xi'$$

représentent *tous* les systèmes vérifiant les deux équations

$$\Phi(x,\ y) = 0 \quad \text{et} \quad \Psi(x,\ y) = 0.$$

Mais nous avons vu tout à l'heure que tous ces systèmes sont compris parmi les combinaisons des racines ξ_k et η_k de $R_2(x) = 0$ et de $R_1(y) = 0$. Donc

$$\xi' = \xi_k \quad \text{et} \quad \zeta - u\xi' = \eta_k$$

c'est à dire

$$\zeta = u\xi_k + v\eta_k.$$

Ainsi chaque racine du résultant $R(z)$ égalé à zéro est une fonction linéaire et homogène des racines des résultants des deux fonctions considérées, par rapport à x et à y, et nous pouvons écrire

$$R(z) = \prod_{(k)} (z - u\xi_k - v\eta_k).$$

L'équation $R(z) = 0$ est entièrement équivalente au système

$$[\Phi(x, y) = 0, \quad \Psi(x, y) = 0]$$

car à tout système vérifiant simultanément les deux équations $\Phi = 0$ et $\Psi = 0$ correspond une racine de l'équation $R(z) = 0$, et inversement à toute racine $u\xi_k + v\eta_k$ de l'équation $R(z) = 0$, correspond un système (ξ_k, η_k) tel que

$$\Phi(\xi_k, \eta_k) = 0 \quad \text{et} \quad \Psi(\xi_k, \eta_k) = 0.$$

C'est pourquoi nous dirons que $R(z) = 0$ est *l'équation résolvante* et $R(z)$ *le résolvant* du système $[\Phi(x, y), \Psi(x, y)]$.

Comme

$$R(z) = \prod_{(k)} (z - u\xi_k - v\eta_k) = \prod_{(k)} [u(x - \xi_k) + v(y - \eta_k)]$$

il suffit, pour obtenir les systèmes cherchés (ξ_k, η_k) de décomposer la fonction homogène de u et de v, $R(ux + vy)$ en ses facteurs linéaires,

$$u(x - \xi_k) + v(y - \eta_k).$$

Chacun de ces facteurs linéaires, égalé à zéro, nous donne un des systèmes cherchés; car u étant indéterminée, de l'égalité

$$u(x - \xi_k) + v(y - \eta_k) = 0$$

on déduit

$$x = \xi_k; \qquad y = \eta_k.$$

La différence essentielle entre R et la fonction V de GALOIS consiste en ce que dans R, u désigne une indéterminée, tandis que dans V, u et v sont remplacés par des nombres entiers. Cette différence est très-importante, comme nous nous en apercevrons peu à peu dans la suite de nos recherches.

Dès maintenant nous voyons que la méthode précédente a l'avantage de nous donner *simultanément* les deux éléments ξ, η d'un même système, et c'est à l'emploi de l'indéterminée u que nous devons ce résultat.

POISSON fait déjà usage des indéterminées et obtient le même résultat; mais là s'arrête l'analogie de sa méthode et de celle de M. KRONECKER. Il me semble que POISSON considère les indéterminées plutôt comme des auxiliaires commodes pour le *calcul,* tandis que M. KRONECKER s'en sert surtout pour pénétrer plus avant dans la nature des systèmes vérifiant les équations données. Déjà la recherche sur la décomposition des systèmes que nous allons aborder à l'instant, indiquera clairement l'importance théorique des indéterminées en Algèbre.

L'équivalence

$$[\Phi(x, y) = 0, \quad \Psi(x, y) = 0] \sim [R(z) = 0]$$

suppose expressément u indéterminée. Mais si, faisant pour un instant abstraction de cette équivalence, nous nous proposons simplement de trouver les systèmes (ξ, η) vérifiant à la fois les deux équations

$$\Phi(x, y) = 0 \quad \text{et} \quad \Psi(x, y) = 0$$

il nous suffira de remplacer u et v par des quantités variables, et alors nous pourrons toujours, comme nous l'avons fait voir dans le second chapitre de ce Mémoire, donner à ces variables des valeurs a et b, telles que ξ et η soient fonctions rationnelles de $a\xi + b\eta$. A la recherche des deux genres ξ et η est alors substituée, comme chez GALOIS, celle du genre unique qui les contient tous deux. Nous rencontrons ici le genre de la méthode qui permet de donner une figuration bien simple d'un système d'équations à un nombre quelconque d'inconnues.

2. Nous venons de parler de l'équivalence des systèmes d'équations $[\Phi(x, y) = 0, \ \Psi(x, y) = 0]$ et $[R(z) = 0]$, équivalence qui est le théorème fondamental de la théorie de l'élimination, dans le cas de deux fonctions

de deux variables. Il nous faut maintenant rechercher si à cette équivalence correspond une équivalence entre le système

$$[\Phi(x, y), \quad \Psi(x, y)],$$

qui est à proprement parler l'objet de nos recherches, et son résolvant $R(ux + vy)$, et si cette équivalence répond à la définition algébrique que j'ai donnée dans le chapitre précédent, où deux systèmes étaient dits équivalents lorsque chacun d'eux contenait l'autre dans le sens plus général de contenant et de contenu introduit en Algèbre par M. KRONECKER.

Comme l'équation $R(ux + vy) = 0$ n'est la résolvante du système donné que si u est indéterminée, elle représente non pas une équation entre x et y, mais plusieurs. Si, en effet,

$$R(ux + y) = \sum_{k=0}^{m} r_k(x, y) u^k$$

nous aurons à la fois, précisément parce que u est indéterminée,

$$r_0(x, y) = 0, \quad r_1(x, y) = 0, \quad \ldots, \quad r_m(x, y) = 0$$

et le nombre de ces équations peut être fort grand. C'est ce système d'équations qui, en réalité, est équivalent au système

$$[\Phi(x, y) = 0, \quad \Psi(x, y) = 0];$$

nous l'avons seulement *condensé* en une seule équation, à l'aide de l'indéterminée u, afin d'obtenir simultanément les valeurs correspondantes ξ et η; mais dans des recherches d'équivalences il nous faut revenir aux équations qui lient les variables x et y indépendamment de l'indéterminée u; nous comparerons donc les deux systèmes

$$[\Phi(x, y); \ \Psi(x, y)] \quad \text{et} \quad [r_0(x, y), r_1(x, y), \ldots, r_m(x, y)].$$

Le résultant $R(z)$ est une fonction linéaire et homogène des deux fonctions $\varphi(x, z)$ et $\psi(x, z)$, c'est à dire des deux fonctions $\Phi(x, y)$ et $\Psi(x, y)$ et les coefficients de cette fonction linéaire et homogène sont des fonctions entières de x et de z. Ils sont seulement rationnels en u; mais après avoir multiplié par une fonction entière convenable de u, l'expression $R(z)$ et la fonction linéaire et homogène qui la représente, on peut com-

parer les coefficients des puissances correspondantes de u; on obtient alors, pour $k = 0, 1, 2, \ldots, m$,

$$r_k(x, y) \equiv 0 \ [\text{modd } \Phi(x, y), \ \Psi(x, y)]$$

ce qui démontre la congruence

$$[r_0(x, y), r_1(x, y), \ldots, r_m(x, y)] \equiv 0 \ [\text{modd } \Phi(x, y), \ \Psi(x, y)].$$

Ainsi le système donné est contenu dans le système des coefficients du résolvant. Il s'agit maintenant de vérifier si, inversement, le système des coefficients du résolvant est contenu dans le système donné.

Une restriction est ici nécessaire. Nous savons que la fonction $\Phi(x, y)$ s'annule pour les systèmes (ξ, η) vérifiant simultanément les équations $r_0(x, y) = 0, r_1(x, y) = 0, \ldots, r_m(x, y) = 0$. Ce que nous voulons démontrer revient donc à généraliser la proposition élémentaire qu'une fonction $\Phi(x)$ qui s'annule pour toutes les racines d'une équation $r(x) = 0$, est divisible par $r(x)$. Mais cette proposition élémentaire suppose déjà que toutes les racines de l'équation $r(x) = 0$ soient inégales; il est donc naturel de faire la même restriction dans le cas des fonctions de deux variables et de supposer que tous les systèmes (ξ, η) soient inégaux, c'est à dire que l'équation résolvante $R(z) = 0$ n'ait point de racines multiples.

C'est seulement sous cette hypothèse que je résoudrai complètement le problème proposé. Elle revient à supposer l'inégalité

$$\prod_{(i)} \Delta(\xi_i, \eta_i) \gtrless 0,$$

où $\Delta(x, y)$ désigne le déterminant fonctionnel des deux fonctions $\Phi(x, y)$ et $\Psi(x, y)$, et où le produit est étendu à tous les systèmes (ξ, η) communs à ces deux fonctions; mais comme dans ce qui va suivre je ne fais pas usage de ce théorème, j'en renverrai la démonstration à une autre occasion.

Je démontrerai, par contre, par une méthode qui sera applicable à un système de fonctions contenant un nombre quelconque de variables, que toutes les fonctions

$$r_0(x, y), \ r_1(x, y), \ \ldots, \ r_m(x, y)$$

n'ont pas de diviseur commun. Je formerai, à cet effet, les deux expressions

$$H(x, y) = \sum_{k=0}^{m} r_k(x, y)U_k \quad \text{et} \quad K(x, y) = \sum_{k=0}^{m} r_k(x, y)V_k$$

où $U_0, U_1, \ldots, U_m$ et $V_0, V_1, \ldots, V_m$ sont de nouvelles indéterminées et je montrerai d'abord que de l'hypothèse que nous venons de faire on déduit l'inégalité

$$\prod_{(i)} \Gamma(\xi_i, \eta_i) \gtrless 0$$

où $\Gamma(x, y)$ désigne le déterminant fonctionnel des deux fonctions $H(x, y)$ et $K(x, y)$ et où le produit est étendu à toutes les racines du résolvant $R(z)$ égalé à zéro.

Dans ce but, il suffit de remarquer qu'en désignant par u et u_1 deux indéterminées différentes, les fonctions

$$H(x, y) = \sum_{(k)} r_k(x, y)U_k \quad \text{et} \quad K(x, y) = \sum_{(k)} r_k(x, y)V_k$$

se transforment en

$$R(ux + y) = \sum_{(k)} r_k(x, y)u^k \quad \text{et} \quad R(u_1x + y) = \sum_{(k)} r_k(x, y)u_1^k$$

par une substitution qui spécialise les indéterminées U et V.

Si donc le déterminant fonctionnel

$$\Gamma(x, y) = \begin{vmatrix} D_xH(x, y), & D_yH(x, y) \\ D_xK(x, y), & D_yK(x, y) \end{vmatrix}$$

était nul, pour un des systèmes (ξ, η) considérés, il faudrait que pour ce même système, le déterminant

$$\begin{vmatrix} D_xR(ux + y), & D_yR(ux + y) \\ D_xR(u_1x + y), & D_yR(u_1x + y) \end{vmatrix}$$

fût également nul. Mais, si $z_1 = u_1x + y$,

$$D_xR(ux + y) = uD_zR(z); \quad D_yR(ux + y) = D_zR(z)$$

$$D_xR(u_1x + y) = u_1D_{z_1}R(z_1); \quad D_yR(u_1x + y) = D_{z_1}R(z_1).$$

Nous aurions donc aussi l'égalité

$$(u - u_1) D_z R(z) D_{z_1} R(z_1) = 0$$

c'est à dire, ou bien $D_z R(z) = 0$, ou bien $D_{z_1} R(z_1) = 0$, pour un système (ξ, η) qui annule le résolvant $R(z)$ et pour lequel nous avons à la fois $R(ux + y) = 0$ et $R(u_1 x + y) = 0$. Ce résultat est contraire à l'hypothèse d'après laquelle $R(z)$ n'a point de facteurs multiples. Il est donc impossible que le produit

$$\prod_{(i)} I'(\xi_i, \eta_i)$$

soit nul.

Mais alors il est également impossible que toutes les fonctions $r_0(x, y)$, $r_1(x, y)$, ..., $r_m(x, y)$ aient un diviseur commun; car si elles avaient un diviseur commun $P(x, y)$, $P(x, y)$ serait aussi diviseur de $H(x, y)$ et de $K(x, y)$; les deux fonctions $H(x, y)$ et $K(x, y)$ s'annuleraient donc pour l'un des systèmes (ξ, η), et nous aurions pour ce système

$$I'(\xi, \eta) = 0$$

contrairement à ce que je viens de démontrer.

D'autre part, comme par hypothèse le résolvant $R(z)$ n'a pas de facteurs multiples et que $D_x R(ux + y) = u D_z R(z)$, les deux fonctions

$$\sum_{(k)} r_k(x, y) u^k \quad \text{et} \quad \sum_{(k)} D_x r_k(x, y) u^k$$

n'ont pas de diviseur commun, pour des valeurs indéterminées de y. On voit donc que $K(x, y)$ et sa dérivée par rapport à x ne peuvent avoir de diviseur commun tant que y reste indéterminée.

Ainsi de l'hypothèse que $R(z)$ n'a pas de facteurs multiples, résultent les deux équivalences

$$[H(x, y), K(x, y)] \sim 1$$

et

$$[K(x, y), D_x K(x, y)] \sim 1$$

relativement à x, pour y indéterminée.

Ceci posé, je vais chercher à vérifier la congruence

$$\Phi(x, y) \equiv 0 \ [\mathrm{modd}\, r_0(x, y), r_1(x, y), \ldots, r_m(x, y)].$$

A cet effet il est nécessaire de déterminer des multiplicateurs $q_0(x, y)$, $q_1(x, y)$, $\ldots$, $q_m(x, y)$, fonctions *entières* de x et de y, et tels que $\Phi(x, y)$ soit égal à

$$q_0(x, y)r_0(x, y) + q_1(x, y)r_1(x, y) + \ldots + q_m(x, y)r_m(x, y).$$

Ce problème serait résolu si nous pouvions déterminer des fonctions *entières* de x et de y, $\alpha(x, y)$ et $\beta(x, y)$ telles que

$$\Phi(x, y) = \alpha(x, y)H(x, y) + \beta(x, y)K(x, y)$$

c'est à dire, si nous pouvions déterminer une seule fonction *entière* de x et de y, $\alpha(x, y)$, telle que

$$\Phi(x, y) \equiv \alpha(x, y)H(x, y) \ [\mathrm{mod}\, K(x, y)].$$

La formule de LAGRANGE nous donne immédiatement une fonction rationnelle de x et de y, entière en x,

$$\alpha(x, y) = \sum_{(i)} \frac{\Phi(x_i, y)}{H(x_i, y)} \frac{K(x, y)}{x - x_i} \frac{1}{D_x K(x, y)_{x=x_i}}$$

vérifiant cette congruence; la somme est étendue à toutes les racines x_i du polynôme $K(x, y)$ considéré comme une fonction de x seulement et égalé à zéro. Si la fonction rationnelle $\alpha(x, y)$ est aussi *entière* en y, le problème est résolu; il s'agit donc simplement de voir quand cette expression se présente sous une forme illusoire. Dans ce but nous rechercherons les valeurs des variables qui annulent son dénominateur.

Et d'abord les deux dernières équivalences nous montrent que pour y indéterminée, $H(x_i, y)$ et $D_x K(x, y)_{x=x_i}$ sont nécessairement différents de zéro.

De plus, si nous donnons à y, une valeur y_0 indépendante des indéterminées U et V, et telle que $H(x_i, y_0)$ soit nulle, nous aurons à la fois

$$H(x_i, y_0) = 0 \quad \text{et} \quad K(x_i, y_0) = 0.$$

Mais alors le système (x_i, y_0) annule simultanément toutes les fonctions $r_h(x, y)$, $(h = 0, 1, \ldots, m)$; il est donc identique à l'un des systèmes (ξ, η) considérés, et comme pour chacun de ces systèmes on a $\Phi(\xi, \eta) = 0$, notre expression se présente sous une forme indéterminée. En tenant compte de l'égalité $K(x_i, y) = 0$, on trouve facilement, par le procédé bien connu de différentiation du numérateur et du dénominateur, la vraie valeur de la fraction $\frac{\Phi(\xi_i, \eta_i)}{H(\xi_i, \eta_i)}$. Elle est égale à

$$\left[\frac{D_y\Phi(x, y)D_xK(x, y) - D_x\Phi(x, y)D_yK(x, y)}{D_yH(x, y)D_xK(x, y) - D_xH(x, y)D_yK(x, y)}\right]_{\substack{x=\xi_i \\ y=\eta_i}}.$$

Le dénominateur est égal, au signe près, à $I'(\xi_i, \eta_i)$; il est donc différent de zéro et la vraie valeur de la fraction

$$\frac{\Phi(\xi_i, \eta_i)}{H(\xi_i, \eta_i)}$$

est finie et déterminée.

Si donc, en s'annulant, la fonction de y,

$$T(y, U, V) = \prod_{(h)} H(x_k, y)$$

rend illusoire l'expression du multiplicateur $\alpha(x, y)$ donnée par la formule de LAGRANGE, ce ne peut être que pour des valeurs de y qui dépendent des indéterminées U et V. En d'autres termes, si nous déterminons le plus grand commun diviseur $A(y)$ des coefficients de la fonction $T(y, U, V)$ ordonnée par rapport aux indéterminées U et V, et que nous mettions $T(y, U, V)$ sous la forme

$$T(y, U, V) = A(y)E_1(y, U, V)$$

les racines de l'équation $A(y) = 0$ ne rendront pas infinie l'expression trouvée pour $\alpha(x, y)$.

Je rappelle qu'on entend par *forme primitive* d'un nombre quelconque d'indéterminées, une fonction entière de ces indéterminées dont les coefficients n'ont aucun diviseur commun. $E_1(y, U, V)$ est donc une forme primitive des indéterminées U et V

Il serait possible que pour une valeur déterminée de y, indépendante des indéterminées U et V, $y = y_1$, la fonction $K(x, y)$ et sa dérivée par rapport à x, aient un diviseur commun. L'expression trouvée pour $\alpha(x, y)$ se présenterait alors, pour $y = y_1$, sous une forme illusoire. Mais je vais montrer que si W désigne une indéterminée, il est impossible que la fonction

$$K(x, y_1) + WH(x, y_1)$$

et sa dérivée par rapport à x, aient un diviseur commun.

Et d'abord les deux fonctions de x, $H(x, y_1)$ et $K(x, y_1)$ ne peuvent avoir de diviseur commun. En effet, si la fonction $P(x, y_1)$ divisait à la fois $H(x, y_1)$ et $K(x, y_1)$ elle diviserait aussi $\Gamma(x, y_1)$. - Mais alors en déterminant x_1 par l'égalité $P(x_1, y_1) = 0$, nous aurions à la fois

$$H(x_1, y_1) = 0, \qquad K(x_1, y_1) = 0, \qquad \Gamma(x_1, y_1) = 0$$

ce qui est impossible, puisque des deux premières de ces égalités nous pouvons conclure que le système (x_1, y_1) est égal à l'un des systèmes (ξ, η), à condition toutefois que nous ne considérions que des valeurs y_1 indépendantes des indéterminées U et V.

Ceci posé, supposons que la fonction $K(x, y_1) + WH(x, y_1)$ et sa dérivée par rapport à x aient un diviseur commun, $L(x, y_1, W)$. Des deux égalités

$$K(x, y_1) + WH(x, y_1) = L(x, y_1, W)M(x, y_1, W)$$

et

$$D_x K(x, y_1) + WD_x H(x, y_1) = L(x, y_1, W)N(x, y_1, W)$$

on déduit immédiatement la relation

$$K(x, y_1)D_x H(x, y_1) - H(x, y_1)D_x K(x, y_1)$$
$$= L(x, y_1, W)[M(x, y_1, W)D_x H(x, y_1) - N(x, y_1, W)D_x K(x, y_1)]$$

dans laquelle la quantité entre parenthèses est différente de zéro. En effet, dans le cas contraire le terme de gauche serait égal à zéro, donc les deux fonctions de x, $H(x, y_1)$ et $K(x, y_1)$, auraient un diviseur commun, contrairement à ce que nous venons de démontrer. Mais alors, nous

pouvons déduire de l'égalité précédente que la fonction $L(x, y, W)$ est nécessairement contenue dans l'expression

$$K(x, y_1)D_xH(x, y_1) - H(x, y_1)D_xK(x, y_1);$$

elle est, par suite, indépendante de l'indéterminée W; donc, comme $K + WH = L.M$, elle est contenue à la fois dans $H(x, y_1)$ et dans $K(x, y_1)$. Mais nous avons vu plus haut que ces deux fonctions n'ont pas de diviseur commun; donc la fonction $K(x, y_1) + WH(x, y_1)$ et sa dérivée, par rapport à x, sont premières entre elles.

En appliquant aux deux fonctions de x,

$$K(x, y_1) + WH(x, y_1) \quad \text{et} \quad D_xK(x, y_1) + WD_xH(x, y_1)$$

le théorème fondamental sur le résultant de deux fonctions entières, on voit maintenant qu'il est possible de déterminer une constante C, telle que la fonction

$$K(x, y_1) + CH(x, y_1)$$

n'ait également aucun diviseur commun avec sa dérivée par rapport à x.

D'ailleurs les deux systèmes

$$[H(x, y), K(x, y)] \quad \text{et} \quad [H(x, y), K(x, y) + CH(x, y)]$$

sont entièrement équivalents.

Ainsi, après avoir transformé, si cela est nécessaire, le système proposé en un système équivalent convenable, en désignant encore par $H(x, y)$ et $K(x, y)$ les deux éléments de ce système, et par y_1 une valeur déterminée indépendante des indéterminées U et V, nous ne pouvons avoir simultanément les deux équations

$$K(x_k, y_1) = 0 \quad \text{et} \quad D_xK(x, y_1)_{x=x_k} = 0.$$

Comme la première de ces égalités est vérifiée, quelle que soit y, la seconde ne l'est jamais. En d'autres termes, le produit

$$\prod_{(k)} D_xK(x, y)_{x=x_k} = T_1(y, U, V)$$

est une forme primitive des indéterminées U et V.

En multipliant la fonction entière de x, $\alpha(x, y)$ par le produit $E(y, U, V)$ des deux formes primitives $E_1(y, U, V)$ et $T_1(y, U, V)$, nous obtenons donc une fonction *entière de x et de y*. Comme le produit de deux formes primitives est lui-même une forme primitive, la forme $E(y, U, V)$ est primitive.

Nous avons jusqu'ici, à l'aide de la formule de LAGRANGE, déterminé $\alpha(x, y)$ de manière que la fonction entière de x et de y ainsi que des indéterminées U et V

$$E(y)[\Phi(x, y) - \alpha(x, y)H(x, y)]$$

soit divisible par $K(x, y)$, considérée comme une fonction de x seulement; le quotient

$$\beta(x, y) = \frac{E(y)[\Phi(x, y) - \alpha(x, y)H(x, y)]}{K(x, y)}$$

est donc une fonction entière de x. Mais nous avons démontré que si le quotient de deux fonctions entières de plusieurs variables $x, y, z, \ldots$, est une fonction entière de x et si la fonction diviseur ne contient pas un facteur indépendant de x, ce même quotient est fonction entière de *toutes* les variables $x, y, z, \ldots$. La fonction entière $K(x, y)$ ne contient manifestement aucun facteur indépendant de x; donc $\beta(x, y)$ est une fonction entière de x *et* de y, ainsi que des indéterminées U et V, et nous pouvons écrire

$$E(y)\Phi(x, y) = [E(y)\alpha(x, y)]H(x, y) + \beta(x, y)K(x, y)$$

les coefficients de $H(x, y)$ et de $K(x, y)$ étant fonctions entières de x, de y et des indéterminées U et V.

Nous avons donc démontré, non pas que la fonction $\Phi(x, y)$ contient le système de modules

$$[H(x, y), K(x, y)],$$

mais seulement que le produit

$$E(y)\Phi(x, y)$$

de la fonction $\Phi(x, y)$ et d'une forme primitive $E(y)$, contient ce système de modules. Mais comme dans la forme primitive $E(y)$ ne paraît qu'une variable y, tout est bien simple maintenant.

En ordonnant par rapport aux indéterminées U et V les deux termes de l'égalité

$$E(y)\Phi(x, y) = E(y)\alpha(x, y)H(x, y) + \beta(x, y)K(x, y)$$

et en comparant les coefficients, nous obtenons un système d'équations

$$S^{(k)}(y)\Phi(x, y) = r_0(x, y)s_0^{(k)}(x, y) + r_1(x, y)s_1^{(k)}(x, y) + \ldots + r_m(x, y)s_m^{(k)}(x, y)$$

pour $k = 1, 2, 3, \ldots$. Comme la variable x ne paraît pas dans la forme $E(y)$, chacune des fonctions $S^{(k)}(y)$ ne contient qu'une seule variable; ces fonctions $S^{(k)}(y)$ n'ont d'ailleurs pas de diviseur commun puisque la forme $E(y)$ est *primitive;* nous pouvons donc déterminer des fonctions entières à coefficients rationnels $\sigma_k(y)$, telles que l'égalité

$$\sum_{(k)} \sigma_k(y) S^{(k)}(y) = 1$$

soit vérifiée. En multipliant chacune des équations précédentes par la fonction $\sigma_k(y)$ correspondante et en ajoutant les différentes équations ainsi obtenues nous avons donc enfin

$$\Phi(x, y) \equiv 0 \ [\mathrm{modd}\, r_0(x, y), r_1(x, y), \ldots, r_m(x, y)].$$

L'on obtient, tout à fait de même, la seconde congruence

$$\Psi(x, y) \equiv 0 \ [\mathrm{modd}\, r_0(x, y), r_1(x, y), \ldots, r_m(x, y)].$$

Mais alors on peut écrire

$$[\Phi(x, y), \Psi(x, y)] \equiv 0 \ [\mathrm{modd}\, r_0(x, y), r_1(x, y), \ldots, r_m(x, y)].$$

Il suffit de joindre à ce résultat, celui que nous avons obtenu plus haut, pour avoir démontré l'équivalence

$$[\Phi(x, y), \Psi(x, y)] \sim [r_0(x, y), r_1(x, y), \ldots, r_m(x, y)].$$

L'équivalence d'un système de deux fonctions de deux variables et du système formé à l'aide des coefficients de son résolvant ordonné par rapport aux indéterminées qui y paraissent est donc bien de celles que nous avons définies dans le chapitre précédent.

