ANNALES SCIENTIFIQUES DE L'É.N.S.

HARRIS HANCOCK

Sur les systèmes modulaires de Kronecker

Annales scientifiques de l'É.N.S. 3^e série, tome 18 (1901), p. 3-115 (supplément)
<http://www.numdam.org/item?id=ASENS_1901_3_18__S3_0>

MÉMOIRE

SUR LES

SYSTÈMES MODULAIRES DE KRONECKER,

PAR M. HARRIS HANCOCK.

INTRODUCTION.

Les recherches de Kummer sur les unités complexes et sa découverte des nombres premiers idéaux qui, considérés comme les éléments extrêmes de cette théorie, occupent la même place que les nombres premiers dans la théorie générale des nombres rationnels, furent étendues à la théorie générale des nombres algébriques par Dedekind d'une part et par Kronecker de l'autre.

Dedekind, en considérant ces quantités simplement comme des nombres abstraits, a donné leurs propriétés fondamentales et caractéristiques et a établi ainsi une théorie pour ces nombres, comme l'avait fait Gauss pour les nombres rationnels ordinaires.

Kronecker, en employant ces nombres algébriques comme coefficients de fonctions d'une ou de plusieurs variables, a inauguré une théorie qui est la généralisation de la théorie des nombres rationnels et des nombres algébriques. Le domaine de rationalité le plus général n'est plus pour lui celui des nombres rationnels ou algébriques, c'est le domaine qui contient les fonctions rationnelles d'une ou de plusieurs variables à coefficients algébriques, ces coefficients appartenant à un domaine algébrique donné. Dans ce domaine, ce sont les fonctions de plusieurs variables à coefficients algébriques qui prennent la place des nombres rationnels dans la théorie ordinaire des nombres. Dans les domaines de Kronecker ce sont les systèmes modulaires pre-

miers qui remplacent les entiers rationnels premiers de la théorie ordinaire les nombres.

Il y a beaucoup de points communs à la théorie de Dedekind et à celle de Kronecker et qui sont dus, à vrai dire, à ce qu'il y a de commun aux domaines de rationalité d'où elles tirent leur origine; et c'est pour cette raison que dans la première Partie de cet Ouvrage, après avoir donné un historique du développement de la théorie des nombres algébriques, nous traitons brièvement quelques-uns des points essentiels des domaines algébriques de rationalité, en cherchant surtout à mettre en évidence les propriétés caractéristiques qui sont communes à la fois aux modules et aux idéaux de Dedekind d'une part et aux systèmes modulaires de Kronecker de l'autre. Nous pouvons ainsi étendre beaucoup de théorèmes sur les modules et les idéaux à la théorie des systèmes modulaires. En nous servant des idéaux premiers, nous pouvons effectuer la réduction des systèmes modulaires généraux d'une manière simple et tout à fait analogue à la réduction déjà donnée (*Journal de Crelle*, t. 119, p. 148) pour les systèmes dans lesquels les coefficients des éléments sont exclusivement des entiers rationnels.

Nous avons jugé qu'il était nécessaire de faire une digression sur la théorie des équations afin d'acquérir quelques notions sur les systèmes d'équations des différentes espèces (*Stufe*), auxquels la définition des systèmes modulaires des différentes espèces et des diviseurs des différentes espèces se trouve intimement liée.

Nous pouvons de cette façon avoir une notion plus précise des systèmes modulaires premiers.

L'auteur ne veut pas laisser échapper cette occasion d'exprimer à M. George Frobenius toute sa gratitude pour la courtoisie dont il a fait preuve en lui permettant de faire un libre usage des leçons sur la *Théorie générale des nombres algébriques* qui furent faites à Berlin par ce distingué professeur et qui lui ont été un guide précieux dans le présent Ouvrage, tout particulièrement dans l'exposition de la théorie de Dedekind.

Dans la seconde Partie de l'Ouvrage, nous nous occupons des systèmes modulaires dans le domaine algébrique général Ω. Ces systèmes sont réduits à leurs formes les plus simples et nous avons pu en donner

les formes canoniques par des méthodes analogues à celle donnée dans le *Journal de Crelle* (*loc. cit.*), ces formes étant de telle nature que, de quelque façon que l'on ait effectué la réduction du système initial, la forme finale qui est équivalente à la forme canonique lui est identique.

Les systèmes modulaires premiers ont, vis-à-vis des systèmes modulaires, les propriétés caractéristiques des nombres premiers dans la théorie ordinaire des nombres, et ces systèmes modulaires premiers ont aussi, vis-à-vis des domaines de rationalité dans lesquels ils entrent, des propriétés caractéristiques analogues à celles dont jouissent les entiers rationnels premiers relativement au domaine des nombres rationnels.

Après avoir déterminé les systèmes premiers dans chaque domaine, nous en déduisons quelques théorèmes, en particulier ceux qui sont les analogues du théorème donné par Fermat et de celui donné par Wilson pour la théorie ordinaire des nombres rationnels.