Comme

$$R(ux + y) = \sum_{(k)} r_k(x, y)u^k$$

quelle que soit l'indéterminée u, nous pouvons en considérant successivement plusieurs indéterminées différentes u, u_1, ..., représenter chacune des fonctions $r_k(x, y)$ par une fonction linéaire de $R(ux+y)$, $R(u_1x+y)$,.... Il est bon de remarquer que les coefficients de ces fonctions R sont, en général, fonctions *rationnelles* des indéterminées u, u_1, ... La fonction $R(ux + y)$ prise un certain nombre de fois et pour des indéterminées différentes, et le système $[r_0(x, y), r_1(x, y), \ldots, r_m(x, y)]$ sont donc équivalents. C'est pourquoi nous pouvons dire que l'équivalence démontrée

$$[\Phi(x, y), \Psi(x, y)] \sim [r_0(x, y), r_1(x, y), \ldots, r_m(x, y)]$$

indique aussi qu'à l'aide des indéterminées u, la fonction $R(z)$ remplace entièrement le système donné $[\Phi(x, y), \Psi(x, y)]$.

3. Il nous faut maintenant faire les mêmes recherches dans le cas où l'on nous donné non pas deux, mais un nombre quelconque de fonctions de deux variables. En introduisant la notion de système de diviseurs j'ai déjà insisté sur ce que le nombre d'éléments de ces systèmes ne jouait qu'un rôle secondaire dans l'étude de leurs propriétés. Pour légitimer cette remarque, j'ai de suite montré que l'on peut augmenter à volonté le nombre des éléments d'un système sans rien changer à sa signification. La méthode que je vais suivre pour transformer un système composé d'un nombre quelconque d'éléments et qui est toute semblable à celle que j'ai suivie lorsque le système n'était composé que de deux éléments seulement, vérifie entièrement cette remarque dans le cas de deux variables.

Soient $A_1(x, y)$, $A_2(x, y)$, ..., $A_\mu(x, y)$, μ fonctions entières de x et de y, que nous pouvons supposer sans diviseur commun dans le domaine de rationalité considéré, puisque nous connaissons une méthode pour déterminer le plus grand commun diviseur d'un nombre quelconque de fonctions entières dans un domaine général de rationalité. Nous cherchons s'il est possible de décomposer le système

$$[A_1(x, y), A_2(x, y), \ldots, A_n(x, y)]$$

en systèmes plus simples. Relions, à cet effet, les éléments $A_1, A_2, \ldots, A_\mu$ par deux systèmes d'indéterminées $U_1, U_2, \ldots, U_\mu$ et $V_1, V_2, \ldots, V_\mu$ et formons le résolvant des deux fonctions

$$\sum_{i=1}^{\mu} U_i A_i(x, y) \quad \text{et} \quad \sum_{i=1}^{\mu} V_i A_i(x, y);$$

ce résolvant sera fonction entière de $z = ux + vy$ et des indéterminées U et V; désignons-le par

$$S(z, U, V)$$

et soit $R(z)$ le plus grand commun diviseur des coefficients de S considérée comme une fonction des indéterminées U et V seulement; nous pourrons alors écrire

$$S(z, U, V) = R(z) E(z, U, V)$$

et $E(z, U, V)$ sera une forme primitive des indéterminées U et V.

Ceci posé, supposons que pour un système (ξ, η), les fonctions $A_1(x, y), A_2(x, y), \ldots, A_\mu(x, y)$ s'annulent simultanément; alors les deux sommes

$$\sum_{(i)} U_i A_i(\xi, \eta) \text{ et } \sum_{(i)} V_i A_i(\xi, \eta) \qquad (i = 1, 2, \ldots, \mu)$$

seront également nulles, et nous aurons, par suite, d'après ce que nous avons démontré sur le résolvant de deux fonctions entières

$$S(u\xi + v\eta, U, V) = 0.$$

Mais, pour une valeur de z indépendante des indéterminées U et V, la fonction $S(z, U, V)$ ne peut s'annuler que si $R(z)$ s'annule. Si donc nous avons simultanément

$$A_1(\xi, \eta) = 0, \; A_2(\xi, \eta) = 0, \; \ldots, \; A_\mu(\xi, \eta) = 0,$$

nous avons aussi

$$R(u\xi + v\eta) = 0.$$

Inversement, comme chaque racine $\zeta = u\xi + v\eta$ de l'équation $R(z) = 0$

vérifie l'équation $S(z, U, V) = 0$, nous aurons à la fois, d'après ce que nous avons démontré sur le résolvant de deux fonctions entières,

$$\sum_{(i)} U_i A_i(x, y) = 0 \text{ et } \sum_{(i)} V_i A_i(x, y) = 0 \qquad (i = 1, 2, \ldots, \mu)$$

pour $x = \xi$ et $y = \eta$; mais de ces deux équations résultent immédiatement les suivantes

$$A_1(\xi, \eta) = 0, \; A_2(\xi, \eta) = 0, \; \ldots, \; A_\mu(\xi, \eta) = 0.$$

Ainsi la fonction $R(z)$ joue, dans le cas général que nous considérons, le même rôle que le résolvant dans le cas particulier de deux fonctions entières seulement. C'est pourquoi nous dirons que $R(z)$, le plus grand commun diviseur des coefficients de la forme $S(z, U, V)$, est le *résolvant* du système

$$[A_1(x, y), \; A_2(x, y), \; \ldots, \; A_\mu(x, y)].$$

Nous allons montrer que tout système est équivalent à son résolvant.

Et d'abord $R(z)$ contient le système $[A_1(x, y), A_2(x, y), \ldots, A_\mu(x, y)]$. Nous obtenons, en effet, le résolvant $S(z, U, V)$ des deux fonctions entières

$$\sum_{(i)} U_i A_i(x, y) \text{ et } \sum_{(i)} V_i A_i(x, y) \qquad (i = 1, 2, \ldots, \mu)$$

en formant le résultant, par rapport à x, des deux fonctions

$$\sum_{(i)} U_i A_i(x, z - ux) \text{ et } \sum_{(i)} V_i A_i(x, z - ux); \qquad (i = 1, 2, \ldots, \mu)$$

il en résulte que $S(z, U, V)$ est une fonction linéaire et homogène des deux fonctions entières de x, de y et des U, V,

$$\sum_{(i)} U_i A_i(x, y) \text{ et } \sum_{(i)} V_i A_i(x, y) \qquad (i = 1, 2, \ldots, \mu)$$

dont les coefficients sont également fonctions entières de x, de y et des U, V. En ordonnant S, ainsi que cette fonction linéaire et homogène, par rapport aux indéterminées U et V, et en comparant les coefficients correspondants, nous aurons donc, si $S^{(k)}(z)$, $(k = 1, 2, \ldots, \tau)$ sont les coefficients de la forme primitive $E(z, U, V)$, une suite de congruences

$$R(z) S^{(k)}(z) \equiv 0 \; [\text{modd } A_1(x, y), \; A_2(x, y), \; \ldots, \; A_\mu(x, y)]$$

pour $k = 1, 2, \ldots, \tau$. Comme les fonctions $S^{(k)}(z)$ n'ont pas de diviseur commun et sont fonctions d'une seule variable, nous déduisons facilement de cette suite de congruences, celle que nous voulons démontrer

$$R(z) \equiv 0 \ [\text{modd } A_1(x, y), A_2(x, y), \ldots, A_\mu(x, y)].$$

Après avoir, dans les deux termes de l'égalité correspondante, chassé le dénominateur qui est une fonction entière de u, il vient en comparant les coefficients des puissances correspondantes de u et en posant

$$R(z) = \sum_{(i)} r_i(x, y) u^i \qquad (i = 0, 1, 2, \ldots, m)$$

$$r_i(x, y) \equiv 0 \ [\text{modd } A_1(x, y), A_2(x, y), \ldots, A_\mu(x, y)] \qquad (i = 0, 1, 2, \ldots, m)$$

et, par suite,

$$[r_0(x, y), r_1(x, y), r_2(x, y), \ldots, r_m(x, y)] \equiv 0$$
$$[\text{modd } A_1(x, y), A_2(x, y), \ldots, A_\mu(x, y)].$$

Cette dernière congruence ne contient plus aucune indéterminée.

Si, comme toujours, nous supposons que les racines du résolvant $R(z)$ ne soient pas multiples, chacun des éléments $A_i(x, y)$, $(i = 1, 2, \ldots, \mu)$ contient également le système $[r_0(x, y), r_1(x, y), \ldots, r_m(x, y)]$. Il suffit, pour s'en assurer, de démontrer que $A_i(x, y)$ contient le système

$$[\sum_{(i)} U_i r_i(x, y), \sum_{(i)} V_i r_i(x, y)]. \qquad (i = 0, 1, 2, \ldots, m)$$

Ici le raisonnement est identique à celui que nous avons fait pour démontrer la congruence

$$\Phi(x, y) \equiv 0 \ [\text{modd } H(x, y), K(x, y)].$$

A l'aide de la formule de LAGRANGE, on forme d'abord une fonction entière $E(y)\alpha(x, y)$ vérifiant la congruence

$$E(y) A_j(x, y) \equiv E(y)\alpha(x, y) \sum_{(i)} U_i r_i(x, y) \ [\text{mod} \sum_{(i)} V_i r_i(x, y)]$$

où $E(y)$ désigne une forme primitive des indéterminées U et V, dont

les coefficients ne dépendent que d'une seule variable; puis on en déduit, comme tout à l'heure, la congruence que nous voulons démontrer

$$A_j(x, y) \equiv 0 \,[\text{modd } r_0(x, y), r_1(x, y), \ldots, r_m(x, y)]$$

pour $j = 1, 2, \ldots, \mu$.

En joignant ce résultat à celui que nous avons obtenu à l'instant, nous pouvons écrire l'équivalence

$$[A_1(x, y), \ldots, A_\mu(x, y)] \sim [r_0(x, y), \ldots, r_m(x, y)].$$

Cette équivalence indique aussi, qu'à l'aide des indéterminées u, la fonction $R(z)$ remplace entièrement le système donné

$$[A_1(x, y), \ldots, A_\mu(x, y)].$$

Comme deux systèmes équivalents à un même troisième sont équivalents, nous avons ainsi démontré le théorème fondamental: *Tous les systèmes de fonctions entières de deux variables, ayant même résolvant, sont équivalents.*

Dans le chapitre précédent, une des raisons données pour légitimer l'introduction des systèmes de diviseurs en Algèbre, était que toute fonction $M(x, y)$ qui s'annule pour les systèmes de racines (ξ, η) communs à plusieurs fonctions $A_k(x, y)$, $(k = 1, 2, \ldots)$ de deux variables, sans diviseur commun, est une fonction homogène et linéaire de $A_1(x, y)$, $A_2(x, y)$, $\ldots$, à coefficients fonctions entières de x et de y. Nous pouvons maintenant considérer ce théorème comme démontré. Il faut toutefois que le résolvant $R(z)$ des fonctions $A_k(x, y)$ ne contienne pas de facteurs multiples; la démonstration de la congruence

$$M(x, y) \equiv 0 \,[\text{modd } r_0(x, y), \ldots, r_m(x, y)]$$

de laquelle on déduit, d'après ce que nous venons de voir,

$$M(x, y) \equiv 0 \,[\text{modd } A_1(x, y), \ldots, A_\mu(x, y)]$$

repose, en effet, sur cette hypothèse. En cherchant à déterminer directement deux fonctions entières $\alpha(x, y)$ et $\beta(x, y)$, vérifiant l'égalité

$$M(x, y) = \alpha(x, y) \sum_{(i)} U_i A_i(x, y) + \beta(x, y) \sum_{(i)} V_i A_i(x, y)$$

on voit cependant que, même si les systèmes (ξ_i, η_i) sont multiples, on peut encore vérifier la congruence cherchée lorsque la fonction $M(x, y)$ s'annule pour chaque $x = \xi_i$ et $y = \eta_i$, au moins autant de fois que le résolvant $R(ux + vy)$.

4. Je dis enfin que la transformation du système

$$[A_1(x, y), A_2(x, y), \ldots, A_\mu(x, y)]$$

en une seule fonction $R(z)$ contenant l'indéterminée u, nous donne vraiment une *décomposition*, en systèmes plus simples, du système $[A_1(x, y), A_2(x, y), \ldots, A_\mu(x, y)]$ dont les éléments n'ont aucun diviseur commun.

Pour nous en assurer, décomposons dans un domaine de rationalité que nous fixerons arbitrairement, le polynôme $R(z)$ en deux facteurs $F(z)$ et $G(z)$ de sorte que

$$R(z) = F(z)G(z)$$

et supposons que

$$F(z) = \sum_{(i)} f_i(x, y)u^i \qquad (i = 0, 1, 2, \ldots, m)$$

$$G(z) = \sum_{(i)} g_i(x, y)u^i. \qquad (i = 0, 1, 2, \ldots, n)$$

Si, à la décomposition de $R(z)$ en deux facteurs, correspond vraiment une *décomposition du système donné en deux systèmes plus simples,* il faut que réciproquement en *composant* de nouveau ces deux systèmes on obtienne un système équivalent au système donné. Or le produit de la composition des deux systèmes $[f_0(x, y), f_1(x, y), \ldots, f_m(x, y)]$ et $[g_0(x, y), g_1(x, y), \ldots, g_n(x, y)]$ est équivalent au système dont les éléments sont des produits de chaque élément du premier système par chaque élément du second, c'est à dire au système

$$[f_0(x, y)g_0(x, y), \ldots, f_0(x, y)g_n(x, y), f_1(x, y)g_0(x, y), \ldots, f_m(x, y)g_n(x, y)].$$

Les éléments de ce système composé ne peuvent être nuls simultanément que si, ou bien $f_0(x, y) = 0$, $f_1(x, y) = 0$, $\ldots$, $f_m(x, y) = 0$, ou bien $g_0(x, y) = 0$, $g_1(x, y) = 0$, $\ldots$, $g_n(x, y) = 0$, comme on s'en assure facilement; dans les deux cas les éléments de l'un des deux systèmes composants

sont eux-mêmes nuls. Il est d'ailleurs manifeste que $F(z) = 0$ est l'équation résolvante du système $[f_0(x, y) = 0, f_1(x, y) = 0, \ldots, f_m(x, y) = 0]$ et que $G(z) = 0$ est l'équation résolvante du système

$$[g_0(x, y) = 0, \ldots, g_n(x, y) = 0].$$

Il faut donc, ou bien que $F(z)$ s'annule, ou bien que $G(z)$ s'annule; $R(z)$ n'ayant, par hypothèse, aucun facteur double, $F(z)$ et $G(z)$ sont premiers entre eux; il faut donc de toute manière que $R(z)$ s'annule.

Inversement, si pour $z = \zeta = u\xi + \eta$, l'on a $R(z) = 0$, il faut, ou bien que $F(\zeta) = 0$, ou bien que $G(\zeta) = 0$; l'un des deux systèmes composants et, par suite, le système composé a donc tous ses éléments égaux à zéro, pour $x = \xi$, $y = \eta$.

Ainsi $R(z)$ est bien le résolvant du système composé,

$$[f_0(x, y), f_1(x, y), \ldots, f_m(x, y)][g_0(x, y), g_1(x, y), \ldots, g_n(x, y)].$$

Comme $R(z)$ est aussi le résolvant du système donné

$$[\Lambda_1(x, y), \Lambda_2(x, y), \ldots, \Lambda_\mu(x, y)],$$

nous avons démontré l'équivalence

$$[f_0(x, y), f_1(x, y), \ldots, f_m(x, y)][g_0(x, y), g_1(x, y), \ldots, g_n(x, y)]$$
$$\sim [\Lambda_1(x, y), \Lambda_2(x, y), \ldots, \Lambda_\mu(x, y)].$$

Donc, à la décomposition de $R(z)$ en deux facteurs, correspond une décomposition du système donné en deux systèmes faciles à déterminer.

Ce que nous venons de montrer pour deux facteurs est immédiatement étendu à un nombre quelconque de facteurs. Si donc, en adjoignant au domaine de rationalité les racines de l'équation résolvante $R(z) = 0$ nous décomposons le résolvant en ses facteurs linéaires, à chacun de ces facteurs linéaires correspond une partie du système

$$[\Lambda_1(x, y), \Lambda_2(x, y), \ldots, \Lambda_\mu(x, y)];$$

à $u(x - \xi_i) + v(y - \eta_i)$, par exemple, correspond l'élément

$$(x - \xi_i, y - \eta_i),$$

et nous pouvons écrire

$$[A_1(x, y), A_2(x, y), \ldots, A_\mu(x, y)] \sim \prod_{(i)} (x - \xi_i, y - \eta_i).$$

Ce résultat, qui est loin d'être évident, est semblable à celui que M. KRONECKER a obtenu dans le paragraphe 20 de son grand mémoire, dans le cas général de n fonctions de n variables. Pour bien le mettre en évidence, je nommerai chacun des facteurs $(x - \xi_i, y - \eta_i)$ *diviseur irréductible de rang deux* du système donné; le mot irréductible se rapportant au domaine de rationalité qui a été fixé.

6. Il me reste à parler du cas où le résolvant a des facteurs multiples. Alors encore, nous pouvons résoudre le problème de l'élimination et obtenir toutes les courbes et tous les points du plan qui vérifient le système considéré. Mais si des systèmes d'équations nous passons aux systèmes de fonctions nous rencontrons une équivalence d'une nature plus générale que celle dont nous avons parlé jusqu'ici. C'est le théorème fondamental, démontré à la page 71, qui nous indique la généralisation à effectuer.

En nous conformant aux nôtations de ce théorème, nous dirons, mais dans ce numéro seulement, que le système dont les éléments sont les coefficients de la forme ψ, *contient* le système dont les éléments sont les coefficients $f_1, \ldots, f_{mn}$ de la forme φ, ou encore que la forme ψ contient la forme φ. La forme contenant est donc racine d'une équation d'un degré déterminé ρ; dans cette équation, le coefficient de la puissance $(\rho - k)$ est une fonction homogène, de dimension k, des coefficients de la forme contenu, pour $k = 1, 2, \ldots, \rho$. Comme il est manifeste que, dans le théorème cité, la forme φ contient la forme ψ, les deux formes φ et ψ, et, par suite, les systèmes de leurs coefficients sont encore dits *équivalents.* Cette équivalence comprend celle des numéros précédents, où $\rho = 1$. On voit de suite que 1° si a est équivalent à b, b est aussi équivalent à a, et que 2° si a contient b, et si b contient c, a contient aussi c; donc que 3° si a est équivalent à b, et si b est équivalent à c, que a est aussi équivalent à c. On peut donc opérer avec ces équivalences comme avec les précédentes.

Ceci posé, je reprends les notations de ce chapitre et je suppose que

le résolvant $R(z)$ contienne des facteurs multiples. Désignant par R_k' la dérivée de R_k par rapport à z, je pose

$$R_1 = R : \mathrm{Dv}(R,\ R');\ R_2 = R_1 : \mathrm{Dv}(R_1,\ R_1');\ \ldots$$

il vient alors

$$R(z) = \sum_{k=1}^{m} r_k(x,\ y)u^k = \prod_{i=1}^{\nu} R_i(z)$$

ν indiquant l'ordre de multiplicité le plus élevé qui paraisse dans les facteurs linéaires de $R(z)$. Chacune des fonctions $R_i(z) = \sum_{(k)} r_k^{(i)}(x,\ y)u_i^k$ ne contiendra plus de facteurs linéaires multiples. Il en résulte, d'après les théorèmes démontrés dans les numéros précédents, les congruences

$$\Lambda_h \equiv 0\ (\mathrm{modd}\ r_1^{(i)},\ r_2^{(i)},\ \ldots); \qquad \begin{pmatrix} h=1,\ 2,\ \ldots,\ \mu \\ i=1,\ 2,\ \ldots,\ \nu \end{pmatrix}$$

donc aussi

$$\Lambda_h^{\nu} \equiv 0\ [\mathrm{modd} \prod_{i=1}^{\nu} (r_1^{(i)},\ r_2^{(i)},\ \ldots)]. \qquad (h=1,\ 2,\ \ldots,\ \mu)$$

Mais, d'autre part, dans le sens général donné maintenant à l'équivalence, Λ_h^{ν} est équivalent à Λ_h et $\prod_{(i)}(r_1^{(i)},\ r_2^{(i)},\ \ldots)$ est équivalent à $(r_0,\ r_1,\ \ldots,\ r_m)$. Λ_h, et, par suite, le système $(\Lambda_1,\ \Lambda_2,\ \ldots,\ \Lambda_\mu)$ contient donc le système $(r_0,\ r_1,\ \ldots,\ r_m)$. Il est d'ailleurs manifeste que $(r_0,\ r_1,\ \ldots,\ r_m)$ contient $(\Lambda_1,\ \Lambda_2,\ \ldots,\ \Lambda_\mu)$. Ainsi, dans le cas où le résolvant a des facteurs multiples, les systèmes sont encore *équivalents*, si nous élargissons la notion d'équivalence dans le sens du théorème de la page 71.

Dans le même ordre d'idées, on peut énoncer le théorème plus général que celui de la page 101:

Toute fonction qui s'annule pour les systèmes de racines communs à plusieurs fonctions quelconques, sans diviseur commun, est racine d'une équation algébrique dont les coefficients sont des fonctions homogènes déterminées des fonctions quelconques considérées.

M. Netto a le premier fait remarquer que cette équation est nécessairement binôme et de degré ν.

7. Mais nous sommes loin d'avoir ainsi résolu la *décomposition* des systèmes, dans le cas où le résolvant a des facteurs multiples. Il nous faudrait pour cela démontrer qu'à chaque décomposition du résolvant en

facteurs, correspond une décomposition du système. Or ici se présente un fait bien remarquable. *Le contraire peut avoir lieu.* M. KRONECKER en donne un exemple dans le paragraphe 21 de son mémoire. Voici cet exemple: $(x^2 + y, y^2)$ est un système qui n'est certes pas irréductible, puisque le système $(x^2 + y = 0, y^2 = 0)$ contient le système $(x = 0, y = 0)$. Cependant, et ici paraît, dans toute son évidence, la différence essentielle entre les diviseurs de rang deux et ceux de rang un, le système

$$(x^2 + y, y^2)$$

n'est pas décomposable en deux systèmes dont l'un est (x, y), comme il est facile de s'en assurer.

Il y a donc des systèmes qui ne sont pas décomposables et ne sont cependant pas irréductibles. Ces systèmes doivent répondre au cas où le résolvant a des facteurs multiples, puisque dans le cas des facteurs simples nous avons pu toujours effectuer une décomposition en facteurs irréductibles.

Nous pouvons encore énoncer ce fait de la manière suivante. Lorsqu'on compose de toutes les manières possibles les fonctions irréductibles d'une ou de deux variables on obtient toutes les fonctions de ces variables que l'on puisse concevoir. La même chose a lieu pour les systèmes de rang *un*. Eh bien, en composant de toutes les manières possibles tous les systèmes irréductibles de rang *deux*, on n'obtient pas tous les systèmes possibles, de rang deux.

On peut maintenant être tenté, ou bien de rejeter entièrement, comme impropres, les systèmes que l'on n'obtient pas par composition des systèmes irréductibles, ou bien de chercher à élargir l'idée même de décomposition. Mais dans ce dernier cas, il semble que cette idée perdrait tout à fait le caractère essentiel de *séparation* que l'on y attache toujours. Rejetons-les donc et ne considérons que les systèmes obtenus en composant, de toutes les manières possibles, les systèmes irréductibles de rangs *un* et *deux*, de deux variables. Alors le problème de la décomposition des systèmes, toujours possible, sera entièrement résolu, que les facteurs du résolvant soient multiples ou non.

J'ai ainsi exposé simultanément la théorie générale de l'élimination, et celle de la décomposition d'un système dans le cas de deux variables seulement. Pour faire image, j'ai introduit les diviseurs de rang *deux*, en considérant des fonctions de deux variables et en ne tenant pas compte

des nombres entiers. En réalité, les systèmes de fonctions de deux variables, admettent non seulement des diviseurs de rang deux, mais aussi des diviseurs de rang trois et déjà les fonctions d'une variable admettent des diviseurs de rang deux, comme je l'ai fait voir, par un exemple, à la page 55. Maintenant que nous sommes familiarisés avec la notion de *rang*, il est facile de répéter les raisonnements de ce chapitre sur des fonctions d'une variable seulement, en tenant compte des nombres entiers.

§ 2.

Cas général d'un nombre quelconque de variables.

1. La méthode que nous avons suivie pour étudier la décomposition d'un système formé par un nombre quelconque de fonctions entières de deux variables, indique clairement la voie que nous devrons suivre pour parvenir à une décomposition d'un système quelconque de fonctions entières. Elle nous empêche cependant de traiter ce problème dans toute sa généralité, en nous enlevant la possibilité de tenir toujours compte des cas où les résolvants que nous formerons, ont des facteurs multiples. Une méthode directe, dans laquelle nous ne supposerions pas connue l'existence des nombres algébriques nous permettrait, sans doute, d'éviter cette restriction. Il serait possible que la nouvelle généralisation de la notion de contenant et de contenu donnée par M. KRONECKER, et dont j'ai développé le théorème fondamental dans le chapitre précédent soit suffisante pour arriver, dans cet ordre d'idées, à débarasser la théorie de la décomposition des systèmes de toute restriction. Pour le moment je me contenterai de résoudre le problème, parallèlement au cas de deux variables, en ne considérant que les systèmes tels que chacun des résolvants que je formerai, n'ait pas de facteurs multiples. Soient donc

$$G_1(x_1, x_2, \ldots, x_n)$$
$$G_2(x_1, x_2, \ldots, x_n)$$
$$\ldots\ldots\ldots$$
$$G_m(x_1, x_2, \ldots, x_n)$$

un nombre quelconque de fonctions entières d'un nombre également quelconque de variables $x_1, x_2, \ldots, x_n$, et $(\Re, \Re', \Re'', \ldots, \Re^{(\rho)})$ le domaine de rationalité dont font partie les coefficients des fonctions entières et dans lequel nous allons chercher à décomposer le système considéré en systèmes plus simples.

Nous commencerons par transformer linéairement les variables $x_1, x_2, \ldots, x_n$ en posant

$$x_h = \sum_{i=1}^{n} \alpha_i^{(h)} x_i' \qquad (h = 1, 2, \ldots, n)$$

et en déterminant les coefficients $\alpha_i^{(h)}$ de manière que pour $k = 1, 2, \ldots, m$, le degré de la fonction entière G_k, par rapport à chacune des variables $x_1, x_2, \ldots, x_n$, soit égal à la dimension ν_k de cette fonction. Cette transformation est toujours possible; car si $g_k(x_1, x_2, \ldots, x_n)$ désigne l'ensemble des termes de la plus haute dimension de la fonction $G_k(x_1, x_2, \ldots, x_n)$, nous avons

$$g_k(x_1, x_2, \ldots, x_n) = g_k(\alpha_1^{(1)} x_1' + \ldots + \alpha_n^{(1)} x_n'; \ \ldots; \ \alpha_1^{(n)} x_1' + \alpha_2^{(n)} x_2' + \ldots + \alpha_n^{(n)} x_n')$$

$$= g_k(\alpha_1^{(1)}, \alpha_2^{(1)}, \ldots, \alpha_n^{(1)}) x_1'^{\nu_k} + g_k(\alpha_1^{(2)}, \alpha_2^{(2)}, \ldots, \alpha_n^{(2)}) x_2'^{\nu_k} + \ldots$$

$$\ldots + g_k(\alpha_1^{(n)}, \alpha_2^{(n)}, \ldots, \alpha_n^{(n)}) x_n'^{\nu_k}$$

et des termes de dimension ν_k contenant plusieurs des variables $x_1, x_2, \ldots, x_n$. Comme, par hypothèse, $g_k(x_1, x_2, \ldots, x_n)$ n'est pas identiquement nulle, nous pouvons toujours déterminer les systèmes $\alpha_1^{(h)}, \alpha_2^{(h)}, \ldots, \alpha_n^{(h)}$, $(h = 1, 2, \ldots, n)$ tels que pour ces systèmes $g_k(x_1, x_2, \ldots, x_n)$ $(k = 1, 2, \ldots, m)$ soit différente de zéro; alors pour $k = 1, 2, \ldots, m$, le degré de $G_k(x_1, x_2, \ldots, x_n)$ par rapport à chacun des variables $x_1', x_2', \ldots, x_n'$ sera bien égal à la dimension ν_k de cette fonction.

Si, par cette transformation $G_k(x_1, x_2, \ldots, x_n)$ devient $H_k(x_1', x_2' \ldots, x_n')$ $(k = 1, 2, \ldots, m)$, nous pouvons dire que les deux systèmes

$$(G_1, G_2, \ldots, G_m) \text{ et } (H_1, H_2, \ldots, H_m)$$

sont équivalents et nous borner à l'étude de la décomposition du second système $(H_1, H_2, \ldots, H_m)$ en systèmes plus simples.

Cette première transformation a, pour nous, un grand avantage. Aucune des fonctions $H_1, H_2, \ldots, H_m$, ne peut, en effet, contenir un

facteur qui ne soit fonction de toutes les variables $x'_1, x'_2, \ldots, x'_n$; nous savons donc que tous les diviseurs de $H_1, H_2, \ldots, H_m$ sont de variété $n^{\text{ième}}$.

Nous pourrions maintenant, en appliquant les méthodes du chapitre deux, rechercher si les fonctions $H_1, H_2, \ldots, H_m$ ont un diviseur commun; mais afin de pouvoir considérer simultanément les différentes variables, $x'_1, x'_2, \ldots, x'_n$, nous allons auparavant, comme dans le cas de deux fonctions de deux variables seulement, introduire une nouvelle quantité x' fonction linéaire et homogène des variables $x'_1, x'_2, \ldots, x'_n$ à coefficients indéterminées $u_1, u_2, \ldots, u_{n-1}$, de sorte que

$$x' = u_1x'_1 + u_2x'_2 + \ldots + u_{n-1}x'_{n-1} + u_nx'_n; \qquad u_n = 1.$$

Alors, en remplaçant x'_n par $x' - u_1x'_1 - u_2x'_2 - \ldots - u_{n-1}x'_{n-1}$ dans chacune des expressions $H_k(x'_1, x'_2, \ldots, x'_n)$, $(k = 1, 2, \ldots, m)$ et en supposant que par cette substitution $H_k(x'_1, x'_2, \ldots, x'_n)$ devienne

$$K_k(x', x'_1, x'_2, \ldots, x'_{n-1}, u_1, u_2, \ldots, u_{n-1})$$

nous devrons dire que, pour l'objet que nous avons en vue, les deux systèmes

$$[H_1(x'_1, x'_2, \ldots, x'_n), H_2(x'_1, x'_2, \ldots, x'_n), \ldots, H_m(x'_1, x'_2, \ldots, x'_n)]$$

et

$$\begin{aligned}[K_1(x', x'_1, x'_2, \ldots, x'_{n-1}, u_1, u_2, \ldots, u_{n-1})\\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot\\ K_m(x', x'_1, x'_2, \ldots, x'_{n-1}, u_1, u_2, \ldots, u_{n-1})]\end{aligned}$$

sont équivalents, car si nous pouvons décomposer l'un de ces systèmes en systèmes plus simples, nous pourrons manifestement faire de même pour son équivalent; la différence entre les deux systèmes est que nous considérons les éléments du second comme fonctions des variables $x', x'_1, x'_2, \ldots, x'_{n-1}$, sans tenir compte, pour le moment, de la relation $x' = u_1x'_1 + u_2x'_2 + \ldots + u_nx'_n$.

Chacune des fonctions $K(x', x'_1, x'_2, \ldots, x'_{n-1}; u_1, u_2, \ldots, u_{n-1})$ jouit encore de la propriété que son degré, par rapport à chacune des variables $x', x'_1, x'_2, \ldots, x'_{n-1}$ est égal à sa dimension. Si donc nous formons le plus grand commun diviseur des fonctions $K_1, K_2, \ldots, K_m$

nous savons que ce plus grand commun diviseur que nous désignerons par

$$R_1(x', x'_1, x'_2, \ldots, x'_{n-1}; u_1, u_2, \ldots, u_{n-1})$$

contient *toutes* les variables $x', x'_1, x'_2, \ldots, x'_{n-1}$. Nous pouvons ainsi écrire

$$K_\lambda(x', x'_1, \ldots, x'_{n-1}; u_1, \ldots, u_{n-1})$$

$$= R_1(x', x'_1, \ldots, x'_{n-1}; u_1, \ldots, u_{n-1}) L_\lambda(x', x'_1, \ldots, x'_{n-1}; u_1, \ldots, u_{n-1})$$

ainsi que l'équivalence $(\lambda = 1, 2, \ldots, m)$

$$(K_1, K_2, \ldots, K_m) \sim R_1(L_1, L_2, \ldots, L_m).$$

Ceci posé, cherchons à décomposer en systèmes plus simples le système $(L_1, L_2, \ldots, L_m)$. Relativement à la variable x', c'est à dire dans le domaine de rationalité $(x'_1, x'_2, \ldots, x'_{n-1}, \mathfrak{R}, \mathfrak{R}', \ldots, \mathfrak{R}^{(\rho)})$, il est équivalent à l'unité.

Dans le cas des fonctions de deux variables nous avons formé le résultant des deux fonctions et nous avons fait usage du théorème que ce résultant égalé à zéro est la condition nécessaire et suffisante à laquelle doivent satisfaire les variables qui y paraissent, pour que les deux fonctions, sans diviseur commun pour des valeurs indéterminées données à ces variables, aient précisément un diviseur commun. Nous avons ainsi pu déterminer outre les diviseurs ordinaires, communs aux deux fonctions et que nous pouvons nommer *diviseurs de rang un*, d'autres éléments, communs aux deux fonctions, qui sont d'une variété moindre, ce que les points sont aux lignes en géométrie plane, et que nous pouvons, pour cette raison, nommer *diviseurs de rang deux.* Afin de pouvoir appliquer le même théorème dans le cas plus général qui nous occupe et trouver ainsi outre le diviseur $R_1(x', x'_1, \ldots, x'_{n-1}; u_1, \ldots, u_{n-1})$ *de rang un* qui représente une variété $n^{\text{ième}}$, des diviseurs représentant une variété moindre, relions linéairement les fonctions $L_1, L_2, \ldots, L_m$ par deux systèmes d'indéterminées

$$(U_1, U_2, \ldots, U_m) \text{ et } (V_1, V_2, \ldots, V_m)$$

et formons le résultant, par rapport à x'_{n-1}, des deux fonctions

$$\sum_{i=1}^{m} U_i L_i \text{ et } \sum_{i=1}^{m} V_i L_i.$$

Ce résultant sera une fonction entière des variables x', x'_1, ..., x'_{n-2}, et des indéterminées u_1, u_2, ..., u_{n-1}, U_1, U_2, ..., U_m, V_1, V_2, ..., V_m. Nous le désignerons par

$$S_1(x', x'_1, \ldots, x'_{n-2}; u_1, u_2, \ldots, u_{n-1}; U_1, \ldots, U_m; V_1, \ldots, V_m; \mathfrak{R}, \mathfrak{R}', \ldots, \mathfrak{R}^{(\rho)}).$$

Le degré de $U_1L_1 + U_2L_2 + \ldots + U_mL_m$, par rapport à x'_{n-1}, est manifestement égal à la dimension de cette fonction; il en est de même de celui de $V_1L_1 + V_2L_2 + \ldots + V_mL_m$. Les coefficients a_0 et b_0 des plus hautes puissances de ces fonctions ordonnées par rapport à x'_{n-1} sont donc des fonctions entières des indéterminées U et V, et sont, par suite, différentes de zéro, quelles que soient les relations qui lient les autres variables x', x'_1, ..., x'_{n-2}. Donc $S_1 = 0$ est la condition nécessaire et suffisante pour que $U_1L_1 + U_2L_2 + \ldots + U_mL_m$ et $V_1L_1 + V_2L_2 + \ldots + V_mL_m$ aient un diviseur commun.

Soient s'_1, s''_1, ..., $s_1^{(m_1)}$ les coefficients de S_1 considérée comme fonction des indéterminées U et V; chacune des quantités $s_1^{(k)}$, $(k = 1, 2, \ldots, m_1)$ est alors une fonction entière des variables x', x'_1, ..., x'_{n-2} et des indéterminées u, dont les coefficients font partie du domaine de rationalité $(\mathfrak{R}, \mathfrak{R}', \ldots, \mathfrak{R}^{(\rho)})$. Si le système d'équations $s'_1 = 0$, $s''_1 = 0$, ..., $s_1^{(m_1)} = 0$, est vérifié, la fonction S_1 sera nulle, donc $U_1L_1 + U_2L_2 + \ldots + U_mL_m$ et $V_1L_1 + V_2L_2 + \ldots + V_mL_m$ auront un diviseur commun; ce diviseur est indépendant des indéterminées U_1, U_2, ..., U_m puisqu'il divise $V_1L_1 + V_2L_2 + \ldots + V_mL_m$; il est indépendant des indéterminés V_1, V_2, ..., V_m puisqu'il divise $U_1L_1 + U_2L_2 + \ldots + U_mL_m$; il est donc contenu dans chacune des fonctions L_1, L_2, ..., L_m. Inversement, si pour certaines liaisons des variables x', x'_1, ..., x'_{n-2}, les fonctions L_1, L_2, ..., L_m ont un diviseur commun, il en est de même des deux fonctions $U_1L_1 + U_2L_2 + \ldots + U_mL_m$ et $V_1L_1 + V_2L_2 + \ldots + V_mL_m$, donc $S_1 = 0$. Rien n'empêche d'ailleurs de prendre autant de systèmes d'indéterminées que l'on veut, $U_1^{(h)}$, $U_2^{(h)}$, ..., $U_m^{(h)}$ et $V_1^{(h)}$, $V_2^{(h)}$, ..., $V_m^{(h)}$, et de former pour chacun d'eux le résultant $S_1^{(h)}$ des deux fonctions $U_1^{(h)}L_1 + U_2^{(h)}L_2 + \ldots + U_m^{(h)}L_m$ et $V_1^{(h)}L_1 + V_2^{(h)}L_2 + \ldots + V_m^{(h)}L_m$. Toutes ces fonctions $S_1^{(h)}$ seront nulles; elles ne diffèrent que par les indéterminées qui y paraissent; donc les coefficients de ces indéterminées

seront nuls, et nous voyons que, dans notre hypothèse, le système d'équations

$$s_1' = 0,\ s_1'' = 0,\ \ldots,\ s_1^{(m_1)} = 0$$

est vérifié.

Le système $(s_1' = 0,\ s_1'' = 0,\ \ldots,\ s_1^{(m_1)} = 0)$ est ainsi entièrement équivalent au système $(L_1 = 0,\ L_2 = 0,\ \ldots,\ L_m = 0)$. Mais il a sur ce système un grand avantage; il ne contient plus explicitement la variable x_{n-1}'. Chacune des fonctions $s_1^{(h)}$ contient, il est vrai, les indéterminées $u_1, u_2, \ldots, u_{n-1}$; le système d'équations

$$s_1' = 0,\ s_1'' = 0,\ \ldots,\ s_1^{(m_1)} = 0,$$

représente donc un grand nombre de relations entre les variables $x', x_1', \ldots, x_{n-2}'$; mais le nombre d'éléments d'un système n'est pas ce qui le caractérise comme je l'ai déjà observé plus d'une fois; le grand nombre de relations que nous obtenons pour notre système transformé ne contrebalance donc pas l'avantage qui résulte de la réduction du nombre des variables.

Cette réduction est absolument la même que celle que nous avons obtenue dans le cas de deux fonctions de deux variables; comme alors, c'est l'emploi des indéterminées $u_1, u_2, \ldots, u_n$ qui nous permet de *joindre* deux variables en une seule; pour $h = 1, 2, \ldots, m_1$, la fonction

$$s_1^{(h)}(x', x_1', \ldots, x_{n-2}'; u_1, u_2, \ldots, u_n)$$

est identiquement égale à

$$s_1^{(h)}(u_1x_1' + u_2x_2' + \ldots + u_nx_n'; x_1', x_2', \ldots, x_{n-2}'; u_1, u_2, \ldots, u_n);$$

c'est une fonction entière des variables $x_1', x_2', \ldots, x_{n-2}'$ et de

$$u_{n-1}x_{n-1}' + u_nx_n',$$

tandis que dans chacune des fonctions entiéres

$$L(x', x_1', \ldots, x_{n-1}'; u_1, u_2, \ldots, u_n)$$

les variables x_{n-1}' et x_n' ne paraissent pas, jointes par les indéterminées

u_{n-1} et u_n. Ces indéterminées ne sont d'ailleurs contenues qu'en apparence dans l'expression

$$L(u_1x'_1 + u_2x'_2 + \ldots + u_nx'_n;\ u_1,\ u_2,\ \ldots,\ u_n;\ x'_1,\ x'_2,\ \ldots,\ x'_{n-1})$$

car le produit des deux fonctions entières de $u_1,\ u_2,\ \ldots,\ u_n$

$$R_1(u_1x'_1 + u_2x'_2 + \ldots + u_nx'_n;\ x'_1,\ x'_2,\ \ldots,\ x'_{n-1};\ u_1,\ u_2,\ \ldots,\ u_n)$$

et

$$L_k(u_1x'_1 + u_2x'_2 + \ldots + u_nx'_n;\ x'_1,\ x'_2,\ \ldots,\ x'_{n-1};\ u_1,\ u_2,\ \ldots,\ u_n)$$

est identiquement égal à

$$H_k(x'_1,\ x'_2,\ \ldots,\ x'_n);$$

pour bien le mettre en évidence, nous poserons

$$L(u_1x'_1 + u_2x'_2 + \ldots + u_nx'_n;\ x'_1, x'_2, \ldots, x'_{n-1};\ u_1, u_2, \ldots, u_n) = \Lambda(x'_1, x'_2, \ldots, x'_n).$$

2. Recherchons maintenant si l'équivalence des deux systèmes

$$(s'_1,\ s''_1,\ \ldots,\ s_1^{(m_1)}) \text{ et } (L_1,\ L_2,\ \ldots,\ L_m)$$

est de la nature de celles que nous avons définies dans le chapitre précédent. Nous observons d'abord que le résultant S_1 des deux fonctions $U_1L_1 + U_2L_2 + \ldots + U_mL_m$ et $V_1L_1 + V_2L_2 + \ldots + V_mL_m$ étant une fonction homogène et linéaire de ces deux fonctions dont les coefficients sont fonctions entières des quantités $x,\ x_1,\ x_2,\ \ldots,\ x_{n-1},\ u_1,\ u_2,\ \ldots,\ u_n$, S_1 contiendra le système $(L_1,\ L_2,\ \ldots,\ L_m)$; il en résulte que chacune des fonctions $s_1^{(k)}$, $(k = 1,\ 2,\ \ldots,\ m_1)$, contiendra le même système ou encore le système

$$(\Lambda_1,\ \Lambda_2,\ \ldots,\ \Lambda_m).$$

Mais alors pour $k = 1,\ 2,\ \ldots,\ \tau$, les coefficients $\sigma_i^{(k)}$, $(i = 1,\ 2,\ \ldots,\ \nu)$, de $s^{(k)}$ considérée comme fonctions des indéterminées $u_1,\ u_2,\ \ldots,\ u_n$, sont eux-mêmes fonctions linéaires et homogènes de $\Lambda_1,\ \Lambda_2,\ \ldots,\ \Lambda_m$ à coefficients fonctions entières, de sorte que nous avons le système de congruences

$$\sigma_{1,i}^{(k)} \equiv 0 \,(\text{modd } \Lambda_1,\ \Lambda_2,\ \ldots,\ \Lambda_m). \qquad \begin{pmatrix} k=1,2,\ldots,m_1 \\ i=1,2,\ldots,\nu_1 \end{pmatrix}$$

D'autre part, si nous considérons les deux fonctions

$$M_1(x'_1,\ x'_2,\ \ldots,\ x'_n) = \sum_{\substack{(h,\,k)\\ \binom{h=1,\,2,\,\ldots,\,m_1}{k=1,\,2,\,\ldots,\,\nu_1}}} w_h^{(k)}\sigma_h^{(k)}(x'_1,\ x'_2,\ \ldots,\ x'_n)$$

$$N_1(x'_1,\ x'_2,\ \ldots,\ x'_n) = \sum_{(h,\,k)} w_h'^{(k)}\sigma_h^{(k)}(x'_1,\ x'_2,\ \ldots,\ x'_n)$$

où les $w_h^{(k)}$ et $w_h'^{(k)}$ désignent deux systèmes d'indéterminées, et si nous cherchons à déterminer *deux* multiplicateurs *entiers*

$$\alpha_1(x'_1,\ x'_2,\ \ldots,\ x'_n) \text{ et } \beta_1(x'_1,\ x'_2,\ \ldots,\ x'_n)$$

de manière à vérifier l'égalité

$$\Lambda(x'_1,\ x'_2,\ \ldots,\ x'_n)$$

$$= \alpha_1(x'_1,\ x'_2,\ \ldots,\ x'_n)M_1(x'_1,\ x'_2,\ \ldots,\ x'_n) + \beta_1(x'_1,\ x'_2,\ \ldots,\ x'_n)N_1(x'_1,\ x'_2,\ \ldots,\ x'_n)$$

ou, ce qui revient au même, *un* multiplicateur *entier* $\alpha_1(x'_1,\ x'_2,\ \ldots,\ x'_n)$ de manière à vérifier la congruence

$$\Lambda(x'_1,\ x'_2,\ \ldots,\ x'_n) \equiv \alpha_1(x'_1,\ x'_2,\ \ldots,\ x'_n)M(x'_1,\ x'_2,\ \ldots,\ x'_n) \ [\mathrm{mod}\ N(x'_1,\ x'_2,\ \ldots,\ x'_n)],$$

nous avons, d'après la formule de LAGRANGE,

$$\alpha_1(x'_1,\ x'_2,\ \ldots,\ x'_n)$$

$$= \sum_{(k)} \frac{\Lambda(x'_1,\ \ldots,\ x'_{n-1},\ \xi_n^{(k)})}{M_1(x'_1,\ \ldots,\ x'_{n-1},\ \xi_n^{(k)})} \frac{N_1(x'_1,\ \ldots,\ x'_{n-1},\ x'_n)}{x'_n - \xi_n^{(k)}} \frac{1}{D_{x'_n}N_1(x'_1,\ \ldots,\ x'_{n-1},\ x'_n)_{x'_n=\xi_n^{(k)}}}$$

$\xi^{(k)}$ désignant l'une quelconque des racines de l'équation

$$N_1(x'_n) = 0$$

et la somme étant étendue à toutes ces racines.

Le problème est maintenant identique à celui qui s'est présenté dans le paragraphe précédent. Il s'agit de voir si la forme sous laquelle nous venons d'écrire le multiplicateur $\alpha_1(x'_1,\ x'_2,\ \ldots,\ x'_n)$ peut être illusoire, pour des valeurs particulières données aux variables $x'_1,\ x'_2,\ \ldots,\ x'_n$.

Convenons, une fois pour toutes, de ne restreindre la variabilité des variables $x'_1,\ x'_2,\ \ldots,\ x'_{n-1}$ que par *une* équation, ce qui revient à laisser

par exemple $x'_1, x'_2, \ldots, x'_{n-2}$ indéterminées, à les joindre au domaine de rationalité et à donner alors à x'_{n-1} une valeur particulière; ou encore, à relier $x_1, x_2, \ldots, x_n$ par deux relations indépendantes, seulement. Nous nous apercevrons bientôt de la raison qui nous amène à faire cette restriction; sans elle, en effet, nous ne pourrions pas résoudre le problème de l'équivalence des systèmes de fonctions d'un nombre quelconque de variables.

Il nous faut faire encore une autre hypothèse. Nous n'avons pu résoudre entièrement la question proposée, pour $n = 2$, que dans le cas où le résolvant du système considéré, qui était le plus grand commun diviseur des coefficients de la forme $S(U, V)$, n'a pas de facteurs multiples; et nous avons vu qu'alors le dénominateur $H(x_k, y)$ ne pouvait être nul que du premier ordre pour une valeur particulière donnée à y. Nous ferons ici l'hypothèse équivalente en supposant que, les $n - 2$ variables $x'_1, x'_2, \ldots, x'_{n-2}$ restant indéterminées, le plus grand commun diviseur des coefficients de la fonction $S(x', x'_1, \ldots, x'_{n-2})$, considérée comme une fonction des indéterminées w et w', n'ait pas de facteurs multiples; alors, lorsque le dénominateur $M_1(x'_1, \ldots, x'_{n-1}, \xi_n^{(k)})$ s'annule pour une valeur déterminée, indépendante des indéterminées w et w', donnée à x'_{n-1}, il ne sera nul que du premier ordre.

Cette hypothèse est plus que suffisante pour l'objet que nous avons en vue; car il suffirait, pour démontrer que l'expression précédente de $\alpha_1(x'_1, x'_2, \ldots, x'_n)$ n'est pas illusoire, de supposer simplement que la fonction $A(x'_1, x'_2, \ldots, x'_{n-1}, \xi_n^{(k)})$ qui s'annule en même temps que $M(x'_1, x'_2, \ldots, x'_{n-1}, \xi_n^{(k)})$ pour des systèmes indépendants des indéterminées w et w', soit, pour ces systèmes, au moins nulle d'un ordre aussi élevé que $M(x'_1, x'_2, \ldots, x'_{n-1}, \xi_n^{(k)})$.

Sous cette hypothèse, on voit facilement que l'expression de $\alpha_1(x'_1, \ldots, x'_n)$ donnée par la formule de LAGRANGE, n'est pas illusoire, pour des valeurs indépendantes des indéterminées w et w' données à $x'_1, x'_2, \ldots, x'_n$. Le raisonnement est le même que dans le cas de deux variables, et je ne le répéterai pas.

Le produit

$$\prod_{(k)} M_1(x'_1, x'_2, \ldots, x'_{n-1}, \xi_n^{(k)}) \prod_{(k)} D_{x'_n} N(x'_1, x'_2, \ldots, x'_{n-1}, x'_n)_{x'_n = \xi^{(k)}}$$

est une fonction entière des indéterminées w et w'; nous pouvons le mettre sous la forme

$$f(x'_1, x'_2, \ldots, x'_{n-1})E(x'_1, x'_2, \ldots, x'_{n-1}; w, w')$$

en désignant par $f(x'_1, x'_2, \ldots, x'_{n-1})$ le plus grand commun diviseur des coefficients des indéterminées w et w', et, par suite, par $E(x'_1, x'_2, \ldots, x'_{n-1}; w, w')$ une forme *primitive* des mêmes indéterminées. Les coefficients de cette forme, n'ayant aucun facteur commun, ne peuvent s'annuler simultanément lorsque la variabilité de $x'_1, x'_2, \ldots, x'_{n-1}$ n'est limitée que par une relation algébrique.

Posons, pour abréger,

$$\gamma(x'_1, x'_2, \ldots, x'_n) = E(x'_1, x'_2, \ldots, x'_{n-1}; w, w')\alpha(x'_1, x'_2, \ldots, x'_n).$$

Le résultat obtenu est que la fonction $\gamma(x'_1, x'_2, \ldots, x'_n)$ ne se présente jamais sous une forme illusoire. Mais alors la fonction rationnelle de $x'_1, x'_2, \ldots, x'_{n-1}$, donnée par la formule de LAGRANGE,

$$\gamma(x'_1, x'_2, \ldots, x'_n)$$

est sûrement fonction entière de x'_{n-1}; elle est donc fonction entière de $x'_1, \ldots, x'_{n-2}$; en effet, nous avons démontré dans le second chapitre, qu'une fonction rationnelle de plusieurs variables $x, y, z, \ldots$ qui est entière par rapport à l'une des variables x, est également entière par rapport à toutes les autres $y, z, \ldots$, à condition toutefois que le dénominateur de la fonction rationnelle ne contienne pas de facteur indépendant de x. Cette condition peut être, ici, considérée comme vérifiée puisque nous avons commencé par transformer les variables $x_1, x_2, \ldots, x_n$ à l'aide d'une substitution linéaire à coefficients constants, et que nous pouvons choisir ces coefficients d'une manière arbitraire, pourvu qu'une relation déterminée ne soit pas vérifiée; nous les choisirons, après coup, tels, qu'en outre, la dimension de $f(x'_1, x'_2, \ldots, x'_{n-1})$ soit égale au degré de cette fonction par rapport à la variable x'_{n-1}; en répétant alors tous nos raisonnements, nous serons certain que $\gamma(x'_1, x'_2, \ldots, x'_{n-1}, x'_n)$ est une fonction entière des n variables $x'_1, x'_2, \ldots, x'_n$.

La congruence

$$E(x_1', x_2', \ldots, x_{n-1}'; w, w')A(x_1', x_2', \ldots, x_n') \equiv \gamma(x_1', x_2', \ldots, x_n')M_1(x_1', x_2', \ldots, x_n') \quad [\mathrm{mod}\ N_1(x_1', x_2', \ldots, x_n')]$$

une fois vérifiée, le quotient

$$\beta_1(x_1', x_2', \ldots, x_n') = \frac{E(x_1', \ldots, x_{n-1}'; w, w')A(x_1', \ldots, x_n') - \gamma_1(x_1', \ldots, x_n')M_1(x_1', \ldots, x_n')}{N_1(x_1', x_2', \ldots, x_n')}$$

est nécessairement une fonction entière de x_n'; toujours d'après le même théorème, il est donc également fonction entière des autres variables $x_1', x_2', \ldots, x_{n-1}'$.