Si M désigne un système modulaire premier dont les éléments sont des fonctions irréductibles des variables x, y, z, ... à coefficients entiers appartenant à Ω, et si r est une fonction quelconque entière des variables x, y, z, ..., à coefficients entiers appartenant à Ω, le théorème de Fermat consiste en ce que, élevée à la puissance p^k, p étant un entier rationnel premier déterminé et k un entier rationnel fixé d'une manière déterminée, la fonction r satisfait à la congruence

$$r^{p^k} \equiv r \pmod{\mathrm{M}}.$$

Si h est le plus petit entier positif tel que

$$r^{p^h} \equiv r \pmod{\mathrm{M}},$$

h peut être appelé la *hauteur* de la fonction r relativement au système modulaire M.

Nous avons le remarquable théorème suivant :

$$r^{p^h} - r \equiv \Pi_i (r - r_i) \equiv \mathrm{IP}(r, x, y, z, \ldots) \pmod{\mathrm{M}},$$

où le premier produit doit être étendu à un système de p^h fonctions incongrues $r_i (i = 1, 2, \ldots, p^h)$ suivant le mod M, qui sont de hauteur h ou de hauteur d, d étant un diviseur de h; et où le second

produit s'étend à un nombre déterminé de fonctions irréductibles $P(r, x, y, z, \ldots)$ qui sont entières en toutes les variables. Ces fonctions sont de degré h ou d en r, de degrés déterminés par rapport aux variables $x, y, z, \ldots$, les coefficients des plus hautes puissances de r dans ces fonctions étant l'unité, tandis que tous les autres coefficients sont des entiers rationnels qui ont été réduits suivant le mod p.

PREMIÈRE PARTIE.

HISTORIQUE (1).

Les recherches relatives à la théorie des nombres n'ont porté, jusqu'au commencement de ce siècle, que sur les nombres rationnels, c'est-à-dire sur les nombres qui dérivent de l'unité par les opérations de l'addition, de la soustraction, de la multiplication et de la division, et qui ont la propriété de se reproduire par ces opérations. L'introduction de nombres algébriques dans de telles recherches est due à Abel qui, dans l'introduction au Mémoire intitulé *Sur la résolution algébrique des équations* (*Œuvres Sylow-Lie*, t. II, p. 219) se demande : « D'abord qu'est-ce que cela veut dire que de satisfaire algébriquement à une équation algébrique? » Comme réponse à cette question, il écrit : « Lorsqu'il s'agit d'une équation générale, dont tous les coefficients peuvent, par conséquent, être regardés comme des variables indépendantes, la résolution d'une telle équation doit consister à exprimer les racines par des fonctions algébriques des coefficients. Ces fonctions

(1) Donnant un exposé des recherches faites sur les nombres algébriques jusqu'à la publication de l'Ouvrage de KRONECKER : *Grundzüge einer arithmetischen Theorie der algebraischen Grössen* (*Festschrift zu Herrn E.-E. Kummers's funfzigjährigen Doctor-Jubiläum*). Berlin, Reimer; 1882.

pourront, selon la conception vulgaire de ce mot, contenir des quantités constantes quelconques, algébriques ou non. On pourra y ajouter, si l'on veut, comme condition particulière, que ces constantes seront de même des quantités algébriques : ce qui modifierait un peu le problème. En général, il y a deux cas différents selon que les coefficients seront des quantités variables ou non. » La classe spéciale d'équations résolubles qu'Abel traite dans son Ouvrage est celle des équations appelées par Jordan et Kronecker *équations abéliennes*.

Une quantité ξ est appelée *nombre algébrique* lorsqu'elle satisfait à une équation de la forme

$$x^n + c_1 x^{n-1} + c_2 x^{n-2} + \ldots + c_n = 0,$$

où les c sont des nombres rationnels; lorsque les c sont des entiers rationnels, ξ est un *entier algébrique;* lorsque les c sont des fonctions rationnelles d'un certain nombre de variables w, z, z', z'', ..., ξ est dit une *fonction algébrique* de ces variables; et lorsque les c sont des polynomes entiers par rapport aux variables qu'ils contiennent, ξ est un *entier algébrique fonction* de ces variables. Parmi les variables qui entrent dans les c nous pouvons en regarder au moins une, soit w, comme indépendante. Outre ces variables qui entrent dans l'expression des racines, il peut apparaître certaines espèces de nombres constants algébriques ou rationnels. Il semble résulter des remarques faites dans le Mémoire mentionné plus haut (*voir* aussi KRONECKER, *Werke,* édité par Hensel, t. II, la première Note de la p. 253) qu'Abel désirait, dans la solution générale des équations, considérer aussi des quantités qui n'étaient pas algébriques, les quantités transcendantes. Les résultats qui ont été obtenus dans l'étude de ces quantités sont, comme leur définition, de nature négative (1).

---

(1) Consulter sur ce sujet LIOUVILLE, *Sur des classes très étendues de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationnelles algébriques* (*Journal de Math.,* t. XVI; 1851).