Ainsi l'égalité

$$E(x_1', \ldots, x_{n-1}'; w, w')A(x_1', \ldots, x_n') = \gamma_1(x_1', \ldots, x_n')M_1(x_1', \ldots, x_n') + \beta_1(x_1', \ldots, x_n')N_1(x_1', \ldots, x_n')$$

est vérifiée pour les deux fonctions entières $\gamma_1(x_1', \ldots, x_n')$ et $\beta_1(x_1', \ldots, x_n')$ que nous venons de former. Ces fonctions entières dépendent des indéterminées w et w'; ordonnons les deux termes de l'égalité précédente, suivant ces indéterminées, et comparons les coefficients. Dans chacune des égalités que nous obtenons, le terme de droite est une fonction linéaire et homogène des fonctions $\sigma(x_1', x_2', \ldots, x_n')$; les coefficients de ces fonctions $\sigma(x_1', x_2', \ldots, x_n')$ sont des fonctions entières des variables $x_1', x_2', \ldots, x_n'$; si pour une valeur particulière donnée à x_n' et une relation particulière entre $x_1', \ldots, x_{n-1}'$, toutes les fonctions $\sigma(x_1', x_2', \ldots, x_n')$ sont nulles, le terme de droite est nul, donc aussi le terme de gauche. Pour en conclure que la fonction $A(x_1', \ldots, x_n')$ est alors elle-même nulle, ce qui est nécessaire pour que cette égalité réponde à notre recherche, il serait nécessaire de savoir que pour la relation particulière considérée, le coefficient de $A(x_1', \ldots, x_n')$ ne peut être nul. Or, nous savons seulement que tous les coefficients de la forme primitive

$$E(x_1', x_2', \ldots, x_{n-1}'; w, w')$$

ne peuvent être nuls simultanément pour cette relation particulière; mais chacun d'eux peut parfaitement s'annuler à son tour, si nous considérons successivement plusieurs relations particulières. Aucune des égalités précédentes ne répond donc à notre recherche.

Nous parvenons cependant bien simplement au résultat, et cela en divisant les deux termes de l'égalité démontrée par une forme primitive $E(x'_1, \ldots, x'_{n-1}; t, t')$ dont les coefficients sont identiques à ceux de la forme primitive $E(x'_1, \ldots, x'_{n-1}; w, w')$. Nous obtenons alors, en effet, une nouvelle égalité,

$$\frac{E(x'_1, \ldots, x'_{n-1}; w, w')}{E(x'_1, \ldots, x'_{n-1}; t, t')} \Delta(x'_1, \ldots, x'_n) = \sum_{(h)} \tau_h(x'_1, \ldots, x'_n; w, w', t, t') \sigma_h(x'_1, \ldots, x'_n)$$

dans laquelle les expressions $\tau_h(x'_1, x'_2, \ldots, x'_n; w, w', t, t')$ sont, il est vrai, des fonctions *rationnelles* de $x'_1, x'_2, \ldots, x'_{n-1}$, mais ne contiennent au dénominateur qu'une forme *primitive* des indéterminées t et t'. Si donc toutes les fonctions $\sigma(x'_1, \ldots, x'_n)$ s'annulent lorsque, x'_n ayant une valeur déterminée, les variables $x'_1, x'_2, \ldots, x'_{n-1}$ sont liées par *une* relation particulière, les coefficients $\tau(x'_1, \ldots, x'_n)$ de ces fonctions, quoique se présentant sous forme de fractions ne seront pas infinis, et, par suite, comme tout à l'heure, l'expression

$$\frac{E(x'_1, \ldots, x'_{n-1}; w, w')}{E(x'_1, \ldots, x'_{n-1}; t, t')} \Delta(x'_1, x'_2, \ldots, x'_n)$$

sera nulle. Mais maintenant nous pouvons en conclure que la fonction $\Delta(x'_1, x'_2, \ldots, x'_n)$ sera elle-même égale à zéro; car le quotient des deux formes *primitives* $E(w, w')$ et $E(t, t')$ ne saurait être, pour une relation particulière entre $x'_1, x'_2, \ldots, x'_{n-1}$, ni nul, ni infini.

Nous voyons donc que s'il est impossible de mettre toujours les quantités $\Delta(x'_1, \ldots, x'_{n-1})$, elles-mêmes, sous la forme de fonctions linéaires et homogènes des quantités $\sigma(x'_1, \ldots, x'_n)$, dont les coefficients soient fonctions entières de $x'_1, \ldots, x'_n$, il est, par contre, toujours possible de mettre sous la forme d'une fonction linéaire et homogène des quantités $\sigma(x'_1, \ldots, x'_n)$, le produit de la fonction $\Delta(x'_1, \ldots, x'_n)$ par le quotient de deux formes primitives ayant mêmes coefficients, les coefficients de cette fonction homogène et linéaire étant toujours finis et déterminés,

lorsque les variables $x'_1, \ldots, x'_{n-1}$ ne sont liées que par *une* relation algébrique. Nous sommes ainsi amenés à dire qu'*une fonction entière F d'un nombre quelconque n de variables, contient un système donné* $(f_1, f_2, \ldots, f_m)$, et à écrire

$$F \equiv 0 \,(\mathrm{modd}\, f_1,\ f_2,\ \ldots,\ f_m)$$

lorsque nous pouvons, en multipliant F par le quotient de deux formes primitives, ayant mêmes coefficients, établir une égalité

$$\frac{E(U)}{E(V)} F = \sum_{k=1}^{m} \varphi_k . f_k$$

dans laquelle nous soyons certain que tous les coefficients φ_k soient finis et déterminés, quelle que soit la relation particulière qui lie les $(n-1)$ variables paraissant au dénominateur.

Le quotient $\frac{E(U)}{E(V)}$ des deux formes primitives $E(U)$ et $E(V)$ joue vraiment ici le rôle d'une *unité.*

C'est dans ce sens plus large que celui que nous avions donné en commençant, parce qu'il suffisait dans le cas des fonctions de deux variables, qu'il faut entendre l'équivalence des deux systèmes

$$[A_1(x'_1, \ldots, x'_n),\ A_2(x'_1, \ldots, x'_n),\ \ldots,\ A_m(x'_1, \ldots, x'_n)]$$

et

$$[\sigma'_{11}(x'_1, \ldots, x'_n),\ \sigma'_{12}(x'_1, \ldots, x'_n),\ \ldots,\ \sigma^{(m_1)}_{1,\nu_1}(x'_1, \ldots, x'_n)].$$

Nous appliquerons aussi à ce genre d'équivalences, le symbole $\sim$, et nous écrirons

$$(A_1, A_2, \ldots, A_m) \sim (\sigma'_{11}, \sigma'_{12}, \ldots, \sigma'_{1,\nu_1}, \sigma''_{11}, \ldots\ldots, \sigma^{(m_1)}_{1,\nu_1}).$$

Nous voyons enfin facilement qu'à l'aide des indéterminées $u_1, u_2, \ldots, u_{n-1}$, prises plusieurs fois, les deux systèmes

$$[A_1(x'_1, \ldots, x'_n),\ A_2(x'_1, \ldots, x'_n),\ \ldots,\ A'_m(x'_1, \ldots, x'_n)]$$

et

$$[s'_1(x', x'_1, \ldots, x'_{n-2}),\ s''_1(x', x'_1, \ldots, x'_{n-2}),\ \ldots,\ s^{(m_1)}_1(x', x'_1, \ldots, x'_{n-2})]$$

sont aussi équivalents.

3. Nous avons jusqu'ici ramené l'étude du système quelconque donné à celui d'un système

$$(s_1', s_1'', \ldots, s_1^{(m_1)})$$

dont les éléments, considérés comme des fonctions des variables

$$x', x_1', x_2', \ldots, x_{n-2}',$$

contiennent une variable de moins que ceux du système proposé, et nous avons vu ce qu'il faut entendre par équivalence de ces deux systèmes, puisque nous venons de traduire cette équivalence par une équation algébrique.

Il nous faut maintenant répéter sur le système $(s_1', s_1'', \ldots, s_1^{(m_1)})$ les mêmes raisonnements que nous avons faits tout à l'heure sur le système $(G_1, G_2, \ldots, G_m)$. Nous introduirons tout d'abord de nouvelle variables

$$x_1'', x_2'', \ldots, x_{n-1}''$$

fonctions linéaires des précédentes et nous déterminerons les coefficients de ces fonctions linéaires de manière que pour $i = 1, 2, \ldots, m_1$, le degré de $s_1^{(i)}$ par rapport à chacune des nouvelles variables soit égal à la dimension de cette fonction. Le système

$$[s_1'(x', x_1', \ldots, x_{n-2}', u_1, \ldots, u_n); s_1''(x', x_1', \ldots, x_{n-2}', u_1, \ldots, u_n); \ldots$$
$$\ldots; s_1^{(m_1)}(x', x_1', \ldots, x_{n-2}', u_1, \ldots, u_n)]$$

est ainsi transformé en un système équivalent que nous désignerons par

$$[H_1'(x_1'', x_2'', \ldots, x_{n-1}'', u_1, \ldots, u_n); H_2'(x_1'', x_2'', \ldots, x_{n-1}'', u_1, \ldots, u_n); \ldots$$
$$\ldots; H_{m_1}'(x_1'', x_2'', \ldots, x_{n-1}'', u_1, \ldots, u_n)].$$

Nous relierons ensuite les nouvelles variables par une fonction homogène et linéaire à coefficients indéterminés

$$x'' = v_1 x_1'' + v_2 x_2'' + \ldots + v_{n-1} x_{n-1}''; \qquad v_{n-1} = 1,$$

et nous substituerons à x''_{n-1} sa valeur dans chacune des m_1 fonctions considérées. Nous obtiendrons ainsi un système

$$\begin{aligned}
&[K'_1(x'', x''_1, \ldots, x''_{n-2}, u_1, \ldots, u_n, v_1, \ldots, v_{n-1});\\
&\quad K'_2(x'', x''_1, \ldots, x''_{n-2}, u_1, \ldots, u_n, v_1, \ldots, v_{n-1});\\
&\quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&\quad K'_{m_1}(x'', x''_1, \ldots, x''_{n-2}, u_1, \ldots, u_n, v_1, \ldots, v_{n-1})]
\end{aligned}$$

équivalent au précédent. Si les éléments de ce système ont un diviseur commun

$$R_2(x'', x''_1, \ldots, x''_{n-2}, u_1, \ldots, u_n, v_1, \ldots, v_{n-1}),$$

ce diviseur contiendra nécessairement les $(n-1)$ variables x'', x''_1, …, x''_{n-2}; posons

$$\begin{aligned}
&K'_h(x'', x''_1, \ldots, x''_{n-2}, u_1, \ldots, u_n, v_1, \ldots, v_{n-1})\\
&= \left\{ \begin{array}{l} R_2(x'', x''_1, \ldots, x''_{n-2}, u_1, \ldots, u_n, v_1, \ldots, v_{n-1}) \\ \times\ L'_h(x'', x''_1, \ldots, x''_{n-2}, u_1, \ldots, u_n, v_1, \ldots, v_{n-1}) \end{array} \right\}; \quad {\scriptstyle (h=1,2,\ldots,m_1)}
\end{aligned}$$

l'équivalence

$$(K'_1, K'_2, \ldots, K'_{m_1}) \sim R_2(L'_1, L'_2, \ldots, L'_{m_1})$$

sera certainement vérifiée, et il nous suffira de considérer le système

$$\begin{aligned}
&[L'_1(x'', x''_1, \ldots, x''_{n-2}, u_1, \ldots, u_n, v_1, \ldots, v_{n-1});\\
&\quad L'_2(x'', x''_1, \ldots, x''_{n-2}, u_1, \ldots, u_n, v_1, \ldots, v_{n-1});\\
&\quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&\quad L'_{m_1}(x'', x''_1, \ldots, x''_{n-2}, u_1, \ldots, u_n, v_1, \ldots, v_{n-1})]
\end{aligned}$$

qui, *relativement* à la variable x'', est équivalent à l'unité, comme tout à l'heure le système

$$[L_1(x', x'_1, \ldots, x'_{n-1}, u_1, \ldots, u_n); \ldots\ldots; L_m(x', x'_1, \ldots, x'_{n-1}, u_1, \ldots, u_n)],$$

relativement à la variable x'.

Après avoir relié les éléments $L'_1, L'_2, \ldots, L'_{m_1}$, par deux systèmes d'indéterminées $U_1, U_2, \ldots, U_{m_1}$ et $V_1, V_2, \ldots, V_{m_1}$, nous formons le résultant S_2 des deux fonctions

$$\sum_{(k)} U_k L'_k \quad \text{et} \quad \sum_{(k)} V_k L'_k \qquad (k = 1, 2, \ldots, m_1)$$

par rapport à la variable x''_{n-2}. Si $s'_2, s''_2, \ldots, s_2^{(m_2)}$, désignent les coefficients de la fonction S_2 ordonnée suivant les puissances des indéterminées U et V, et si $\sigma_{2i}^{(k)}$, $(k = 1, 2, \ldots, m_2;\ i = 1, 2, \ldots, \nu_2)$ sont les coefficients des fonctions $s'_2, s''_2, \ldots, s_2^{(m_2)}$ ordonnées par rapport aux puissances des indéterminées $v_1, v_2, \ldots, v_{n-1}$, nous voyons, en raisonnant comme tout à l'heure, que le système

$$(\sigma'_{21}, \sigma'_{22}, \sigma'_{23}, \ldots, \sigma'_{2\nu_2}, \sigma''_{21}, \ldots, \sigma_{2\nu_2}^{(m_2)})$$

est équivalent au système

$$(A'_1, A'_2, \ldots, A'_{m_1})$$

dans le sens que nous avons été amenés à donner à l'équivalence en recherchant les rapports des deux systèmes

$$(A_1, A_2, \ldots, A_m) \quad \text{et} \quad (\sigma'_{11}, \sigma'_{12}, \ldots, \sigma'_{1\nu_1}, \sigma''_{11}, \ldots, \sigma_{1\nu_1}^{(m_1)}).$$

Les indéterminées $v_1, v_2, \ldots, v_{n-1}$ ne sont contenues qu'en apparence dans les éléments $L'_1, L'_2, \ldots, L'_{m_1}$, considérés comme fonctions de $x''_1, x''_2, \ldots, x''_{n-1}$; c'est pourquoi nous avons posé pour plus de clarté

$$A'_h(x''_1, x''_2, \ldots, x''_{n-1})$$
$$= L'_h(v_1 x''_1 + v_2 x''_2 + \ldots + v_{n-1} x''_{n-1}, x''_1, x''_2, \ldots, x''_{n-2}, v_1, v_2, \ldots, v_{n-1}). \qquad (h = 1, 2, \ldots, m_1)$$

Mais les indéterminées $u_1, u_2, \ldots, u_n$ font partie intégrante des fonctions $L'_1, L'_2, \ldots, L'_{m_1}$, et sont, par suite, contenues dans les fonctions $A'_1, A'_2, \ldots, A'_{m_1}$; il ne faut donc pas ici, pour rechercher l'équivalence des systèmes, revenir aux coefficients des fonctions $\sigma_{2i}^{(k)}$, ordonnées suivant les puissances des indéterminées $u_1, u_2, \ldots, u_n$; il faut, au contraire, comparer les systèmes qui contiennent encore ces indéterminées. Cette différence ne change rien au raisonnement que nous avons fait plus

haut; nous pouvons, par exemple, joindre simplement $u_1, u_2, \ldots, u_n$ au domaine de rationalité. En répétant alors le même raisonnement nous voyons que chacune des fonctions $A'_k(x''_1, x''_2, \ldots, x''_{n-1}, u_1, \ldots, u_n)$, $(k = 1, 2, \ldots, m_1)$, multipliée par le quotient de deux formes primitives par rapport aux variables $x''_1, x''_2, \ldots, x''_{n-2}$, peut être mise sous la forme d'une fonction linéaire et homogène des fonctions

$$\sigma''^{(k)}_{2i}(x''_1, x''_2, \ldots, x''_{n-1}, u_1, \ldots, u_n), \qquad (i=1,2,\ldots,\nu_2;\ k=1,2,\ldots,m_2)$$

dont les coefficients sont fonctions entières de x''_{n-1} et ne contiennent au dénominateur qu'une forme primitive par rapport aux variables $x''_1, x''_2, \ldots, x''_{n-2}$. Le système $(A'_1, A'_2, \ldots, A'_{m_1})$ *contient* donc le système $(\sigma'_{21}, \sigma'_{22}, \ldots, \sigma'_{2\nu_2}, \sigma''_{21}, \ldots, \sigma''^{(m_2)}_{2\nu_2})$. Inversement S_2 et, par suite, le système $(\sigma'_{21}, \sigma'_{22}, \ldots, \sigma_{2\nu_2}, \sigma''_{21}, \ldots, \sigma''^{(m_2)}_{2\nu_2})$ *contient* le système $(A'_1, A'_2, \ldots, A'_{m_1})$. Les deux systèmes que nous comparons sont donc *équivalents,* et nous pouvons écrire

$$(A'_1, A'_2, \ldots, A'_{m_1}) \sim (\sigma'_{21}, \sigma'_{22}, \ldots, \sigma'_{2\nu_2}, \sigma''_{21}, \ldots, \sigma''^{(m_2)}_{2\nu_2}).$$

De plus, comme le système $(\sigma'_{21}, \sigma'_{22}, \ldots, \sigma'_{2\nu_2}, \sigma''_{21}, \ldots, \sigma''^{(m_2)}_{2\nu_2})$ est lui-même équivalent au système formé par les éléments $s'_2, s''_2, \ldots, s''^{(m_2)}_2$, pris un certain nombre de fois, et pour des systèmes différents d'indéterminées $v_1, \ldots, v_{n-1}$, nous avons aussi démontré l'équivalence, à l'aide d'indéterminées v en nombre suffisant, des deux systèmes

$$[A'_1(x''_1, x''_2, \ldots, x''_{n-1}),\ A'_2(x''_1, x''_2, \ldots, x''_{n-1}),\ \ldots,\ A'_{m_1}(x''_1, x''_2, \ldots, x''_{n-1})]$$

et

$$[s'_2(x'', x''_1, \ldots, x''_{n-3}),\ s''_2(x'', x''_1, \ldots, x''_{n-3}),\ \ldots,\ s''^{(m_2)}_2(x'', x''_1, \ldots, x''_{n-3})]$$

où, pour abréger, nous n'avons écrit qu'une fois, dans la dernière parenthèse, chacun des éléments $s''^{(i)}_2$.

4. Nous continuons ainsi et nous formons successivement une série de fonctions

$$R_1, R_2, R_3, \ldots, R_{n-2}, R_{n-1}$$

contenant respectivement $n, n-1, n-2, \ldots, 3$, et enfin deux variables. Nous retombons en dernier lieu dans le cas particulier d'un nombre quel-

conque de fonctions de deux variables, cas particulier que nous avons étudié dans le paragraphe précédent.

Soient

$$R_{n-1}(x^{(n-1)},\ x_1^{(n-1)};\ u_1,\ \ldots,\ u_n;\ v_1,\ \ldots,\ v_{n-1};\ \ldots\ldots;\ w_1,\ w_2)$$

le plus grand commun diviseur de ces fonctions de deux variables, et

$$[L_1^{(n-2)}(x^{(n-1)},\ x_1^{(n-1)},\ u_1,\ \ldots,\ u_n,\ v_1,\ \ldots,\ v_{n-1},\ \ldots\ldots,\ w_1,\ w_2);\ \ldots\ldots;\ L_{m_{n-2}}^{(n-2)}(x^{(n-1)},\ x_1^{(n-1)},\ u_1,\ \ldots,\ u_n,\ v_1,\ \ldots,\ v_{n-1},\ \ldots\ldots,\ w_1,\ w_2)]$$

le système débarassé de ce plus grand commun diviseur et déjà transformé de manière que pour $i = 1, 2, \ldots, m_{n-2}$, le degré de la fonction $L_i^{(n-2)}$, par rapport à $x^{(n-1)}$ et à $x_1^{(n-1)}$ soit égal à la dimension de cette fonction.

Nous formons le résultant, par rapport à $x_1^{(n-1)}$, des deux fonctions

$$\sum_{(k)} U_k L_k^{(n-2)} \quad \text{et} \quad \sum_{(k)} V_k L_k^{(n-2)}; \qquad (k=1,2,\ldots,m_{n-2})$$

si nous désignons par

$$S_{n-1}(x^{n-1},\ u_1,\ \ldots,\ u_n,\ v_1,\ \ldots,\ v_{n-1},\ \ldots\ldots,\ w_1,\ w_2;\ U_1,\ \ldots,\ U_{m_{n-2}},\ V_1,\ \ldots,\ V_{m_{n-2}})$$

ce résultant; par

$$s_{n-1}^{(h)}(x^{(n-1)},\ u_1,\ \ldots,\ u_n,\ v_1,\ \ldots,\ v_{n-1},\ \ldots\ldots,\ w_1,\ w_2) \qquad (h=1,2,\ldots,m_{n-1})$$

les coefficients de S_{n-1}, ordonnée par rapport aux indéterminées U et V; par

$$\sigma'_{n-1,1},\ \sigma'_{n-1,2},\ \sigma'_{n-1,3},\ \ldots\ldots,\ \sigma_{n-1,\nu_{n-1}}^{(m_{n-1})}$$

les coefficients des $s_{n-1}^{(h)}$, $(h = 1, 2, \ldots, m_{n-1})$ ordonnées par rapport aux indéterminées w_1 et w_2, après que l'on a substitué à $x^{(n-1)}$ sa valeur

$$w_1 x_1^{(n-1)} + w_2 x_2^{(n-1)};$$

et enfin par

$$\Lambda_i^{(n-2)}(x_1^{(n-1)},\ x_2^{(n-1)},\ u_1,\ \ldots,\ u_n,\ v_1,\ \ldots,\ v_{n-1},\ \ldots\ldots) \qquad (i=1,2,\ldots,m_{n-2})$$

les fonctions

$$L_i^{(n-2)}(w_1 x_1^{(n-1)} + w_2 x_2^{(n-1)},\ x_r^{(n-1)},\ u_1,\ \ldots,\ u_n,\ v_1,\ \ldots,\ v_{n-1},\ \ldots\ldots,\ w_1,\ w_2)$$
$$(i=1,2,\ldots,m_{n-2})$$

qui ne contiennent qu'en apparence les indéterminées w_1 et w_2, nous voyons, comme dans le paragraphe précédent, que les deux systèmes

$$(A_1^{(n-2)},\ A_2^{(n-2)},\ \ldots,\ A_{m_{n-2}}^{(n-2)}) \quad \text{et} \quad (\sigma'_{n-1,1},\ \sigma'_{n-1,2},\ \ldots\ldots,\ \sigma_{n-1,\nu_{n-1}}^{(m_{n-1})})$$

sont équivalents, dans le sens que nous avons attaché à ce mot dans le chapitre précédent, et, à plus forte raison, dans le sens plus général que nous lui avons donné dans ce paragraphe-ci.

Soient

$$R_n(x^{(n-1)},\ u_1,\ \ldots,\ u_n,\ v_1,\ \ldots,\ v_{n-1},\ \ldots,\ w_1,\ w_2)$$

le plus grand commun diviseur des fonctions $s_{n-1}^{(h)}$, $(h = 1, 2, \ldots, m_{n-1})$ et

$$s_{n-1}^{(h)}(x^{(n-1)},\ u_1,\ \ldots,\ w_2) = R_n(x^{(n-1)},\ u_1,\ \ldots,\ w_2)\, L_h^{(n-1)}(x^{(n-1)},\ u_1,\ \ldots,\ w_2).$$
$$(h=1,2,\ldots,m_{n-1})$$

Les fonctions $L_1^{(n-1)}$, $L_2^{(n-1)}$, $\ldots$, $L_{m_{n-1}}^{(n-1)}$ de la seule variable $x^{(n-1)}$ étant sans diviseur commun, l'équivalence *absolue*

$$(L_1^{(n-1)},\ L_2^{(n-1)},\ \ldots,\ L_{m_{n-1}}^{(n-1)}) \sim 1$$

est manifeste.

Si cependant nous considérons, outre les variables, les nombres entiers, il est possible que les fonctions $L_1^{(n-1)}$, $L_2^{(n-1)}$, $\ldots$, $L_{m_{n-1}}^{(n-1)}$ aient un diviseur commun de rang deux. Je rappelle l'exemple donné dans le chapitre précédent. Pour obtenir ce diviseur, formons le résultant, par rapport à $x^{(n-1)}$, des deux fonctions

$$\sum_{(k)} U_k L_k^{(n-1)} \quad \text{et} \quad \sum_{(k)} V_k L_k^{(n-1)}.$$

Ce résultant sera une forme, à coefficients *entiers,* des indéterminées $u, v, \ldots, w$. Soit R_{n+1} le plus grand commun diviseur des coefficients

de cette forme; comme toute forme primitive, à coefficients entiers, est équivalente à l'unité, nous aurons l'équivalence *absolue*

$$(L_1^{(n-1)},\ L_2^{(n-1)},\ \ldots,\ L_{m_{n-1}}^{(n-1)}) \sim R_{n+1}.$$

5. Ainsi l'ensemble des fonctions R_1, R_2, ..., R_{n+1}, ou, si nous ne tenons pas compte des nombres entiers, l'ensemble des fonctions R_1, R_2, ..., R_n remplace le système donné, et le remplace complètement. La première condition de toute *décomposition* d'un système de fonctions se trouve aussi remplie; car chaque fonction R_k contient un nombre différent de variables, et nous avons ainsi isolés les variétés d'ordres différents représentées par le système d'équations correspondant. C'est à la *condensation* des variables x_1, x_2, ..., x_n, à l'aide des indéterminées u, v, ..., w, que nous devons ce résultat.

Il y a plus; le théorème sur la décomposition des systèmes que nous avons démontré à la fin du paragraphe précédent, a encore lieu. Cependant comme sa démonstration, tout en étant analogue au cas de deux variables, exige la notation du résultant de n fonctions de n variables, notion que nous ne pouvons pas établir sans longueurs avant d'avoir résolu le problème général de l'élimination, nous ne la donnerons pas ici.(1) Mais, comme de ce théorème résulte que c'est bien une *décomposition* du système $(G_1, G_2, \ldots, G_m)$ que nous avons obtenue, et que ce fait est de la plus haute importance, nous introduirons, dès maintenant, une terminologie qui le mette bien en évidence. Nous nommerons R_1 *résolvant de rang un*, R_2 *résolvant de rang deux*, et, en général

$$R_k(x^{(k-1)},\ x_1^{(k-1)},\ \ldots,\ x_{n-k}^{(k-1)},\ u_1,\ \ldots,\ u_n,\ v_1,\ \ldots)$$

résolvant de rang k du système considéré. Un ou plusieurs de ces résolvants peuvent, pour des systèmes particuliers donnés, se réduire à l'unité.

Nous pouvons alors aussi définir rigoureusement ce qu'il faut entendre par *rang* d'un système de modules contenu dans un autre système de modules, ou encore par *rang de divisibilité*. Nous avons obtenu le résol-

(1) Comparez KRONECKER, Festschrift § 20.

vant de rang un, en cherchant le plus grand commun diviseur de toutes les fonctions $K_1, K_2, \ldots, K_m$ dont le système est équivalent à celui des fonctions $G_1, G_2, \ldots, G_m$. Ce résolvant R_1 est, dans le sens ordinaire du mot, contenu dans le système

$$(K_1, K_2, \ldots, K_m);$$

nous dirons qu'il est *le plus grand commun diviseur, de rang un,* de ce système. Mais le système

$$(L_1, L_2, \ldots, L_m)$$

est également contenu dans le système $(K_1, K_2, \ldots, K_m)$; il est, de plus, équivalent au système $(\sigma'_{11}, \sigma'_{12}, \ldots, \sigma'^{(m_1)}_{1\nu_1})$ ou encore au système dont les éléments sont les coefficients $s'_1, s''_1, \ldots, s^{(m_1)}_1$ de la forme $S_1(w, w')$, ces coefficients étant pris pour plusieurs systèmes d'indéterminées $u_1, u_2, \ldots, u_n$; mais, ces éléments $s'_1, s''_1, \ldots, s^{(m_1)}_1$, ont, comme plus grand commun diviseur *de rang un,* le résolvant R_2 *de rang deux;* c'est pourquoi nous dirons que le système $(L_1, L_2, \ldots, L_m)$, ou encore le système $(\sigma'_{11}, \sigma'_{12}, \ldots, \sigma'^{(m_1)}_{1\nu_1})$, ou tout autre système équivalent, est un diviseur *de rang deux* du système donné.

Comme le système $(s'_1, s''_1, \ldots, s^{(m_1)}_1)$ est équivalent au produit $R_2(L'_1, L'_2, \ldots, L'_{m_1})$, le système $(L'_1, L'_2, \ldots, L'_{m_1})$ est contenu dans le système $(L_1, L_2, \ldots, L_m)$ et, par suite aussi, dans le système donné $(G_1, G_2, \ldots, G_m)$. Il est cependant bien évident que $(L'_1, L'_2, \ldots, L'_{m_1})$ n'est pas contenu dans le système donné au même titre que R_1 ou que $(L_1, L_2, \ldots, L_m)$. C'est pourquoi, comme $(L'_1, L'_2, \ldots, L'_{m_1})$ est équivalent au système $(\sigma'_{21}, \sigma'_{22}, \ldots, \sigma'^{(m_2)}_{2\nu_2})$, ou encore au système dont les éléments ont, comme plus grand commun diviseur *de rang un,* le résolvant R_3 *de rang trois,* nous dirons que $(L'_1, L'_2, \ldots, L'_{m_1})$ ainsi que tous ses équivalents sont *diviseurs de rang trois* du système $(G_1, G_2, \ldots, G_m)$. Ainsi de suite. En général nous dirons que le rang d'un système de modules contenu dans un autre système de modules est égal au rang de celui des résolvants du système contenant que l'on rencontre le premier en partant du système contenu et en formant aussi ses résolvants. Bien entendu, il est absolument nécessaire de tenir compte des résolvants qui se réduisent à l'unité.

Pour être conséquent nous devrons aussi dire que le système $(L'_1, L'_2, \ldots, L'_{m_1})$, par exemple, qui est diviseur *de rang trois* de $(G_1, G_2, \ldots, G_m)$, est diviseur *de rang deux* du système $(L_1, L_2, \ldots, L_m)$ à condition de considérer chacun des éléments du premier système comme une fonction des $(n - 1)$ variables x'', x''_1, x''_2, $\ldots$, x''_{n-2}, et chacun des éléments du dernier système comme une fonction des n variables x', x'_1, x'_2, $\ldots$, x'_{n-1}. En général nous devrons dire que le système

$$(L_1^{(h)}, L_2^{(h)}, \ldots, L_{m_h}^{(h)})$$

est diviseur *de rang* $(i + 1)$ du système

$$(L_1^{(h-i)}, L_2^{(h-i)}, \ldots, L_{m_{h-i}}^{(h-i)}),$$

chaque élément $L^{(h)}$ étant considéré comme une fonction des $(n - h)$ variables $x^{(h-1)}$, $x_1^{(h-1)}$, $\ldots$, $x_{n-h-1}^{(h-1)}$ et chaque élément $L^{(h-i)}$ comme une fonction des $(n - h + i)$ variables $x^{(h-i+1)}$, $x_1^{(h-i+1)}$, $\ldots$, $x_{n-h+i-1}^{(h-i+1)}$; ainsi, lorsque deux systèmes sont divisibles l'un par l'autre, leur *rang de divisibilité* moins 1, sera donné par la différence de l'ordre des variétés représentées par les éléments de l'un des systèmes et par ceux de l'autre. En un mot, *le rang* est relatif à la variabilité donnée; il est égal à la diminution du nombre des variables + 1, par une condensation de ces variables, à l'aide des indéterminées u, v, $\ldots$, w.

Il me reste à faire une remarque importante sur la généralisation de l'idée de contenant et de contenu que nous avons été amenés à donner dans ce paragraphe. En disant que les formes E considérées étaient *primitives,* je me suis conformé au langage habituel et j'ai entendu par forme primitive une forme dont tous les coefficients n'ont pas de diviseur commun. Maintenant que nous avons introduit la notion de diviseur d'un rang quelconque, il faut distinguer; j'adopterai à cet effet, la terminologie de Gauss et j'entendrai par *forme proprement primitive* une forme dont tous les coefficients n'ont aucun diviseur commun *d'un rang quelconque.* Or rien ne nous dit que les coefficients des formes E considérées n'ont aucun diviseur commun de rang supérieur au premier; nous savons au contraire que des fonctions de deux variables déjà, sans diviseur commun de rang un, peuvent s'annuler pour des valeurs particulières données à ces variables. Il en résulte que ces formes E ne sont en général pas proprement primi-

tives, mais seulement *improprement primitives,* et que les équivalences, et par suite aussi la décomposition, obtenues ne doivent être considérées que comme des *équivalences impropres* et une *décomposition impropre,* c'est à dire telle que chaque pas fait en avant se rapporte, non pas à tout l'ensemble de la décomposition, mais seulement *au rang* où l'on se trouve. C'est dans ce sens, et dans ce sens seulement, qu'il faut entendre l'équivalence du système $(G_1, G_2, \ldots, G_m)$ et de l'ensemble des fonctions $R_1, R_2, \ldots, R_{n+1}$. Nous réserverons le symbole $\sim$ au cas où les formes E sont proprement primitives.

Pour terminer, nous pouvons répéter, pour chaque rang plus grand que *un,* les raisonnements de la fin du paragraphe précédent. Nous sommes alors amenés à distinguer entre les systèmes décomposables et les systèmes impropres que nous avons exclus de nos recherches, au moins dans ce Mémoire. Pour compléter la théorie générale de la décomposition des systèmes, il reste à caractériser plus spécialement ces systèmes impropres dont M. KRONECKER a, le premier, donné un exemple.

CHAPITRE V.

Théorie générale de l'élimination.

§ 1.

De l'équation résolvante.

1. Le but que l'on se propose dans le théorie *générale* de l'élimination est de reconnaître la nature des restrictions apportées à la variabilité d'un nombre quelconque de quantités variables par un nombre également quelconque d'équations algébriques reliant ces quantités.

Dans la théorie de l'élimination proprement dite, on étudie de plus près les systèmes d'équations algébriques soumis à des conditions plus spéciales, particulièrement ceux où le nombre des équations est égal au nombre des variables.

Nous nous occuperons ici exclusivement de la théorie générale de l'élimination.

C'est DESCARTES qui, le premier, considéra la solution d'une équation $F(x) = 0$, comme la recherche des restrictions apportées à la variabilité de la quantité essentiellement variable x, par la condition déterminée $F(x) = 0$. Avant lui, on n'avait envisagé la résolution des équations que comme la recherche des valeurs qui, substituées aux inconnues, vérifient les équations données. Dans la théorie générale dè l'élimination on néglige entièrement ce dernier point de vue et l'on se place à celui de DESCARTES en l'étendant à un nombre quelconque d'équations entre un nombre également quelconque de variables. Le mot éliminer n'a pas le sens de *laisser de côté,* mais au contraire, celui de *fixer, en les séparant,* les restrictions apportées à la variabilité de plusieurs variables, par des équations algébriques.

Soient donc

$$G_k(x_1, x_2, \ldots, x_n) = 0, \qquad (k=1, 2, \ldots, m)$$

m équations algébriques reliant les n variables $x_1, x_2, \ldots, x_n$. Les coefficients des fonctions entières $G_1, G_2, \ldots, G_m$ font partie d'un domaine de rationalité donné sur lequel nous n'avons aucune prise. Nous avons prise au contraire sur les variables $x_1, x_2, \ldots, x_n$, et nous cherchons la nature des restrictions apportées à ces variables par les équations considérées. Comme le domaine de rationalité peut lui-même contenir autant de variables que l'on veut, le problème ainsi posé est plus général que si l'on se proposait de trouver la nature des restrictions apportées à toutes les variables paraissant dans les polynômes $G_1, G_2, \ldots, G_m$, par les relations $G_1 = 0, G_2 = 0, \ldots, G_m = 0$.

Les restrictions dont nous parlons se distingueront tout d'abord par le plus ou moins de variabilité qu'elles laissent aux quantités $x_1, x_2, \ldots, x_n$. Nous devons donc chercher, avant tout, à transformer le système d'équations

$$G_1 = 0, G_2 = 0, \ldots, G_m = 0$$

en un autre qui, tout en lui étant équivalent, sépare nettement les différents degrés de variabilité que possèdent encore les quantités $x_1, x_2, \ldots, x_n$.

L'analogie de ce problème et de celui dont nous avons exposé la solution dans le chapitre précédent est manifeste; la seule différence est, qu'au lieu d'un système de fonctions, nous considérons un système d'équations, et que, par suite, au lieu de la transformation du système $(G_1, G_2, \ldots, G_m)$ en $R_1, R_2, \ldots, R_n$, nous obtenons celle du système d'équations

$$G_1 = 0,\ G_2 = 0,\ \ldots,\ G_m = 0$$

en une seule équation

$$R_1 . R_2 . R_3 \ldots R_n = 0,$$

l'équation résolvante du système.

En conservant les mêmes notations que dans la recherche précédente, nous voyons immédiatement que si les variables $x_1, x_2, \ldots, x_n$ sont liées par les relations

$$G_1 = 0,\ G_2 = 0,\ \ldots,\ G_m = 0$$

il faut, ou bien que le résolvant R_1 soit nul, ou que nous ayons à la fois

$$L_1 = 0,\ L_2 = 0,\ \ldots,\ L_m = 0.$$

Si ce dernier système d'équations est vérifié, il faut, ou bien que le résolvant R_2 soit nul, ou que nous ayons à la fois

$$L'_1 = 0,\ L'_2 = 0,\ \ldots,\ L'_{m_1} = 0.$$

Ainsi de suite. Enfin, si le système

$$L_1^{(n-2)} = 0,\ L_2^{(n-2)} = 0,\ \ldots,\ L_{m_{n-2}}^{(n-2)} = 0$$

est vérifié, il faut, ou bien que le résolvant R_n soit nul, ou que nous ayons à la fois

$$L_1^{(n-1)} = 0,\ L_2^{(n-1)} = 0,\ \ldots,\ L_{m_{n-1}}^{(n-1)} = 0.$$

Cette dernière alternative est impossible, puisque les fonctions $L_1^{(n-1)}$, $L_2^{(n-1)}, \ldots, L_{m_{n-1}}^{(n-1)}$ de la seule variable $x^{(n)}$, sont sans diviseur commun.

Donc, si les équations

$$G_1 = 0,\ G_2 = 0,\ \ldots,\ G_m = 0$$

sont vérifiées il faut que l'un des résolvants $R_1, R_2, \ldots, R_n$ s'annule. Inversement, si l'un de ces résolvants s'annule, nous avons à la fois

$$G_1 = 0, \quad G_2 = 0, \quad \ldots, \quad G_m = 0.$$

Les restrictions apportées à la variabilité de $x_1, x_2, \ldots, x_n$ d'une part par le système d'équations

$$(G_1 = 0, \; G_2 = 0, \; \ldots, \; G_m = 0)$$

et de l'autre par l'équation unique

$$R_1 R_2 \ldots R_n = 0$$

sont donc absolument les mêmes.

Nous sommes ici dispensés de rechercher, comme nous l'avons fait dans le chapitre précédent, la nature de l'équivalence des systèmes $(L_1^{(k)}, L_2^{(k)}, \ldots, L_{m_k}^{(k)})$ et de ceux dont les éléments sont les coefficients des formes S_k, ce qui simplifie considérablement le problème. Il n'y a plus d'équivalence propre ou impropre; l'équivalence indique tout simplement que les restrictions apportées à la variabilité de $x_1, x_2, \ldots, x_n$ par le système d'équations données et par son équation résolvante sont identiques; nous pouvons donc écrire

$$(G_1 = 0, \; G_2 = 0, \; \ldots, \; G_m = 0) \sim (R_1 R_2 \ldots R_n = 0).$$

De plus, le problème général de l'élimination peut toujours être résolu, tandis que nous avons vu que celui de l'équivalence des systèmes ne peut l'être complètement que si les différents résolvants n'ont pas de facteurs doubles. Il est vrai que cette restriction qui est, comme nous l'avons vu, dans la nature des choses, puisqu'il y a des systèmes non décomposables sans être irréductibles, a une fâcheuse influence sur la théorie générale de l'élimination. Elle nous empêche de tenir compte de l'ordre de multiplicité des solutions du problème. Ainsi, en appliquant la théorie de l'élimination à la géométrie, nous isolerons certainement *toutes* les surfaces, courbes et points donnés par un nombre quelconque d'équations entre trois variables x, y et z; nous marquerons *tous* les points de l'espace dont les coordonnées vérifient simultanément les équations

données; mais si A sont ces surfaces, B ces courbes et C ces points, il se pourrait fort bien que les surfaces représentées par les équations données eussent, par exemple, outre les points C un point commun sur B, sans que nous obtenions autrement ce point que comme un des points de la courbe B.

Pour ne pas être obligé de changer de notations dans le courant de ce chapitre, nous désignerons tout de suite par R_h, non pas le plus grand commun diviseur des fonctions $K_1^{(h-1)}$, $K_2^{(h-1)}$, ..., $K_{m_{h-1}}^{(h-1)}$, mais le quotient de ce plus grand commun diviseur et du plus grand commun diviseur qu'il a lui-même avec sa dérivée par rapport à $x^{(h)}$, de sorte que, si pour un instant R_h représente encore la fonction considérée jusqu'ici, notre nouvelle fonction R_h sera égale à

$$\frac{R_h}{\mathrm{Dv}(R_h,\ D_{x^{(h)}}R_h)}$$

c'est à dire à l'ancienne fonction R_h débarassée de ses facteurs multiples. Comme nous ne pourrons tenir compte des solutions multiples, ce n'est pas une restriction que nous faisons là.

2. Dans ce qui va suivre, nous interpréterons chacune des expressions R_h indépendamment de toutes les autres, en recherchant de quelle manière *chacune* des équations $R_h = 0$ limite la variabilité de $x_1, x_2, \ldots, x_n$. Nous pourrons donc supposer que les systèmes de variables que nous avons distingués en affectant les quantités $x_1, x_2, \ldots, x_n$ d'indices supérieurs soient tous les mêmes; cela revient simplement, géométriquement parlant, à interpréter chacune des équations $R_h = 0$ dans un autre système de coordonnées en nous réservant de choisir convenablement chacun de ces systèmes. Mais pour éviter toute confusion nous désignerons par

$$y_1, y_2, \ldots, y_n$$

au lieu de $x_1, x_2, \ldots, x_n$, les nouvelles variables considérées; ce sont des variables se rapportant à un système d'axes coordonnés mobiles. Nous désignerons de même par y la fonction linéaire à coefficients indéterminés

$$y = u_1y_1 + u_2y_2 + \ldots + u_ny_n; \qquad u_n = 1.$$

Nous aurons alors, dans le domaine de rationalité donné, l'équivalence

$$[G_1(y_1, y_2, \ldots, y_n); \ldots; G_m(y_1, y_2, \ldots, y_n)]$$
$$\sim R_1(y, y_1, \ldots, y_{n-1}, u_1, \ldots, u_n)$$
$$\times [H'_1(y, y_1, \ldots, y_{n-2}, u_1, \ldots, u_n); \ldots; H'_{m_1}(y, y_1, \ldots, y_{n-2}, u_1, \ldots, u_n)].$$

En posant

$$y' = v_{n-1}y + v_1y_1 + \ldots + v_{n-2}y_{n-2}; \qquad v_{n-1} = 1$$

et en remplaçant y par sa valeur tirée de cette équation, il vient

$$[H'_1(y, y_1, \ldots, y_{n-2}, u_1, \ldots, u_n); H'_2(y, y_1, \ldots, y_{n-2}, u_1, \ldots, u_n); \ldots$$
$$\ldots; H'_{m_1}(y, y_1, \ldots, y_{n-2}, u_1, \ldots, u_n)]$$
$$\sim [K'_1(y', y_1, \ldots, y_{n-2}, u_1, \ldots, u_n); K'_2(y', y_1, \ldots, y_{n-2}, u_1, \ldots, u_n); \ldots$$
$$\ldots; K'_{m_1}(y', y_1, \ldots, y_{n-2}, u_1, \ldots, u_n)]$$
$$\sim R_2(y', y_1, \ldots, y_{n-2}, u_1, \ldots, u_n, v_1, \ldots, v_{n-1})$$
$$\times [L'_1(y', y_1, \ldots, y_{n-2}, u_1, \ldots, u_n); \ldots\ldots; L'_{m_1}(y', y_1, \ldots, y_{n-2}, u_1, \ldots, u_n)].$$

Le résultant S_2 sera ensuite pris par rapport à y_{n-2} comme tout à l'heure par rapport à x_{n-2}, et ainsi de suite; mais, après avoir introduit chaque nouvelle fonction linéaire à coefficients indéterminés, $y^{(k)}$, c'est $y^{(k-1)}$, et non pas y_{n-k} par analogie avec x_{n-k}, qu'il faudra remplacer dans le système considéré par sa valeur tirée de cette relation.

D'ailleurs, en désignant par $u_1^{(i)}, u_2^{(i)}, \ldots, u_n^{(i)}$, $(i = 1, 2, \ldots)$ de nouvelles indéterminées on a

$$y' = u'_1y_1 + u'_2y_2 + \ldots + u'_{n-2}y_{n-2} + u_{n-1}y_{n-1} + u_ny_n$$

et, en général,

$$y^{(k)} = u_1^{(k)}y_1 + u_2^{(k)}y_2 + \ldots + u_{n-k-1}^{(k)}y_{n-k-1} + u_{n-k}^{(k-1)}y_{n-k} + \ldots$$
$$\ldots + u'_{n-2}y_{n-2} + u_{n-1}y_{n-1} + u_ny_n. \qquad (k=1,2,\ldots)$$

Nous obtenons ainsi l'équivalence

$$[G_1(y_1, y_2, \ldots, y_n) = 0; G_2(y_1, y_2, \ldots, y_n) = 0; \ldots\ldots; G_m(y_1, y_2, \ldots, y_n) = 0]$$
$$\sim \left[\prod_{h=1}^{n} R_h(y^{(h-1)}, y_1, y_2, \ldots, y_{n-h}, u_1, \ldots, u_n, \ldots, u_1^{(h-1)}, \ldots, u_{n-h}^{(h-1)}) = 0\right].$$

De ce que, les quantités $u_1^{(i)}, u_2^{(i)}, \ldots, u_n^{(i)}$ désignant toujours des indéterminées, l'équation résolvante $R_1 R_2 \ldots R_n = 0$ est la conséquence nécessaire et suffisante du système d'équations $G_1 = 0, G_2 = 0, \ldots, G_m = 0$, nous allons déduire une transformation importante de cette résolvante qui nous fera clairement voir le rôle fondamental que jouent les indéterminées $u_1^{(i)}, u_2^{(i)}, \ldots, u_n^{(i)}$, dans la théorie générale de l'élimination.

A cet effet nous allons d'abord rechercher toutes les valeurs de chacune des variables $y_1, y_2, \ldots, y_n$ qui peuvent vérifier le système donné. Commençons par la variable y_n.

Les expressions $y, y', y'', \ldots, y^{(n-1)}$ se transforment toutes en y_n, lorsque nous substituons aux quantités indéterminées $u_1, u_2, \ldots, u_{n-1}$, $v_1, v_2, \ldots, v_{n-2}, \ldots, w_1$, la valeur zéro. Si donc nous répétons tous les raisonnements qui nous ont amené à la décomposition du système donné sans faire aucune substitution linéaire à coefficients indéterminés, ce qui revient à remplacer $y, y', y'', \ldots, y^{(n-1)}$ par y_n, nous pourrons dire que le résultat obtenu est le même que tout à l'heure, à condition de substituer aux indéterminées les valeurs zéro, à l'exception de $u_{n-1}, v_{n-2}, \ldots, w_2$, qui sont définies égales à l'unité. Nous obtiendrons ainsi l'équivalence

$$(G_1 = 0,\ G_2 = 0,\ \ldots,\ G_m = 0)$$
$$\sim \prod_{k=1}^{n} R_k^{(n)}(y_n,\ y_1,\ y_2,\ \ldots,\ y_{n-k};\ 0,\ 0,\ \ldots,\ 1;\ \ldots..)$$

dans laquelle nous avons donné à R_k l'indice supérieur (n) pour indiquer que $y^{(k)}$, y est remplacé par y_n et que nous considérons spécialement cette expression comme une fonction de y_n. D'après ce que nous venons de dire $R_k^{(n)}$ sera le plus grand commun diviseur des coefficients du résultant $S_{k-1}^{(n)}$ des deux fonctions

$$\sum_{h=1}^{m_{k-2}} U_h L_h^{(k-2)}(y_n,\ y_1,\ y_2,\ \ldots,\ y_{n-k},\ y_{n-k+1};\ 0,\ 0,\ \ldots,\ 1;\ 0,\ \ldots..)$$

et

$$\sum_{h=1}^{m_{k-2}} V_h L_h^{(k-2)}(y_n,\ y_1,\ y_2,\ \ldots,\ y_{n-k},\ y_{n-k+1};\ 0,\ 0,\ \ldots,\ 1;\ 0,\ \ldots..)$$

par rapport à la variable y_{n-k+1}, ce résultant étant considéré comme une fonction des indéterminées U et V.

Les racines de l'équation $R_k^{(n)} = 0$ sont fonctions algébriques de $y_1, y_2, \ldots, y_{n-k}$; soit $\eta_n^{(k-1)}$ l'une quelconque d'entre elles. D'après ce que nous avons vu sur les propriétés du résultant, comme $S_{k-1}^{(n)}$ est nulle pour $y_n = \eta_n^{(k-1)}$, les deux fonctions précédentes auront pour $y_n = \eta_n^{(k-1)}$ un diviseur commun en y_{n-k+1}; il y aura donc sûrement une valeur de y_{n-k+1}, $y_{n-k+1} = \eta_{n-k+1}^{(k-1)}$ telle que nous ayons à la fois

$$\sum_{h=1}^{m_{k-2}} U_h L_h^{(k-2)}(\eta_n^{(k-1)}, y_1, y_2, \ldots, y_{n-k}, \eta_{n-k+1}^{(k-1)}; 0, 0, \ldots, 1; 0, \ldots.) = 0$$

et

$$\sum_{h=1}^{m_{k-2}} V_h L_h^{(k-2)}(\eta_n^{(k-1)}, y_1, y_2, \ldots, y_{n-k}, \eta_{n-k+1}^{(k-1)}; 0, 0, \ldots, 1; 0, \ldots.) = 0$$

et, par suite, simultanément

$$L_h^{(k-2)}(\eta_n^{(k-1)}, y_1, y_2, \ldots, y_{n-k}, \eta_{n-k+1}^{(k-1)}; 0, 0, \ldots, 1; 0, \ldots.) = 0 \qquad (h = 1, 2, \ldots, m_{k-2})$$

comme nous nous en assurons facilement en considérant un nombre assez grand de systèmes d'indéterminées U et V auxquels correspondent, il est vrai, des résultants $S_{k-1}^{(n)}$ différents, mais cependant la même fonction $R_k^{(n)}$.

Puisque toutes les fonctions $L_h^{(k-2)}$ sont nulles pour $y_n = \eta_n^{(k-1)}$ et $y_{n-k+1} = \eta_{n-k+1}^{(k-1)}$ il en sera de même du résultant $S_{k-2}^{(n)}$ des deux fonctions

$$\sum_{h=1}^{m_{k-3}} U_h L_h^{(k-3)}(\eta_n^{(k-1)}, y_1, y_2, \ldots, \eta_{n-k+1}^{(k-1)}, y_{n-k+2}; 0, 0, \ldots, 1; 0, \ldots.)$$

et

$$\sum_{h=1}^{m_{k-3}} V_h L_h^{(k-3)}(\eta_n^{(k-1)}, y_1, y_2, \ldots, \eta_{n-k+1}^{(k-1)}, y_{n-k+2}; 0, 0, \ldots, 1; 0, \ldots.)$$

qui est pris par rapport à y_{n-k+2}; car $K_h^{(k-2)} = R_{k-1} L_h^{(k-2)}$ et les systèmes désignés plus haut par $(s'_{k-2}, s''_{k-2}, \ldots)$, $(H_1^{(k-2)}, H_2^{(k-2)}, \ldots)$ et $(K_1^{(k-2)}, K_2^{(k-2)}, \ldots)$ sont ici identiques. De ce que $S_{k-2}^{(n)}$ est nul pour $y_n = \eta_n^{(k-1)}$ et $y_{n-k+1} = \eta_{n-k+1}^{(k-1)}$, nous concluons comme tout à l'heure qu'il y a sûrement une valeur de y_{n-k+2},

$$y_{n-k+2} = \eta_{n-k+2}^{(k-1)}$$

telle que toutes les fonctions

$$L_h^{(k-3)}(\eta_n^{(k-1)},\ y_1,\ y_2,\ \ldots,\ y_{n-k},\ \eta_{n-k+1}^{(k-1)},\ \eta_{n-k+2}^{(k-1)};\ 0,\ 0,\ \ldots,\ 1;\ 0,\ \ldots..) \qquad (h=1,2,\ldots,m_{k-3})$$

soient nulles simultanément.

En continuant ainsi, nous voyons enfin que le résultant $S_1^{(n)}$ est nul, pour

$$y_n = \eta_n^{(k-1)};\ y_{n-k+1} = \eta_{n-k+1}^{(k-1)};\ y_{n-k+2} = \eta_{n-k+2}^{(k-1)};\ \ldots;\ y_{n-2} = \eta_{n-2}^{(k-1)}.$$

Ce résultant est pris par rapport à y_{n-1}. Il y a donc nécessairement une valeur de y_{n-1}

$$y_{n-1} = \eta_{n-1}^{(k-1)}$$

telle que les équations

$$L_h(\eta_n^{(k)},\ y_1,\ y_2,\ \ldots,\ y_{n-k},\ \eta_{n-k+1}^{(k-1)},\ \eta_{n-k+2}^{(k-1)},\ \ldots,\ \eta_{n-1}^{(k-1)}) = 0 \qquad (h=1,2,\ldots,m)$$

et, par suite, aussi

$$K_h(\eta_n^{(k)},\ y_1,\ y_2,\ \ldots,\ y_{n-k},\ \eta_{n-k+1}^{(k-1)},\ \eta_{n-k+2}^{(k-1)},\ \ldots,\ \eta_{n-1}^{(k-1)}) = 0 \qquad (h=1,2,\ldots,m)$$

soient vérifiées simultanément. Mais

$$K_h(y_n,\ y_1,\ y_2,\ \ldots,\ y_{n-1}) = G_h(y_1,\ y_2,\ \ldots,\ y_{n-1},\ y_n); \qquad (h=1,2,\ldots,m)$$

nous pouvons donc énoncer la proposition suivante:

A toute racine $\eta_n^{(k-1)}$ de l'équation $R_k^{(n)} = 0$ correspond un système au moins

$$\eta_{n-k+1}^{(k-1)},\ \eta_{n-k+2}^{(k-1)},\ \ldots,\ \eta_{n-1}^{(k-1)}$$

tel que les équations

$$G_1(y_1,\ y_2,\ \ldots,\ y_{n-k},\ \eta_{n-k+1}^{(k-1)},\ \eta_{n-k+2}^{(k-1)},\ \ldots,\ \eta_{n-1}^{(k-1)},\ \eta_n^{(k-1)}) = 0$$

$$G_2(y_1,\ y_2,\ \ldots,\ y_{n-k},\ \eta_{n-k+1}^{(k-1)},\ \eta_{n-k+2}^{(k-1)},\ \ldots,\ \eta_{n-1}^{(k-1)},\ \eta_n^{(k-1)}) = 0$$

. . . . . .

$$G_m(y_1,\ y_2,\ \ldots,\ y_{n-k},\ \eta_{n-k+1}^{(k-1)},\ \eta_{n-k+2}^{(k-1)},\ \ldots,\ \eta_{n-1}^{(k-1)},\ \eta_n^{(k-1)}) = 0$$

soient vérifiées simultanément.

Ceci a lieu pour $k = 1, 2, \ldots, n$. Ainsi à chaque racine $y_n = \eta_n$ de chacune des équations $R_1^{(n)} = 0$, $R_2^{(n)} = 0$, $\ldots$, $R_n^{(n)} = 0$, correspondent respectivement des valeurs de $0, 1, \ldots, (n-1)$ des autres variables qui, jointes à η_n elle-même, vérifient simultanément les équations données. Nous obtenons donc des variétés différentes satisfaisant au problème, suivant la résolvante $R_k = 0$ dont nous considérons les racines après avoir substitué aux *indéterminées* la valeur zéro.

Inversement si ζ_n est une valeur de y_n qui permette de vérifier simultanément les équations $G_1 = 0$, $G_2 = 0$, $\ldots$, $G_m = 0$, il faut que, ou bien $R_1^{(n)}$ soit nul pour $y_n = \zeta_n$, c'est à dire que ζ_n soit égale à l'une des racines η_n précédemment définies, ou bien que toutes les équations

$$L_h(\zeta_n, y_1, y_2, \ldots, y_{n-2}; 0, 0, \ldots, 1) = 0 \qquad (h=1,2,\ldots,m)$$

soient vérifiées. Dans ce dernier cas le résultant $S_1^{(n)}$ s'annule pour $y_n = \zeta_n$; donc, ou bien $R_2^{(n)}(\zeta_n) = 0$ et alors ζ_n est égale à l'une des η_n' auxquelles correspondent, dans notre notation, des valeurs de y_{n-1}, $y_{n-1} = \eta_{n-1}'$ telles que

$$G_h(y_1, y_2, \ldots, y_{n-2}, \eta_{n-1}', \eta_n') = 0 \qquad (h=1,2,\ldots,m)$$

ou bien toutes les équations

$$L_h'(\zeta_n, y_1, y_2, \ldots, y_{n-3}; 0, 0, \ldots, 1; 0, 0, \ldots, 1) = 0$$

sont vérifiées. Ainsi de suite. Enfin, ou bien $R_n^{(n)}$ s'annule pour $y_n = \zeta_n$ et alors ζ_n est égale à l'une des racines $\eta_n^{(n-1)}$ auxquelles correspondent des solutions

$$\eta_1^{(n-1)}, \eta_2^{(n-1)}, \ldots, \eta_{n-1}^{(n-1)}$$

telles que

$$G_h(\eta_1^{(n-1)}, \eta_2^{(n-1)}, \ldots, \eta_{n-1}^{(n-1)}, \eta_n^{(n-1)}) = 0, \qquad (h=1,2,\ldots,m)$$

ou bien toutes les fonctions

$$L_h^{(n-1)}(y_n; 0, 0, \ldots, 1; \ldots\ldots; 0, 1) \qquad (h=1,2,\ldots,m_{n-1})$$

s'annulent pour $y_n = \zeta_n$. Ces fonctions étant sans diviseur commun, cette dernière alternative est impossible. Donc toutes les valeurs de y_n pour

lesquelles les équations $G_h = 0$, $(h = 1, 2, \ldots, m)$ peuvent être vérifiées simultanément sont nécessairement racines d'une des équations $R_k^{(n)} = 0$, $(k = 1, 2, \ldots, n)$.

Si nous n'avions pas simplifié l'écriture en considérant les variables y au lieu des variables x, rien ne serait changé au raisonnement lui-même, comme on s'en assure facilement; les variétés obtenues seraient du même ordre; seulement l'énoncé de chaque transformation serait beaucoup plus long, puisque toujours des fonctions linéaires, à coefficients entiers, des éléments considérés remplaceraient chacun de ces éléments.

Pour trouver de même toutes les valeurs de la variable y_{n-i}, $[i = 1, 2, \ldots, (n-1)]$ pouvant vérifier simultanément les équations $G_k = 0$, $(k = 1, 2, \ldots, m)$, nous opérons d'une façon tout à fait analogue. Seulement au lieu de substituer à toutes les indéterminées $u_1, u_2, \ldots, u_{n-1}, v_1, v_2, \ldots, v_{n-2}, \ldots\ldots, w_1$, la valeur zéro, nous excepterons u_{n-i} que nous remplacerons par l'unité. Alors toutes les expressions $y, y', y'', \ldots, y^{(n-1)}$ seront remplacés par $y_{n-i} + y_n$; nous considérerons tous les résultants comme fonctions de cette variable, $y_{n-i} + y_n$, ce que nous indiquerons en les affectant de l'indice supérieur $(n - i)$. Sauf cet indice supérieur rien n'est changé au raisonnement précédent. Donc, toutes les valeurs de y_{n-i} qui vérifient simultanément les équations $G_1 = 0$, $G_2 = 0, \ldots, G_m = 0$ sont nécessairement telles que $y_{n-i} + y_n$ soit racine de l'une des équations $R_k^{(n-i)} = 0$, $(k = 1, 2, \ldots, n)$. En rapprochant ce résultat du précédent nous obtenons toutes les valeurs cherchées de y_{n-i}; elles sont fonctions algébriques d'un nombre de variables indépendantes qui dépend de l'indice k de la fonction $R_k^{(n-i)}$ dont $y_{n-i} + y_n$ est racine. Tout ceci a lieu pour $i = 1, 2, \ldots, (n-1)$.

En résumé, tous les systèmes de valeurs qui vérifient simultanément les équations

$$G_1(y_1, y_2, \ldots, y_n) = 0,\ G_2(y_1, y_2, \ldots, y_n) = 0, \ldots\ldots, G_m(y_1, y_2, \ldots, y_n) = 0,$$

se composent 1° de fonctions algébriques d'un certain nombre de variables $y_1, y_2, \ldots, y_n$ et des éléments du domaine de rationalité donné; 2° de ces variables elles-mêmes qui restent indépendantes. Les fonctions algébriques dont nous parlons sont toutes comprises parmi les racines des équations

$$R_k^{(n-i)} = 0 \qquad \begin{pmatrix} i=0,1,2,\ldots,(n-1) \\ k=1,2,\ldots,n \end{pmatrix}$$

de manière qu'à chaque valeur de i corresponde spécialement un des indices de y. Le nombre de variables restant indépendantes dépend de l'indice k; il est toujours égal à $n - k$, de sorte que pour $k = n$, il est nul.

3. C'est ainsi que l'on peut trouver sans aucun artifice tous les systèmes possibles vérifiant simultanément les équations

$$G_1 = 0, \; G_2 = 0, \; \ldots, \; G_m = 0.$$

Mais ces systèmes se présentent sans aucun ordre et les solutions obtenues ne nous donnent, par suite, aucune vue sérieuse sur les restrictions apportées par les équations $G_1 = 0$, $G_2 = 0$, ..., $G_m = 0$ à la variabilité des quantités essentiellement variables $y_1, y_2, \ldots, y_n$. Or c'est précisément dans l'étude de ces restrictions que consiste la théorie générale de l'élimination. Il nous faut donc chercher une autre solution et c'est ici que les quantités indéterminées $u_1, u_2, \ldots, u_n$ viennent s'imposer tout naturellement à notre attention.

Le résultat obtenu jusqu'ici n'est cependant pas inutile. Il était au contraire nécessaire de l'obtenir tout d'abord et nous en ferons usage dans un instant.

Reprenons tout à fait le même raisonnement que tout à l'heure; mais en faisant cette fois-ci, comme il a été indiqué plus haut, les substitutions linéaires à coefficients indéterminés.

Considérons chaque résolvant R_h, $(h = 1, 2, \ldots, n)$ que nous obtenons ainsi comme une fonction de $y^{(h-1)}$ seulement ce qui revient à joindre les autres variables $y_1, y_2, \ldots, y_{n-h}$, au domaine de rationalité donné. Soit alors $\eta^{(h-1)}$ une quelconque des racines de l'équation $R_h = 0$. Nous allons démontrer qu'à chaque valeur $\eta^{(h-1)}$ correspondent des valeurs de

$$y_n, \; y_{n-1}, \; \ldots, \; y_{n-h-1}$$

qui sont fonctions algébriques de $y_1, y_2, \ldots, y_{n-h}$, et vérifient simultanément les équations $G_1 = 0$, $G_2 = 0$, ..., $G_m = 0$.

Comme, par définition,

$$R_h(\eta^{(h-1)}, \; y_1, \; y_2, \; \ldots, \; y_{n-h}; \; u_1, \; u_2, \; \ldots, \; u_n; \; u'_1, \; u'_2, \; \ldots, \; u'_{n-2}; \; \ldots$$
$$\ldots; \; u_1^{(h-1)}, \; u_2^{(h-1)}, \; \ldots, \; u_{n-h}^{(h-1)}) = 0$$

nous avons aussi

$$K_i^{(h-1)}(\eta^{(h-1)}, y_1, y_2, \ldots, y_{n-h}; u_1, u_2, \ldots, u_n; u'_1, u'_2, \ldots, u'_{n-2}; \ldots$$
$$\ldots; u_1^{(h-1)}, u_2^{(h-1)}, \ldots, u_{n-h}^{(h-1)}) = 0 \qquad (i=1, 2, \ldots, m_{h-1})$$

donc

$$s_i^{(h-1)}(\eta^{(h-1)} - t_1^{(h-1)}y_1 - t_2^{(h-1)}y_2 - \ldots - t_{n-h}^{(h-1)}y_{n-h}; y_1, y_2, \ldots, y_{n-h};$$
$$u_1, \ldots, u_n; u'_1, \ldots, u'_{n-2}; \ldots\ldots; u_1^{(h-2)}, u_2^{(h-2)}, \ldots, u_{n-h+1}^{(h-2)}) = 0$$
$$(i=1, 2, \ldots, m_{h-1})$$

et, par suite

$$S_{h-1}(\eta^{(h-1)} - t_1^{(h-1)}y_1 - t_2^{(h-1)}y_2 - \ldots - t_{n-h}^{(h-1)}y_{n-h}; y_1, y_2, \ldots, y_{n-h};$$
$$u_1, \ldots, u_n; u'_1, \ldots, u'_{n-2}; \ldots\ldots; u_1^{(h-2)}, u_2^{(h-2)}, \ldots, u_{n-h+1}^{(h-2)}, U^{(k)}, V^{(k)}) = 0$$

quel que soit l'indice k des indéterminées U et V.

Mais alors, d'après la propriété fondamentale des résultants, les deux fonctions

$$\sum_{i=1}^{m_{h-2}} [U_i^{(k)} L_i^{(h-2)}(y^{(h-2)}, y_1, \ldots, y_{n-h+1}; u_1, \ldots, u_n; u'_1, \ldots, u'_{n-2}; \ldots$$
$$\ldots; u_1^{(h-2)}, u_2^{(h-2)}, \ldots, u_{n-h+1}^{(h-2)})]$$

et

$$\sum_{i=1}^{m_{h-2}} [V_i^{(k)} L_i^{(h-2)}(y^{(h-2)}, y_1, \ldots, y_{n-h+1}; u_1, \ldots, u_n; u'_1, \ldots, u'_{n-2}; \ldots$$
$$\ldots; u_1^{(h-2)}, u_2^{(h-2)}, \ldots, u_{n-h+1}^{(h-2)})]$$

dont S_{h-1} est le résultant pris par rapport à y_{n-h+1}, auront pour

$$y^{(h-2)} = \eta^{(h-1)} - t_1^{(h-1)}y_1 - t_2^{(h-1)}y_2 - \ldots - t_{n-h}^{(h-1)}y_{n-h}$$

un diviseur commun en y_{n-h+1}; il y aura donc sûrement une valeur de y_{n-h+1}

$$y_{n-h+1} = \eta_{n-h+1}^{(h-1)}$$

telle que les deux équations

$$\sum_{i=1}^{m_{h-2}} [U_i^{(k)} L_i^{(h-2)}(\eta'^{(h-1)} - t_1^{(h-1)} y_1 - \ldots - t_{n-h}^{(h-1)} y_{n-h},\ y_1,\ y_2,\ \ldots,\ y_{n-h},\ \eta_{n-h+1};$$

$$u_1,\ \ldots,\ u_n;\ u_1',\ \ldots,\ u_{n-2}';\ \ldots\ldots;\ u_1^{(h-2)},\ u_2^{(h-2)},\ \ldots,\ u_{n-h+1}^{(h-2)})] = 0$$

$$\sum_{i=1}^{m_{h-2}} [V_i^{(k)} L_i^{(h-2)}(\eta^{(h-1)} - t_1^{(h-1)} y_1 - \ldots - t_{n-h}^{(h-1)} y_{n-h},\ y_1,\ y_2,\ \ldots,\ y_{n-h},\ \eta_{n-h+1};$$

$$u_1,\ \ldots,\ u_n;\ u_1',\ \ldots,\ u_{n-2}';\ \ldots\ldots;\ u_1^{(h-2)},\ u_2^{(h-2)},\ \ldots,\ u_{n-h+1}^{(h-2)})] = 0$$

soient vérifiées. En donnant à l'entier k un nombre assez grand de valeurs, nous voyons que les équations

$$L_i^{(h-2)}(\eta^{(h-1)} - t_1^{(h-1)} y_1 - \ldots - t_{n-h}^{(h-1)} y_{n-h},\ y_1,\ y_2,\ \ldots,\ y_{n-h},\ \eta_{n-h+1};$$

$$u_1,\ \ldots,\ u_n,\ u_1',\ \ldots,\ u_{n-2}',\ \ldots\ldots,\ u_1^{(h-2)},\ \ldots,\ u_{n-h+1}^{(h-2)}) = 0 \qquad (i=1,2,\ldots,m_{h-2})$$

sont elles-mêmes vérifiées. Mais alors il en est de même des équations

$$K_i^{(h-2)}(y^{(h-1)} - t_1^{(h-1)} y_1 - \ldots - t_{n-1}^{(h-1)} y_{n-h},\ y_1,\ y_2,\ \ldots,\ y_{n-h},\ y_{n-h+1};$$

$$u_1,\ \ldots,\ u_n,\ \ldots\ldots,\ u_1^{(h-2)},\ \ldots,\ u_{n-h+1}^{(h-2)}) = 0$$

pour $y^{(h-1)} = \eta^{(h-1)}$ et $y_{n-h+1} = \eta_{n-h+1}^{(h-1)}$; donc aussi des équations

$$S_i^{(h-2)}(\eta^{(h-1)} - t_1^{(h-2)} y_1 - \ldots - t_1^{(h-2)} y_{n-h} - t_1^{(h-2)} \eta_{n-h+1}^{(h-1)},\ y_1,\ y_2,\ \ldots,\ y_{n-h},\ \eta_{n-h+1}^{(h-1)};$$

$$u_1,\ \ldots,\ u_n,\ \ldots\ldots,\ u_1^{(h-3)},\ \ldots,\ u_{n-h+2}^{(h-3)}) = 0 \qquad (i=1,2,\ldots,m_{h-2})$$

et, par suite, l'équation

$$S_{h-2}(\eta^{(h-1)} - t_1^{(h-2)} y_1 - \ldots - t_1^{(h-2)} y_{n-h} - t_1^{(h-2)} \eta_{n-h+1}^{(h-1)},\ y_1,\ y_2,\ \ldots,\ y_{n-h},\ \eta_{n-h+1}^{(h-1)};$$

$$u_1,\ \ldots,\ u_n,\ \ldots\ldots,\ u_1^{(h-3)},\ \ldots,\ u_{n-h+2}^{(h-3)},\ U^{(k)},\ V^{(k)}) = 0$$

est elle-même vérifiée quel que soit l'indice k des indéterminées U et V.

S_{h-2} est le résultant, par rapport à y_{n-h+2} des deux fonctions

$$\sum_{i=1}^{m_{h-3}} [U_i^{(k)} L_i^{(h-3)}(y^{(h-3)}, y_1, y_2, \ldots, y_{n-h+2}, u_1, \ldots, u_n, u'_1, \ldots, u'_{n-2}, \ldots \\ \ldots, u_1^{(h-3)}, \ldots, u_{n-h+2}^{(h-3)})]$$

$$\sum_{i=1}^{m_{h-3}} [V_i^{(k)} L_i^{(h-3)}(y^{(h-3)}, y_1, y_2, \ldots, y_{n-h+2}, u_1, \ldots, u_n, u'_1, \ldots, u'_{n-2}, \ldots \\ \ldots, u_1^{(h-3)}, \ldots, u_{n-h+2}^{(h-3)})].$$

Ces deux fonctions s'annuleront donc simultanément pour une valeur au moins de y_{n-h+2}

$$y_{n-h+2} = \eta_{n-h+2}^{(h-1)}$$

$y^{(h-1)}$ et y_{n-h+1} étant respectivement égales à $\eta^{(h-1)}$ et $\eta_{n-h+1}^{(h-1)}$.

En continuant ainsi nous arrivons au résultant S_1 et nous trouvons des systèmes

$$\eta_{n-h+1}^{(h-1)}, \eta_{n-h+2}^{(h-1)}, \ldots, \eta_{n-2}^{(h-1)}$$

vérifiant l'égalité

$$S_1(\eta^{(h-1)} - t'_1 y_1 - t'_2 y_2 - \ldots - t'_{n-h} y_{n-h} - t'_{n-h+1} \eta_{n-h+1}^{(h-1)} - \ldots - t'_{n-2} \eta_{n-2}^{(h-1)}, \\ y_1, y_2, \ldots, y_{n-h}, \eta_{n-h+1}^{(h-1)}, \ldots, \eta_{n-2}^{(h-1)}, u_1, \ldots, u_n, U^{(k)}, V^{(k)}) = 0;$$

S_1 est le résultant, pris par rapport à y_{n-1}, des deux fonctions

$$\sum_{i=1}^{m} U_i^{(k)} L_i(y, y_1, \ldots, y_{n-2}, y_{n-1}; u_1, \ldots, u_n)$$

$$\sum_{i=1}^{m} V_i^{(k)} L_i(y, y_1, \ldots, y_{n-2}, y_{n-1}; u_1, \ldots, u_n).$$

Ces deux fonctions s'annuleront donc simultanément pour une valeur au moins de y_{n-1}

$$y_{n-1} = \eta_{n-1}^{(h-1)}$$

à condition que

$$y_{n-h+1}, y_{n-h+2}, \ldots, y_{n-2}$$

soient déjà remplacées par leurs valeurs respectives

$$\eta_{n-h+1}^{(h-1)},\ \eta_{n-h+2}^{(h-1)},\ \ldots,\ \eta_{n-2}^{(h-1)}.$$

Nous en concluons que les équations

$$L_i(\eta^{(h-1)} - t'_1y_1 - t'_2y_2 - \ldots - t'_{n-h}y_{n-h} - t'_{n-h+1}\eta_{n-h+1}^{(h-1)} - \ldots - t'_{n-2}\eta_{n-2}^{(h-1)},$$

$$y_1,\ y_2,\ \ldots,\ y_{n-h},\ \eta_{n-h+1}^{(h-1)},\ \eta_{n-h+2}^{(h-1)},\ \ldots,\ \eta_{n-2}^{(h-1)},\ \eta_{n-1}^{(h-1)},\ u_1,\ \ldots,\ u_n) = 0$$

sont vérifiées simultanément, et que, par suite, les fonctions

$$K_i(y,\ y_1,\ y_2,\ \ldots,\ y_{n-1},\ u_1,\ u_2,\ \ldots,\ u_n) \qquad (i=1,2,\ldots,m)$$

s'annulent simultanément pour

$$y = \eta^{(h-1)} - t'_1y_1 - t'_2y_2 - \ldots - t'_{n-2}y_{n-2};$$

$$y_{n-h+1} = \eta_{n-h+1}^{(h-1)};\ y_{n-h+2} = \eta_{n-h+2}^{(h-1)};\ \ldots;\ y_{n-1} = \eta_{n-1}^{(h-1)}.$$

Mais

$$y = u_1y_1 + u_2y_2 + \ldots + u_{n-1}y_{n-1} + u_ny_n,$$

et, en faisant cette substitution, les fonctions K_i se transforment en G_i, $(i = 1, 2, \ldots, m)$. Nous avons donc aussi

$$G_i(y_1,\ y_2,\ \ldots,\ y_{n-1},\ y_n) = 0 \qquad (i=1,2,\ldots,m)$$

pour

$$y_{n-h+1} = \eta_{n-h+1}^{(h-1)},\ y_{n-h+2} = \eta_{n-h+2}^{(h-1)},\ \ldots,\ y_{n-1} = \eta_{n-1}^{(h-1)},$$

et

$$u_1y_1 + u_2y_2 + \ldots + u_{n-1}y_{n-1} + y_n = \eta^{(h-1)} - t'_1y_1 - t'_2y_2 - \ldots - t'_{n-2}y_{n-2},$$

c'est à dire

$$y_n = \eta^{(h-1)} - t_1y_1 - t_2y_2 - \ldots - t_{n-h}y_{n-h} - t_{n-h+1}\eta_{n-h+1}^{(h-1)} - t_{n-h+2}\eta_{n-h+2}^{(h-1)} - \ldots$$

$$\ldots - t_{n-1}\eta_{n-1}^{(h-1)};\qquad t_{n-1} = u_{n-1}.$$

En désignant cette valeur de y_n qui est, comme η_{n-h+1}, η_{n-h+2}, $\ldots$, et η_{n-1}, fonction algébrique de $y_1, y_2, \ldots, y_{n-h}$, par $\eta_n^{(h-1)}$, nous pouvons aussi énoncer le résultat obtenu en disant que pour

$$y^{(h-1)} = t_1 y_1 + t_2 y_2 + \ldots + t_{n-h} y_{n-h} + t_{n-h+1} \eta_{n-h+1}^{(h-1)} + t_{n-h+2} \eta_{n-h+2}^{(h-1)} + \ldots$$
$$\ldots + u_{n-1} \eta_{n-1}^{(h-1)} + u_n \eta_n^{(h-1)}$$

le résolvant

$$R_h(y^{(h-1)}, y_1, y_2, \ldots, y_{n-h}, u_1, \ldots, u_n, \ldots, u_1^{(h-1)}, \ldots, u_{n-h}^{(h-1)})$$

s'annule, tandis que les équations

$$G_i(y_1, y_2, \ldots, y_{n-h}, \eta_{n-h+1}^{(h-1)}, \eta_{n-h+2}^{(h-1)}, \ldots, \eta_n^{(h-1)}) = 0 \quad (i = 1, 2, \ldots, m)$$

sont vérifiées simultanément.

Mais nous avons vu, plus haut, que, pour $y_1, y_2, \ldots, y_{n-h}$ variables, *toutes* les valeurs $\eta_{n-h+1}^{(h-1)}, \eta_{n-h+2}^{(h-1)}, \ldots, \eta_n^{(h-1)}$ vérifiant simultanément les équations

$$G_i(y_1, y_2, \ldots, y_{n-h}, \eta_{n-h+1}^{(h-1)}, \eta_{n-h+2}^{(h-1)}, \ldots, \eta_n^{(n-1)}) = 0 \quad (i = 1, 2, \ldots, m)$$

sont telles que $\eta_{n-h+1}^{(h-1)} + \eta_n^{(h-1)}, \eta_{n-h+2}^{(h-1)} + \eta_n^{(h-1)}, \ldots, \eta_{n-1}^{(h-1)} + \eta_n^{(h-1)}$ et $\eta_n^{(h-1}$ vérifient respectivement les équations

$$R_h^{(n-h+1)} = 0, \; R_h^{(n-h+2)} = 0, \; \ldots, \; R_h^{(n-1)} = 0, \; R_h^{(n)} = 0;$$

toutes ces valeurs $\eta_{n-h+1}^{(h-1)}, \eta_{n-h+2}^{(h-1)}, \ldots, \eta_{n-1}^{(h-1)}, \eta_n^{(h-1)}$, sont, par suite, *indépendantes* des indéterminées $u_1, \ldots$ considérées, et seulement fonctions algébriques de $y_1, y_2, \ldots, y_{n-h}$. Tout ceci a lieu pour $h = 1, 2, \ldots, n$.

D'autre part, comme l'équation résolvante

$$R_1 . R_2 . R_3 \ldots R_n = 0$$

représente exactement les mêmes restrictions apportées à la variabilité de $y_1, y_2, \ldots, y_n$ que les équations

$$G_1 = 0, \; G_2 = 0, \; \ldots, \; G_m = 0$$

chaque système vérifiant simultanément les équations données, doit aussi vérifier l'une ou l'autre des résolvantes $R_h = 0$, $(h = 1, 2, \ldots, n)$.

Donc les systèmes $\eta_{n-h+1}^{(h-1)}, \eta_{n-h+2}^{(h-1)}, \ldots, \eta_{n-1}^{(h-1)}, \eta_n^{(h-1)}$, correspondant à chacune des racines $\eta^{(h-1)}$ de l'équation $R_h = 0$, pour $h = 1, 2, \ldots, n$,

et ces systèmes seulement, vérifient simultanément les équations $G_1 = 0$, $G_2 = 0, \ldots, G_m = 0$. De plus, nous savons maintenant que les éléments de ces systèmes ne sont pas fonctions algébriques des variables qui restent indépendantes et des indéterminées introduites pour résoudre plus symétriquement le problème proposé, mais sont, au contraire, seulement fonctions algébriques des variables qui restent indépendantes.

Nous avons ainsi, comme tout à l'heure, trouvé *toutes* les valeurs de $y_1, y_2, \ldots, y_n$ vérifiant les équations proposées. Mais tandis que sans l'emploi des indéterminées nous ne savions pas comment ces valeurs se groupaient en systèmes, nous obtenons, à l'aide des indéterminées, simultanément les valeurs correspondantes de $y_1, y_2, \ldots, y_n$. Elles nous sont données toutes à la fois par les racines des équations résolvantes $R_h = 0$. A chacune de ces équations répond un nombre différent de variables qui restent indépendantes et, par suite, une variété différente vérifiant le système proposé.

Comme les résolvantes peuvent être mises sous la forme

$$R_1(y, y_1, \ldots, y_{n-1}, u_1, u_2, \ldots, u_n) = \prod_{(i)}(y - \eta_{0i})$$

$$= \prod_{(i)}(y - u_1 y_1 - u_2 y_2 - \ldots - u_{n-1} y_{n-1} - u_n \eta_{ni}) = 0$$

$$R_2(y', y_1, \ldots, y_{n-2}, u_1, \ldots, u_n, u'_1, \ldots, u'_{n-2}) = \prod_{(i)}(y' - \eta'_{0i})$$

$$= \prod_{(i)}(y' - u'_1 y_1 - u'_2 y_2 - \ldots - u'_{n-2} y_{n-2} - u_{n-1}\eta'_{n-1,i} - u_n \eta'_{ni}) = 0$$

et, en général, comme

$$R_h(y^{(h-1)}, y_1, \ldots, y_{n-h}, u_1, \ldots, u_n, \ldots, u_1^{(h-1)}, \ldots, u_{n-h}^{(h-1)}) = \prod_{(i)}(y^{(h-1)} - \eta_{0i}^{(h-1)})$$

$$= \prod_{(i)}(y^{(h-1)} - u_1^{(h-1)} y_1 - \ldots - u_{n-h}^{(h-1)} y_{n-h} - u_{n-h+1}^{(h-2)} \eta_{n-h+1,i}^{(h-1)} - \ldots - u_n \eta_{ni}^{(h-1)}) = 0$$

$$(h = 1, 2, \ldots, n),$$

nous voyons que chacune de ces résolvantes dépend, au plus, de n indéterminées. Dans toutes les fonctions réunies $R_1, R_2, \ldots, R_n$ ne paraissent même que les n indéterminées $u_1^{(n-2)}, u_2^{(n-3)}, \ldots, u'_{n-2}, u_{n-1}, u_n$; on pourrait donc, dès le début, n'introduire qu'un seul système d'indé-

terminées, au lieu de $(n-1)$ systèmes; cependant je crois plus naturel d'opérer comme je l'ai fait.

Nous voyons aussi que, considérée comme une fonction des indéterminées qui y paraissent, la forme R_h est décomposable en facteurs linéaires dont les coefficients sont fonctions algébriques de $y_1, y_2, \ldots, y_{n-h}$ seulement. Nous allons, dans un instant, faire usage de ce résultat important.

En résumé, si l'on nous donne un système quelconque d'équations algébriques reliant un nombre également quelconque de variables et si l'on nous demande de déterminer les différentes variétés vérifiant ce système, nous formerons d'abord l'équation résolvante en égalant à zéro le résolvant total débarassé de ses facteurs multiples. A chacune des résolvantes partielles correspond une variété d'ordre différent répondant au problème. Cet ordre de variété n'est pas représenté lorsque le résolvant correspondant est égal à l'unité. Dans le cas contraire, pour obtenir les systèmes composant cette variété, nous considérerons le résolvant partiel correspondant comme une fonction des n indéterminées qui y paraissent et nous le décomposerons en ses facteurs linéaires. Nous obtiendrons ainsi, en remplaçant dans l'expression précédente de R_h, $y^{(h-1)}$ par sa valeur $u_1^{(h-1)}y_1 + u_2^{(h-1)}y_2 + \ldots + u_{n-1}y_{n-1} + u_n y_n$

$$R_h(y^{(h-1)}, y_1, \ldots, y_{n-h}, u_1^{(h-1)}, \ldots, u_n)$$

$$= \prod_{(i)} \left\{ u_{n-h+1}^{(h-2)}\left(y_{n-h+1} - \eta_{n-h+1,i}^{(h-1)}\right) + u_{n-h+2}^{(h-3)}\left(y_{n-h+2} - \eta_{n-h+2,i}^{(h-1)}\right) + \ldots + u_n\left(y_n - \eta_{n,i}^{(h-1)}\right)\right\} = 0.$$

Pour chaque valeur déterminée de i, nous avons donc

$$u_{n-h+1}^{(h-2)}\left(y_{n-h+1} - \eta_{n-h+1,i}^{(h-1)}\right) + u_{n-h+2}^{(h-3)}\left(y_{n-h+2} - \eta_{n-h+2,i}^{(h-1)}\right) + \ldots + u_n\left(y_n - \eta_{n,i}^{(h-1)}\right) = 0$$

et comme les u sont indéterminées

$$y_{n-h+1} = \eta_{n-h+1,i}^{(h-1)}; \qquad y_{n-h+2} = \eta_{n-h+2,i}^{(h-1)}; \quad \ldots; \quad y_n = \eta_{n,i}^{(h-1)}.$$

Toutes ces expressions sont fonctions algébriques de $y_1, y_2, \ldots, y_{n-h}$. Celles qui correspondent à une même valeur de i, vérifient simultanément les équations données, $y_1, y_2, \ldots, y_{n-h}$ restant indéterminées.

En donnant à h successivement les valeurs 1, 2, ..., n, nous obtenons

tous les systèmes vérifiant les équations données, et simultanément les valeurs correspondantes des éléments de ces systèmes.

§ 2.

De la représentation générale des systèmes d'équations.

Nous allons maintenant considérer séparément chacun des résolvants $R_1, R_2, \ldots, R_n$. Il n'y aura donc aucun inconvénient à laisser aussi de côté, pour simplifier l'écriture, les indices supérieurs de toutes les variables et des indéterminées.

La décomposition en ses facteurs linéaires du résolvant R_h considéré comme une fonction des indéterminées u, a lieu identiquement en ces indéterminées; dans chaque facteur linéaire les coefficients ne dépendent pas des u; nous pouvons donc écrire en substituant à $u_1, u_2, \ldots, u_n$, des quantités variables $\lambda_1, \lambda_2, \ldots, \lambda_n$

$$R_h(y, y_1, \ldots, y_{n-h}; \lambda_1, \lambda_2, \ldots, \lambda_n)$$

$$= \prod_{i=1}^{\rho}(y - \eta_{0,i}) = \prod_{i=1}^{\rho}(y - \lambda_1 y_1 - \ldots - \lambda_{n-h} y_{n-h} - \lambda_{n-h+1}\eta_{n-h+1,i} - \ldots - \lambda_n \eta_{n,i}).$$

Pour une valeur déterminée de k comprise entre 0 et $(h-1)$ nous aurons également, en désignant par α une variable auxiliaire

$$R_h(y, y_1, \ldots, y_{n-h}; \lambda_1, \lambda_2, \ldots, \lambda_{n-k-1}, \lambda_{n-k} + \alpha, \lambda_{n-k+1}, \ldots, \lambda_n)$$

$$= \prod_{i=1}^{\rho}(y - \eta_{0,i} - \alpha\eta_{n-k,i})$$

et pour une valeur déterminée de i, $i = j$, c'est à dire pour une racine déterminée $\eta_{0,j}$ de l'équation $R_h(y) = 0$

$$R_h(y - \eta_{0,j}, y_1, \ldots, y_{n-h}; 0, 0, \ldots, 0, \alpha, 0, \ldots, 0) = \prod_{i=1}^{\rho}(y - \eta_{0,j} - \alpha\eta_{n-k,i})$$

la variable α étant au milieu des zéros à la place qu'occupait dans l'égalité précédente $\lambda_{n-k} + \alpha$.

Les deux produits

$$\prod_{i=1}^{\rho}(y - \eta_{0,i} - \alpha\eta_{n-k,i}) \text{ et } \prod_{i=1}^{\rho}(y - \eta_{0,j} - \alpha\eta_{n-k,i})$$

ont un facteur commun $y - \eta_{0,j} - \alpha\eta_{n-k,j}$, c'est à dire

$$y - \lambda_1 y_1 - \lambda_2 y_2 - \ldots - \lambda_{n-h} y_{n-h} - \lambda_{n-h+1}\eta_{n-h+1,j} - \ldots$$
$$\ldots - \lambda_{n-k-1}\eta_{n+k-1,j} - (\lambda_{n-k} + \alpha)\eta_{n-k,j} - \lambda_{n-k+1}\eta_{n-k+1,j} - \ldots - \lambda_n\eta_{n\,j}.$$

Ils n'en ont point d'autres aussi longtemps que les variables $\lambda_1, \lambda_2, \ldots, \lambda_n$ restent indéterminées. Nous pouvons donc toujours(1) trouver des entiers $p_1, p_2, \ldots, p_n$ tels que

$$y - p_1 y_1 - p_2 y_2 - \ldots - p_{n-h} y_{n-h} - p_{n-h+1}\eta_{n-h+1,j} - \ldots$$
$$\ldots - p_{n-k-1}\eta_{n-k-1,j} - (p_{n-k} + \alpha)\eta_{n-k,j} - p_{n-k+1}\eta_{n-k+1,j} - \ldots - p_n\eta_{n,j}$$

soit le plus grand commun diviseur des deux fonctions

$$R_h(y, y_1, \ldots, y_{n-h}, p_1, \ldots, p_{n-k-1}, p_{n-k} + \alpha, p_{n-k+1}, \ldots, p_n)$$

et

$$R_h(y - \zeta_{0,j}, y_1, \ldots, y_{n-h}, 0, \ldots, 0, \alpha, 0, \ldots, 0)$$

où $\zeta_{0,j}$ désigne ce que devient $\eta_{0,j}$ pour les valeurs particulières

$$\lambda_1 = p_1, \qquad \lambda_2 = p_2, \ldots, \lambda_n = p_n$$

c'est à dire une des ρ racines de l'équation

$$R_h(y; y_1, y_2, \ldots, y_{n-h}, p_1, p_2, \ldots, p_n) = 0.$$

Ni $\eta_{n,i}$ qui est racine de l'équation $R_h^{(n)} = 0$, ni $\eta_{n-k,i} + \eta_{n,i}$ qui est racine de l'équation $R_h^{(n-k)} = 0$, ne dépendent de $\lambda_1, \lambda_2, \ldots, \lambda_n$; les $\eta_{n-k,i}$ ne

(1) Comparez page 145.

changent donc pas pour les valeurs particulières p_1 p_2, ..., p_n données à ces variables.

La recherche du plus grand commun diviseur est une opération essentiellement rationnelle; l'expression

$$\zeta_{0,j} + \alpha\eta_{n-k,j}$$

est donc une fonction rationnelle des coëfficients $\zeta_{0,j}$, y_1, y_2, ..., y_{n-h}, α qui paraissent dans les deux fonctions précédentes. Ainsi en donnant à α une valeur convenable, $\eta_{n-k,j}$ est fonction rationnelle de $\zeta_{0,j}$, y_1, y_2, ..., y_{n-h};

$$\eta_{n-k,j} = f_{n-k}(\zeta_{0,j},\ y_1,\ y_2,\ \ldots,\ y_{n-h}).$$

Partageons maintenant les racines $\zeta_{0,j}$ en groupes correspondant aux facteurs irréductibles de $R_h = 0$. Soient

$$T_{h,1},\ T_{h,2},\ \ldots,\ T_{h,\tau}$$

ces facteurs irréductibles, et

$$T_{h,\nu} = \prod_{(k)} (y - \zeta_{0,k}^{(\nu)}). \qquad \begin{pmatrix} k=1,2,\ldots,\rho_\nu \\ \nu=1,2,\ldots,\tau \end{pmatrix}$$

Comme toute fonction rationnelle qui s'annule pour l'une des racines d'une équation irréductible s'annule pour toutes les racines de cette équation nous obtiendrons la même fonction rationnelle f_{n-k} pour toutes les racines correspondant à la même valeur de ν; nous devrons donc écrire

$$\eta_{n-k,j}^{(\nu)} = f_{n-k}^{(\nu)}(\zeta_{0,j}^{(\nu)},\ y_1,\ y_2,\ \ldots,\ y_{n-h}). \qquad \begin{pmatrix} j=1,2,\ldots,\ \rho_\nu \\ \nu=1,2,\ldots,\ \tau \\ k=0,1,\ldots,(h-1) \end{pmatrix}$$

Une transformation déjà donnée par LAGRANGE nous permet ensuite de former facilement une fonction rationnelle qui reste la même non seulement pour toutes les racines de l'un quelconque des facteurs irréductibles de R_h, mais aussi pour toutes les racines de la fonction R_h elle-même. Nous voyons, en effet, qu'en posant

$$F_{n-k}(y, y_1, \ldots, y_{n-h}) = \sum_{(i,j)} f_{n-k}^{(i)}(\zeta_{0,j}^{(i)}, y_1, \ldots, y_{n-h}) \frac{\prod_{(\nu)} T_{h,\nu}(y).\, T_{h,i}(\zeta_{0,j}^{(i)})}{(y - \zeta_{0,j}^{(i)}) D_y T_{h,i}(y)_{y=\zeta_{0,j}^{(i)}} \prod_{(\nu)} T_{h,\nu}(\zeta_{0,j}^{(i)})}$$

$$\begin{pmatrix} \nu=1,2,\ldots,\tau \\ i=1,2,\ldots,\tau \\ j=1,2,\ldots,\rho_i \end{pmatrix}$$

nous avons à la fois

$$F_{n-k}(\zeta_{0,j}^{(i)},\ y_1,\ \ldots,\ y_{n-h}) = f_{n-k}^{(i)}(\zeta_{0,j}^{(i)},\ y_1,\ \ldots,\ y_{n-h})$$

pour $j = 1, 2, \ldots, \rho_i$ et pour $i = 1, 2, \ldots, \tau$, c'est à dire pour toutes les racines de l'équation $R_h = 0$.

Pour $y = \zeta_{0,1}^{(1)}$, par exemple, la fraction

$$\frac{T_{h,1}(\zeta_{0,1}^{(1)})\,T_{h,2}(\zeta_{0,1}^{(1)})\cdots T_{h,\tau}(\zeta_{0,1}^{(1)})}{(\zeta_{0,1}^{(1)}-\zeta_{0,j}^{(1)})D_y T_{h,1}(y)_{y=\zeta_{0,j}^{(1)}}\,T_{h,2}(\zeta_{0,j}^{(1)})\,T_{h,3}(\zeta_{0,j}^{(1)})\cdots T_{h,\tau}(\zeta_{0,j}^{(1)})}$$

se réduit à l'unité pour $j = 1$, et à zéro pour $j = 2, 3, \ldots, \rho_1$; tandis que pour $i > 1$, la fraction

$$\frac{T_{h,1}(\zeta_{0,1}^{(1)})\,T_{h,2}(\zeta_{0,1}^{(1)})\cdots T_{h,\tau}(\zeta_{0,1}^{(1)})}{(\zeta_{0,1}^{(1)}-\zeta_{0,j}^{(i)})D_y T_{h,i}(y)_{y=\zeta_{0,j}^{(i)}}\,T_{h,1}(\zeta_{0,j}^{(i)})\cdots T_{h,i-1}(\zeta_{0,j}^{(i)})\,T_{h,i+1}(\zeta_{0,j}^{(i)})\cdots T_{h,\tau}(\zeta_{0,j}^{(i)})}$$

est nécessairement nulle.

Il en résulte que

$$F_{n-k}(\zeta_{0,1}^{(1)},\ y_1,\ \ldots,\ y_{n-h}) = f_{n-k}^{(1)}(\zeta_{0,1}^{(1)},\ y_1,\ \ldots,\ y_{n-h}).$$

De même pour les autres racines de l'équation $R_h = 0$.

Nous pouvons donc écrire, pour $j = 1, 2, \ldots, \rho$ et $k = 0, 1, \ldots, (h-1)$,

$$\eta_{n-k,j} = F_{n-k}(\zeta_{0,j},\ y_1,\ y_2,\ \ldots,\ y_{n-h})$$

ou encore, en désignant par Φ_{n-k} et Ψ_{n-k} deux fonctions entières

$$\eta_{n-k,j} = \frac{\Phi_{n-k}(\zeta_{0,j},\ y_1,\ y_2,\ \ldots,\ y_{n-h})}{\Psi_{n-k}(\zeta_{0,j},\ y_1,\ y_2,\ \ldots,\ y_{n-h})}.$$

Ainsi pour chaque valeur déterminée de j, les expressions correspondantes

$$\eta_{n-h+1,j},\ \eta_{n-h+2,j},\ \ldots,\ \eta_{n,j}$$

sont fonctions rationnelles de $\zeta_{0,j}$ et des variables arbitraires $y_1, y_2, \ldots, y_{n-h}$, tandis que $\zeta_{0,j}$ est égale à l'une des racines de l'équation résolvante elle-même $R_h(y) = 0$, dans laquelle les indéterminées $u_1, u_2, \ldots, u_n$ sont remplacées par les entiers $p_1, p_2, \ldots, p_n$. Il est d'ailleurs indifférent de

tirer de cette dernière équation la valeur de y en fonction algébrique de $y_1, y_2, \ldots, y_{n-h}$, pour la substituer dans les fonctions $F_{n-k}(y, y_1, \ldots, y_{n-h})$ comme nous venons de le faire, ou d'en tirer, par exemple, la valeur de y_1 en fonction algébrique de $y, y_2, \ldots, y_{n-h}$ pour la substituer dans ces mêmes fonctions $F_{n-k}(y, y_1, \ldots, y_{n-h})$. De toute manière, le système

$$R_h(y, y_1, \ldots, y_{n-h}, p_1, p_2, \ldots, p_n) = 0$$

$$\eta_{n-k} = F_{n-k}(y, y_1, \ldots, y_{n-h}, p_1, p_2, \ldots, p_n) \qquad (k=0, 1, 2, \ldots, h-1)$$

nous donnera les mêmes solutions que l'équation résolvante

$$R_h(y, y_1, \ldots, y_{n-h}, u_1, u_2, \ldots, u_n) = 0.$$

Une exception se présente toutefois lorsque la fonction rationnelle F_{n-k} est indéterminée. Dans ce cas, nous devons écrire, non pas l'égalité

$$\eta_{n-k} = F_{n-k}(y, y_1, \ldots, y_{n-h}, p_1, p_2, \ldots, p_n)$$

qui n'a aucun sens, mais la suivante

$$\eta_{n-k}\Psi_{n-k}(y, y_1, \ldots, y_{n-h}, p_1, p_2, \ldots, p_n) = \Phi(y, y_1, \ldots, y_{n-h}, p_1, p_2, \ldots, p_n)$$

qui est alors vérifiée quelles que soient les valeurs données à η_{n-k}.

Si donc, pour mettre en évidence que les indéterminées u sont remplacées par les entiers p, nous posons

$$p_1y_1 + p_2y_2 + \ldots + p_ny_n = z_0$$

et si, d'autre part, pour écrire plus symétriquement nos formules, nous convenons d'entendre par $F_1, F_2, \ldots, F_{n-h}$ les variables $y_1 = z_1$, $y_2 = z_2, \ldots, y_{n-h} = z_{n-h}$ elles-mêmes, de sorte que

$$y_i = z_i = F_i(z_0, z_1, z_2, \ldots, z_{n-h}), \qquad (i=1, 2, \ldots, n-h)$$

nous pouvons dire que la résolvante de rang h, du système donné

$$[G_1(y_1, y_2, \ldots, y_n) = 0,\ G_2(y_1, y_2, \ldots, y_n) = 0, \ldots, G_m(y_1, y_2, \ldots, y_n) = 0]$$

est équivalente au système

$$(I)\qquad \begin{cases} R_h(z_0,\ z_1,\ \ldots,\ z_{n-h}) = 0 \\ y_k = F_k(z_0,\ z_1,\ \ldots,\ z_{n-h}) \qquad (k=1,\ 2,\ \ldots,\ n) \\ \prod\limits_{(k)} \Psi_k(z_0,\ z_1,\ \ldots,\ z_{n-h}) \gtrless 0. \end{cases}$$

La première équation de ce système représente déjà une variété $(n-h)^{\text{ième}}$ prise dans la variété $(n-h+1)^{\text{ième}}$ qui est formée par les variables $z_0,\ z_1,\ \ldots,\ z_{n-h}$. Les autres équations nous donnent les valeurs des n variables $y_1,\ y_2,\ \ldots,\ y_n$, en fonctions rationnelles des éléments de la variété $(n-h)^{\text{ième}}$ dont nous venons de parler, pourvu que l'inégalité $\prod\limits_{(k)} \Psi_k(z_0,\ z_1,\ \ldots,\ z_{n-h}) \gtrless 0$ soit vérifiée. C'est pourquoi nous pouvons aussi dire que la variété $(n-h)^{\text{ième}}$ prise dans la variété $(n-h+1)^{\text{ième}}$ formée par les variables $z_0,\ z_1,\ \ldots,\ z_{n-h}$, et définie par le système (I) est une *figuration* de la variété $(n-h)^{\text{ième}}$ contenu dans le système donné.

Le système

$$\begin{cases} R_h(z_0,\ z_1,\ \ldots,\ z_{n-h}) = 0 \\ y_k = F_k(z_0,\ z_1,\ \ldots,\ z_{n-h}) \qquad (k=1,\ 2,\ \ldots,\ n) \end{cases}$$

qui contient $(n+1)$ relations entre $(2n-h+1)$ variables, représente outre la variété $(n-h)^{\text{ième}}$

$$R_h(y,\ y_1,\ \ldots,\ y_n,\ u_1,\ \ldots,\ u_n) = 0$$

des variétés différentes répondant aux solutions où

$$\Phi_k(z_0,\ z_1,\ \ldots,\ z_{n-h}) = \Psi_k(z_0,\ z_1,\ \ldots,\ z_{n-h}) = 0$$

et où y_k est *indéterminée*. Il est donc tout à fait indispensable d'ajouter aux $(n+1)$ égalités précédentes, l'inégalité

$$\prod_{(k)} \Psi_k(z_0,\ z_1,\ \ldots,\ z_{n-h}) \gtrless 0$$

pour avoir une variété ne figurant que la variété considérée d'ordre $(n-h)$.

On peut toujours former une infinité de systèmes d'entiers $p_1^{(i)}$, $p_2^{(i)}$, $\ldots$, $p_n^{(i)}$, tels que

$$y - p_1^{(i)} y_1 - p_2^{(i)} y - \ldots - p_{n-h}^{(i)} y_{n-h} - p_{n-h+1}^{(i)} \eta_{n-h+1,j} - \ldots$$

$$\ldots - p_{n-k-1}^{(i)} \eta_{n-k-1,j} - (p_{n-k}^{(i)} + \alpha)\eta_{n-k,j} - p_{n-k+1}^{(i)} \eta_{n-k+1,j} - \ldots - p_n^{(i)} \eta_{n,j}$$

soit le plus grand commun diviseur des deux fonctions

$$R_h(y, y_1, \ldots, y_{n-h}, p_1^{(i)}, \ldots, p_{n-k-1}^{(i)}, p_{n-k}^{(i)} + \alpha, p_{n-k+1}^{(i)}, \ldots, p_n^{(i)})$$

et

$$R_h(y - \zeta_{0,j}^{(i)}, y_1, y_2, \ldots, y_{n-h}, 0, \ldots, 0, \alpha, 0, \ldots, 0)$$

où $\zeta_{0,j}^{(i)}$ désigne une des racines de l'équation

$$R_h(y; y_1, y_2, \ldots, y_{n-h}, p_1^{(i)}, p_2^{(i)}, \ldots, p_n^{(i)}) = 0.$$

Si nous avions substitué aux indéterminées $u_1, u_2, \ldots, u_n$, un de ces systèmes $p_1^{(i)}, p_2^{(i)}, \ldots, p_n^{(i)}$, nous aurions obtenu une figuration différente de la variété $(n-h)^{\text{ième}}$ contenue dans le système d'équations

$$(G_1 = 0, G_2 = 0, \ldots, G_m = 0).$$

Au lieu de $z_0 = p_1 y_1 + p_2 y_2 + \ldots + p_n y_n$, nous aurions introduit une variable

$$z_0^{(i)} = p_1^{(i)} y_1 + p_2^{(i)} y_2 + \ldots + p_n^{(i)} y_n$$

et nous aurions posé

$$y_k = z_k^{(i)} = F_k(z_0^{(i)}, z_1^{(i)}, \ldots, z_{n-h}^{(i)}); \qquad (k=1, 2, \ldots, n-h)$$

alors la figuration cherchée se serait présentée sous la forme (I) tous les z étant affectés de l'indice supérieur i.

Mais les variables $z^{(i)}$ et y sont manifestement fonctions rationnelles les unes des autres, de même que les variables z et y. Les variables $z^{(i)}$ et z sont donc, elles-mêmes, *fonctions rationnelles les unes des autres*, ce que nous exprimerons en disant, d'après RIEMANN, que les équations $R_h(z_0^{(i)}, z_1^{(i)}, \ldots, z_{n-h}^{(i)}) = 0$ font partie de la même *classe*. Il est indifférent de considérer l'un ou l'autre des individus d'une même classe. Parmi

ces individus sont nécessairement compris ceux que nous obtenons en soumettant les coefficients $p_1^{(i)}, p_2^{(i)}, \ldots, p_n^{(i)}$, à des équations de condition déterminées, pourvu que ces équations ne soient pas en contradiction avec l'inégalité à laquelle doivent satisfaire $p_1^{(i)}, p_2^{(i)}, \ldots, p_n^{(i)}$ et dont nous parlions plus haut; cette remarque peut être utile dans chaque cas particulier donné.

Le résultat obtenu est résumé dans la proposition suivante.

»*Toute variété* $k^{ième}$, *prise dans une variété* $n^{ième}$, *peut être figurée par une variété* $k^{ième}$, *prise dans une variété* $(k+1)^{ième}$, — *par un variété dont le résolvant est, par suite, de rang un; — et cette dernière variété* $k^{ième}$ *peut être choisie arbitrairement parmi tous les individus faisant partie d'une classe déterminée.*»

La figuration d'une variété quelconque, que nous venons de considérer, est tout à fait remarquable. Elle nous donne une vue plus complète sur les dépendances des solutions simultanées du problème, et met en évidence pourquoi finalement la notion de fonction algébrique donnée par un système de fonctions entières égalées à zéro, se réduit à celle donnée par une seule fonction entière égalée à zéro. Quoique cette figuration contienne une inégalité, elle a donc une grande importance. C'est pourquoi il semble bon de lui donner un nom. Je la nommerai *figuration principale* de la variété qu'elle représente.

§ 3.

De la réductibilité des systèmes de fonctions entières.

Nous allons maintenant chercher à résoudre le problème fondamental de la réductibilité des systèmes de fonctions entières.

Il faut avant tout définir ce que l'on veut entendre par système réductible ou irréductible. Comme un système d'équations est entièrement équivalent à sa résolvante, il est naturel, comme dans le cas de deux variables, de nommer réductible tout système d'équations dont le résolvant total se compose de plusieurs résolvants partiels, parce que ce système est

alors vérifié par plusieurs variétés différentes. Il est tout aussi naturel de nommer réductible un système dont le résolvant se compose d'un résolvant partiel qui est, lui-même, décomposable en facteurs dans le domaine de rationalité considéré. Au contraire, lorsque dans un domaine de rationalité donné, le résolvant d'un système ne se compose que d'un seul facteur irréductible, nous dirons que, dans ce domaine, le système est, lui aussi, irréductible.

Le premier théorème que nous démontrerons est tout à fait analogue à celui qui a lieu pour une fonction d'une variable, et légitime ainsi notre définition. Voici ce théorème.

Si une fonction rationnelle de $y_1, y_2, \ldots, y_n$

$$\theta(y_1, y_2, \ldots, y_n)$$

s'annule pour *un* système quelconque de h fonctions algébriques $\eta^{(1)}_{n-h+1}$, $\eta^{(1)}_{n-h+2}, \ldots, \eta^{(1)}_n$ des variables $y_1, y_2, \ldots, y_{n-h}$, vérifiant un système *irréductible* d'équations

$$G_1(y_1, y_2, \ldots, y_n) = 0,\ G_2(y_1, y_2, \ldots, y_n) = 0, \ldots, G_m(y_1, y_2, \ldots, y_n) = 0,$$

elle s'annule pour *tous* les autres systèmes de h fonctions algébriques $\eta^{(i)}_{n-h+1}, \eta^{(i)}_{n-h+2}, \ldots, \eta^{(i)}_n$ de $y_1, y_2, \ldots, y_{n-h}$, $(i = 2, 3, \ldots, \rho)$ vérifiant ce même système d'équations.

En effet, comme le résolvant d'un système irréductible ne se compose que d'un seul facteur R_h, ce système de rang h peut être figuré par le suivant, de rang *un*,

$$R_h(z_0, y_1, \ldots, y_{n-h}) = 0$$

$$y_k = F_k(z_0, y_1, \ldots, y_{n-h})$$

$$\prod_{(k)} \Psi_k(z_0, y_1, \ldots, y_{n-h}) \gtrless 0$$

où $R_h(z_0)$ s'annule pour toutes les valeurs de z_0

$$\zeta_0^{(i)} = p_1 y_1 + \ldots + p_{n-h} y_{n-h} + p_{n-h+1}\eta^{(i)}_{n-h+1} + \ldots + p_n \eta^{(i)}_n. \qquad (i=1, 2, \ldots, \rho)$$

De plus, comme le résolvant d'un système irréductible doit être lui-même

irréductible, nous pourrons toujours déterminer les entiers $p_1, p_2, \ldots, p_n$ de manière que l'expression

$$R_h(z_0, y_1, \ldots, y_{n-h})$$

soit, elle aussi, irréductible. Il va de soi que la condition du paragraphe précédent, que $R_h(z_0, z_1, \ldots, z_{n-h})$ n'ait pas de facteurs doubles, est alors vérifiée d'elle-même.

Comme, par hypothèse,

$$\theta(y_1, y_2, \ldots, y_{n-h}, \eta_{n-h+1}^{(1)}, \ldots, \eta_n^{(1)}) = 0$$

nous avons aussi

$$\theta[y_1, y_2, \ldots, y_{n-h}, F_{n-h+1}(\zeta_0^{(1)}, y_1, \ldots, y_{n-h}), \ldots, F_n(\zeta_0^{(1)}, y_1, \ldots, y_{n-h})]$$
$$= H(\zeta_0^{(1)}, y_1, \ldots, y_{n-h}) = 0.$$

Mais alors, $y_1, y_2, \ldots, y_{n-h}$ restant indéterminées, la fonction rationnelle de z_0

$$H(z_0; y_1, \ldots, y_{n-h})$$

s'annule pour l'une des racines de l'équation irréductible $R_h(z_0) = 0$; d'après un théorème connu, elle s'annulera donc pour *toutes* les racines $\zeta_0^{(i)}$, $(i = 1, 2, \ldots, \rho)$ de cette équation, et nous aurons

$$\theta[y_1, y_2, \ldots, y_{n-h}, F_{n-h+1}(\zeta_0^{(i)}, y_1, \ldots, y_{n-h}), \ldots, F_n(\zeta_0^{(i)}, y_1 \ldots, y_{n-h})] = 0$$

pour $i = 1, 2, \ldots, \rho$. Il en résulte immédiatement que la fonction rationnelle

$$\theta(y_1, y_2, \ldots, y_n)$$

s'annule pour tous les systèmes $y_{n-h+1} = \eta_{n-h+1}^{(i)}, \ldots, y_n = \eta_n^{(i)}$, vérifiant le système irréductible d'équations

$$G_1(y_1, y_2, \ldots, y_n) = 0, \; G_2(y_1, y_2, \ldots, y_n) = 0, \ldots, \; G_m(y_1, y_2, \ldots, y_n) = 0.$$

Inversement, si nous pouvons démontrer que *toute* fonction rationnelle qui s'annule pour un système de valeurs $(y_1, y_2, \ldots, y_{n-h}, \eta_{n-h+1}^{(1)}, \ldots, \eta_n^{(1)})$, vérifiant un système d'équations données, s'annule également pour tous les autres systèmes de valeurs $(y_1, y_2, \ldots, y_{n-h}, \eta_{n-h+1}^{(i)}, \ldots, \eta_n^{(i)})$, véri-

fiant le même système d'équations, nous pouvons en conclure que ce système d'équations est irréductible.

Soit, en effet, $R = 0$, la résolvante de ce système. La fonction R s'annule pour $y_{n-h+1} = \eta^{(i)}_{n-h+1}, \ldots, y_n = \eta^{(i)}_n$; si donc elle était réductible, et si $R = S.T$ il y aurait une équation $S = 0$, ou $T = 0$ qui étant vérifiée pour un système de valeurs $(y_1, y_2, \ldots, y_{n-h}, \eta_{n-h+1}, \ldots, \eta_n)$, ne le serait pas pour tous, contrairement à l'hypothèse. Ainsi l'équation $R = 0$, et, par suite, le système d'équations données est irréductible.

Cette propriété étant nécessaire et suffisante pourrait être donnée comme *définition* de l'irréductibilité d'un système d'équations.

Le problème de la décomposition d'un système d'équations quelconques en systèmes irréductibles peut être maintenant considéré comme résolu en même temps que posé. Soit, en effet, un système donné; nous commencerons par former sa résolvante $R = 0$; nous décomposerons ensuite, dans le domaine de rationalité arbitrairement fixé, la fonction R en ses facteurs irréductibles; à chacun de ces facteurs S_i, égalé à zéro, correspond un système d'équations bien facile à former. Il suffit de développer la fonction irréductible $S_i(u_1 y_1 + \ldots + u_n y_n, y_1, \ldots, y_{n-i}, u_1, \ldots, u_n)$ suivant les puissances des indéterminées $u_1, u_2, \ldots, u_n$, et d'égaler à zéro tous les coefficients

$$\Phi^{(i)}_1(y_1, y_2, \ldots, y_n), \quad \Phi^{(i)}_2(y_1, y_2, \ldots, y_n), \quad \ldots, \quad \Phi^{(i)}_k(y_1, y_2, \ldots, y_n)$$

de ce développement. L'ensemble des équations ainsi formées est certainement équivalent à l'équation $S_i = 0$ elle-même, qui doit être vérifiée indépendamment des indéterminées $u_1, u_2, \ldots, u_n$. En d'autres termes, $S_i = 0$ est identique à l'équation résolvante du système

$$[\Phi^{(i)}_1(y_1, y_2, \ldots, y_n) = 0, \ \Phi^{(i)}_2(y_1, y_2, \ldots, y_n) = 0, \ \ldots, \ \Phi^{(i)}_k(y_1, y_2, \ldots, y_n) = 0].$$

L'ensemble de ces derniers systèmes, formés pour tous les facteurs irréductibles S_i du résolvant R, est équivalent au système donné.

Tout ceci ressort immédiatement de la définition même de l'irréductibilité des systèmes. Mais ce qui est bien remarquable, c'est que l'on puisse toujours former un système irréductible, équivalent au précédent, $(\Phi^{(i)}_1, \Phi^{(i)}_2, \ldots, \Phi^{(i)}_k)$ et composé de $(n + 1)$ éléments seulement. Ce nombre peut se réduire dans chaque cas particulier, mais un seul élément

de plus que le nombre total de variables considérées suffit certainement. Nous allons démontrer ce théorème.

L'équation

$$S_i(y, y_1, y_2, \ldots, y_{n-i}, u_1, u_2, \ldots, u_n) = 0$$

devant être vérifiée identiquement en $u_1, u_2, \ldots, u_n$, sera manifestement vérifiée pour les i systèmes de valeurs suivants donnés à ces indéterminées

$$u_n = 1\,;\ u_1 = u_2 = \ldots = u_{n-1} = 0$$

$$u_{n-1} = u_n = 1\,;\ u_1 = u_2 = \ldots = u_{n-2} = 0$$

$$u_{n-2} = u_n = 1\,;\ u_1 = u_2 = \ldots = u_{n-3} = u_{n-1} = 0$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$u_{n-i+1} = u_n = 1\,;\ u_1 = u_2 = \ldots = u_{n-i} = u_{n-i+2} = \ldots = u_{n-1} = 0.$$

Nous avons ainsi i équations simultanées

$$S_i(y_n;\ y_1, \ldots, y_{n-i},\ 0, \ldots, 0, \ldots, 0, 0, 1;\ \mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)}) = 0$$

$$S_i(y_{n-1} + y_n;\ y_1, \ldots, y_{n-i},\ 0, \ldots, 0, \ldots, 0, 1, 1;\ \mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)}) = 0$$

$$S_i(y_{n-2} + y_n;\ y_1, \ldots, y_{n-i},\ 0, \ldots, 0, \ldots, 1, 0, 1;\ \mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)}) = 0$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$S_i(y_{n-i+1} + y_n;\ y_1, \ldots, y_{n-i},\ 0, \ldots, 1, \ldots, 0, 0, 1;\ \mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(\mu)}) = 0.$$

La première nous permet de déterminer y_n en fonction algébrique de $y_1, y_2, \ldots, y_{n-i}$, et les suivantes y_{n-h}, $[h = 1, 2, \ldots, (i-1)]$ en fonction algébrique des mêmes variables $y_1, y_2, \ldots, y_{n-i}$. Toutes ces équations réunies déterminent donc des variétés dont l'ordre est au plus égal à $(n-i)$. En d'autres termes, si nous formons l'équation résolvante de ce système d'équations, nous sommes certain que les résolvants $R_1, R_2, \ldots, R_{i-1}$ sont égaux à l'unité. De plus, le résolvant de rang i, R_i, contient certainement le résolvant S_i; car

$$S_i = \prod_{(h)} \{u_{n-i+1}(y_{n-i+1} - \eta^{(h)}_{n-i+1}) + u_{n-i+2}(y_{n-i+2} - \eta^{(h)}_{n-i+2}) + \ldots + u_n(y_n - \eta^{(h)}_n)\}$$

et $\eta_n^{(h)}$, $\eta_{n-1}^{(h)} + \eta_n^{(h)}$, $\eta_{n-2}^{(h)} + \eta_n^{(h)}$, $\ldots$, $\eta_{n-i+1}^{(h)} + \eta_n^{(h)}$, sont précisément les racines des équations qui composent le système que nous considérons maintenant; si donc $S_i = 0$, ce système est vérifié par une variété $(n-i)^{\text{ième}}$ et, par suite, $R_i = 0$.

Mais S_i n'est pas nécessairement identique à R_i. Supposons donc qu'il y ait des systèmes de valeurs, formés par certaines combinaisons des racines des i équations précédentes, qui vérifient simultanément ces i équations et, par suite, leur résolvante de rang i, et ne vérifient cependant pas l'équation $S_i(y, y_1, \ldots, y_{n-i}, u_1, \ldots, u_n) = 0$. Ces solutions peuvent alors, il est vrai, pour certaines valeurs particulières données aux entiers $p_1, p_2, \ldots, p_n$, vérifier l'équation

$$S_i(p_1y_1 + p_2y_2 + \ldots + p_ny_n, y_1, \ldots, y_{n-i}, p_1, p_2, \ldots, p_n) = 0$$

mais elle ne saurait vérifier cette équation pour tous les systèmes possibles $p_1, p_2, \ldots, p_n$. D'autre part, l'équation

$$S_i(p_1y_1 + p_2y_2 + \ldots + p_ny_n, y_1, \ldots, y_{n-i}, p_1, \ldots, p_n)$$
$$= \prod_{(h)} \{p_{n-i+1}(y_{n-i+1} - \eta_{n-i+1}^{(h)}) + \ldots + p_n(y_n - \eta_n^{(h)})\} = 0$$

est certainement vérifiée pour toutes les solutions de l'équation

$$S_i(u_1y_1 + u_2y_2 + \ldots + u_ny_n, y_1, \ldots, y_{n-i}, u_1, \ldots, u_n)$$
$$= \prod_{(h)} \{u_{n-i+1}(y_{n-i+1} - \eta_{n-i+1}^{(h)}) + \ldots + u_n(y_n - \eta_n^{(h)})\} = 0.$$

Si donc la fonction

$$S_i(y, y_1, \ldots, y_{n-i}, u_1, \ldots, u_n)$$

ne représente pas à elle seule le résolvant de rang i des i équations considérées, nous pouvons toujours choisir des entiers $p_1, p_2, \ldots, p_n$ tels qu'elle représente, à elle seule, le résolvant de rang i des $(i + 1)$ équations

$$S_i(y_n;\ y_1,\ y_2,\ \ldots,\ y_{n-i},\ 0,\ \ldots,\ 0,\ \ldots,\ 0,\ 1) = 0$$

$$S_i(y_{n-1} + y_n;\ y_1,\ y_2,\ \ldots,\ y_{n-i},\ 0,\ \ldots,\ 0,\ \ldots,\ 1,\ 1) = 0$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$S_i(y_{n-i+1} + y_n;\ y_1,\ y_2,\ \ldots,\ y_{n-i},\ 0,\ \ldots,\ 1,\ \ldots,\ 0,\ 1) = 0$$

$$S_i(p_1y_1 + p_2y_2 + \ldots + p_ny_n;\ y_1, y_2, \ldots, y_{n-i}, p_1, \ldots, p_{n-i+1}, \ldots, p_{n-1}, p_n) = 0$$

dont les résolvants de rang un, deux, ..., $(n-1)$, sont égaux à l'unité.

Le système formé à l'aide des i premières équations précédentes peut également contenir des variétés d'ordres inférieurs à $(n-i)$. Mais si ces variétés sont situées sur la variété

$$S_i(y,\ y_1,\ \ldots,\ y_{n-i},\ u_1,\ \ldots,\ u_n) = 0$$

d'ordre $(n-i)$, comme $S_i = 0$ ne représente *qu'une variété d'ordre* $(n-i)$, nous pouvons toujours choisir les entiers $p_1, p_2, \ldots, p_n$ de manière que ces variétés ne vérifient pas l'équation

$$S_i(p_1y_1 + p_2y_2 + \ldots + p_ny_n,\ y_1,\ \ldots,\ y_{n-i},\ p_1,\ \ldots,\ p_n) = 0.$$

Le système formé à l'aide des $(i+1)$ équations précédentes peut alors contenir encore des variétés d'ordres inférieurs à $(n-i)$; mais ces variétés ne sont pas situées sur la variété représentée par l'équation

$$S_i(y,\ y_1,\ \ldots,\ y_{n-i},\ u_1,\ \ldots,\ u_n) = 0.$$

Cette dernière équation ne sera donc certainement pas vérifiée pour la variété $(n-i-1)^{\text{ième}}$ représentée par la résolvante de rang $(i+1)$ des $(i+1)$ équations considérées, du moins tant que $u_1, u_2, \ldots, u_n$ désignent des indéterminées. Nous pouvons donc toujours déterminer des entiers $p'_1, p'_2, \ldots, p'_n$ tels que le résolvant de rang $(i+1)$ du système

$$S_i(y_n,\ y_1,\ y_2,\ \ldots,\ y_{n-i}) = 0$$

$$S_i(y_{n-1} + y_n,\ y_1,\ y_2,\ \ldots,\ y_{n-i}) = 0$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$S_i(y_{n-i+1} + y_n,\ y_1,\ y_2,\ \ldots,\ y_{n-i}) = 0$$

$$S_i(p_1y_1 + \ldots + p_ny_n,\ y_1,\ y_2,\ \ldots,\ y_{n-i}) = 0$$

$$S_i(p'_1y_1 + \ldots + p'_ny_n,\ y_1,\ y_2,\ \ldots,\ y_{n-i}) = 0$$

soit égal à l'unité et que les résolvants de rangs supérieurs égalés à zéro ne représentent pas des variétés contenues dans la variété $(n-i)^{\text{ième}}$, $S_i = 0$. D'ailleurs le résolvant de rang i de ce système est, comme celui du système précédent, égal à S_i.

En continuant ainsi nous obtenons successivement de nouveaux systèmes contenant chacun une équation de plus que son précédent, et ayant leurs résolvants de rang $(i+1)$, $(i+2)$, ..., égaux à l'unité. Enfin nous parvenons à un système composé de n équations et tel que son résolvant de rang i étant toujours S_i, ses résolvants de rang $(i+1)$, $(i+2)$, ..., $(n-1)$ soient égaux à l'unité; seul son résolvant R_n, de rang n, peut encore être différent de l'unité; mais nous avons pu remplacer les indéterminées $u_1, u_2, \ldots, u_n$, par des systèmes d'entiers $p_1, p_2, \ldots, p_n$ tels que les systèmes isolés que représente l'équation $R_n = 0$ ne soient pas situés sur la variété $S_i = 0$, toujours puisque le résolvant de rang i, égalé à zéro, ne représente qu'une variété d'ordre $(n-i)$. En ajoutant, d'ailleurs, au système précédent composé de n équations, l'équation

$$S_i(y, y_1, y_2, \ldots, y_{n-i}, u_1, \ldots, u_n) = 0$$

nous formons un nouveau système dont le résolvant de rang i est toujours S_i, et les résolvants de rang $(i+1)$, $(i+2)$, ..., $(n-1)$, toujours l'unité, quelles que soient les valeurs par lesquelles on remplace $u_1, u_2, \ldots, u_n$, dans la dernière équation. Comme l'équation $S_i = 0$ n'est pas vérifiée, pour des u indéterminées, par la variété d'ordre zéro représentée par le résolvant R_n égalé à zéro, nous pouvons déterminer des entiers

$$p_1^{(n-i)}, \; p_2^{(n-i)}, \; \ldots, \; p_n^{(n-i)},$$

tels que le résolvant de rang n du système

$$\begin{aligned} S_i(y_h + y_n, y_1, \ldots, y_{n-i}) &= 0 \\ S_i(p_1^{(k)} y_1 + \ldots + p_n^{(k)} y_n, y_1, \ldots, y_{n-i}) &= 0 \end{aligned} \qquad \begin{pmatrix} h=0, n-i+1, \ldots, n-1 \\ k=0, 1, \ldots, n-i \\ y_0 = 0 \end{pmatrix}$$

soit égal à l'unité. Le résolvant total de ce système, qui se compose au plus de $(n+1)$ équations, est alors précisément égal à

$$S_i(y, y_1, \ldots, y_{n-1}, u_1, \ldots, u_n).$$

Dans la démonstration précédente nous avons fait usage de ce que $S_i = 0$ ne représentait qu'une seule variété, mais non de ce que S_i était irréductible. Nous pouvons donc énoncer immédiatement le théorème:

»$(n + 1)$ *équations suffisent toujours et sont en général nécessaires pour isoler, c'est à dire pour figurer à l'exclusion de toute autre variété, une variété d'ordre quelconque, prise dans une variété* $n^{ième}$.»

Nous dirons que cette figuration, par $(n + 1)$ équations, d'un système d'équations représentant une variété déterminée, est la *figuration complète* de ce système d'équations.

Un exemple très-intéressant de la différence essentielle qu'il y a entre la figuration principale et la figuration complète d'un système, est le suivant. Considérons un déterminant formé à l'aide de m^2 variables. D'après le dernier théorème, la condition nécessaire et suffisante pour que tous les mineurs d'ordre $(m - k + 1)$ s'annulent, doit pouvoir s'exprimer par $(m^2 + 1)$ équations, quel que soit k. Mais il suffit d'introduire *une inégalité,* pour que ce nombre d'équations se réduise à k^2, comme M. KRONECKER l'a démontré dans une lettre à M. BALTZER, insérée dans le Journal de CRELLE. La variété représentée par les $(m^2 + 1)$ équations dont nous parlons est donc d'ordre k^2 seulement; et cependant, si nous ne voulons pas introduire d'inégalité, elle ne peut s'exprimer par moins de $(m^2 + 1)$ équations.

Conclusion.

Les recherches contenues dans ce Mémoire amènent à plusieurs résultats intéressants.

1. Nous avons vu que non seulement la théorie de l'irréductibilité des fonctions entières, mais encore celle de systèmes particuliers de fonctions entières, pouvait être résolue sans quitter le domaine de l'Arithmétique et de l'Algèbre. L'importance des indéterminées dans cette recherche indique déjà le grand rôle qu'elles peuvent jouer en Algèbre. Leur association systématique aux éléments de cette science est comme le couronnement du grand trait de génie de GAUSS, qui a donné à l'Arithmétique un caractère tout différent de celui que cette science avait jusqu'alors; et, d'autre part, elle est intimement liée par le principe d'équivalence de M. KUMMER aux belles recherches arithmétiques de cet éminent géomètre.

2. En supposant connue la notion de fonction algébrique, nous avons montré comment on peut résoudre le problème général de la décomposition des systèmes de fonctions entières et ce qu'il fallait entendre par équivalence dans cette décomposition. (Comparez Festschrift § 20).

3. Nous nous sommes ensuite assurés que toute dépendance donnée par un nombre quelconque de fonctions entières égalées à zéro, peut être algébriquement — algébriquement, et non pas seulement logiquement, ce qui serait insuffisant en Algèbre, — ramenée à la dépendance donnée par *une* fonction entière égalée à zéro. Ainsi, en particulier, le domaine de rationalité le plus général que l'on puisse former, est bien celui que nous avons nommé domaine général de rationalité. Ce théorème complète le second chapitre de ce Mémoire. (Comparez Festschrift § 10.)

4. Nous voyons aussi quelle grande simplification la notion de contenant et de contenu, plus générale que celle de la divisibilité, introduit dans nos recherches. Elle n'est d'ailleurs point suffisante et il faut la généraliser encore, comme nous l'avons dit dans le troisième chapitre. Mais déjà la généralisation dont nous nous sommes particulière-

ment occupés, nous a rendu de vrais services et nous avons vu, plusieurs fois, combien elle est naturelle.

5. La théorie générale de l'élimination nous permet également d'énoncer quelques théorèmes fondamentaux qui jettent un nouveau jour sur les formes géométriques d'un nombre quelconque de dimensions. A cet effet il suffit de ne plus limiter le domaine de rationalité.

6. Si nous jettons enfin un coup d'œil sur les méthodes employées, nous voyons que tout revient toujours à la recherche du plus grand commun diviseur. Comme l'élimination est *la cinquième et la plus élevée des opérations de l'Algèbre,* on peut donc dire que la notion du plus grand commun diviseur domine l'Algèbre toute entière. C'est d'ailleurs bien naturel. La notion de plus grand commun diviseur des nombres entiers domine, elle aussi, l'Arithmétique élémentaire, et j'ai insisté, en commençant, sur l'identité des domaines arithmétique et algébrique.

Je termine en remarquant que, dans l'ordre de recherches abordées dans ce Mémoire, il conviendrait

α) d'étudier de plus près le cas si interessant des systèmes impropres à la décomposition, dans le sens que nous avons attaché à ce mot;

β) de débarasser les deux derniers chapitres de la notion de fonction algébrique, comme dans le cas particulier traité dans le chapitre trois.

En un mot, il conviendrait de *substituer davantage, et sans faire usage d'éléments étrangers à l'Arithmétique, la décomposition des systèmes de fonctions entières, à celle des systèmes correspondants d'équations algébriques.*

Paris, 20 Octobre 1883.