CH. HERMITE, *Sur la fonction exponentielle* (*Comptes rendus,* t. LXXVII, 1873).

LINDEMANN, *Ueber die Zahl u* (*Math. Ann.,* t. XX).

WEIERSTRASS, *Zu Lindemann's Abhandlung : Ueber die Ludolph'sche Zahl* (*Sitz. der Ber. Akad.;* 3 décembre 1885).

Voir aussi les *OEuvres* de HILBERT, HURWITZ et GORDAN dans le 43e vol. des *Math. Ann.*

Abel mourut sans avoir fait avancer beaucoup la théorie des nombres algébriques.

Ce fut Gauss qui, le premier, fit faire un grand pas à cette théorie en « élargissant le champ de l'Arithmétique » par l'introduction des quantités algébriques de la forme $a + ib$ (voir *Theoria residuorum biquadraticorum, commentatio secunda*, 1831). Les quantités a et b sont des nombres rationnels et $i = \sqrt{-1}$.

Plus tard il considéra les nombres algébriques plus généraux qui sont composés des racines de l'unité. De tels nombres sont spécialement étudiés par Cauchy (1), Jacobi (2) et Eisenstein (3).

Ces mathématiciens rencontrèrent bientôt ce résultat inattendu que, dans le domaine d'investigation considéré, deux nombres n'avaient pas toujours un plus grand commun diviseur et que des produits de facteurs irréductibles pouvaient être égaux sans que les facteurs simples fussent égaux.

KUMMER [*Gratulationsschrift des Breslauer Universität, etc.* (Breslau, 1844)] écrit : « *Maxime dolendum videtur, quod hæc numerorum realium virtus, ut in factores primos dissolvi possint qui pro eodem numero semper iidem sint, non eadem est numerorum complexorum, quæ si esset tota hæc doctrina, quæ magnis adhuc difficultatibus laborat, facile absolvi et ad finem perduci posset.* »

Un entier algébrique peut être décomposé en un produit d'un nombre fini d'entiers algébriques irréductibles; mais cette décomposition n'est pas *unique* et il n'est plus vrai que si un produit est divisible par un nombre irréductible, un de ses facteurs au moins doit être divisible par ce nombre. KUMMER [*Zur Theorie der complexen Zahlen* (*Crelle*, 35)] imagina un moyen de surmonter cette difficulté par l'introduction d'une nouvelle conception, celle des facteurs premiers idéaux, et montra que les facteurs premiers rationnels n'étaient pas

---

(1) CAUCHY, *Mémoire sur la théorie des nombres* (*Comptes rendus*, 1840). — Trois Notes dans les *Comptes rendus*, p. 347, 407, 1120; 1840.

(2) JACOBI, *Œuvres complètes*, vol. VI, p. 233, 240, 254, 275.

(3) EISENSTEIN, *Ueber eine neue Gattung Zahlentheoretisher Fonctionen*, et *Beweis der allgemeinsten Reciprocitätsgesetzte zwischen reellen und complexen Zahlen* (*Ber. der K. Akad. der Wissen. zu Berlin*, 1850) et de nombreux écrits dans le 27e et le 28e vol. du *Journal de Crelle*.

les *éléments extrêmes* (*ausserste*). Kummer n'appliquait ces principes qu'aux nombres algébriques qui sont dérivés des racines de l'unité. Les facteurs idéaux qu'il a introduits ont servi à écarter beaucoup de dilemmes qui avaient déjà été rencontrés par les mathématiciens cités plus haut, et ont été le point de départ des recherches plus générales de Kronecker et Dedekind.

Les nombreux écrits de Kummer sur les unités complexes sont donnés par Lampe dans le *Nachruf für Ernst Eduard Kummer* (*Iahresbericht der Deutsch. math. Vereinigung*, t. III, p. 23); *cf.* aussi HERMITE, *Notice sur les travaux de M. Kummer* (*Comptes rendus*, 1893, p. 1163).

La théorie des fonctions analytiques fut développée par les savants de l'école française. Pendant son séjour à Paris, Dirichlet avait pu se mettre très au courant de ce sujet, et de retour en Allemagne, par ses leçons sur la théorie des équations aux dérivées partielles, il répandit dans l'école allemande cette théorie déjà bien connue en France, grâce surtout aux efforts de Fourier, Poisson, Ampère et Monge. Riemann l'apprit de Dirichlet, et c'est sur cette base qu'il fonda la théorie de Riemann.

Appliquant ses connaissances des méthodes analytiques aux problèmes qui se posent dans l'étude des quantités complexes, Dirichlet trouva un moyen simple et direct de les résoudre. Sa première communication sur ce sujet est une lettre adressée à Liouville et insérée dans les *Comptes rendus* de 1840.

Les résultats principaux de ces recherches se trouvent dans les *Monatsberichte* de l'Académie de Berlin (octobre 1841, avril 1842 et mars 1846). *Voir* aussi les références sur ses ouvrages dans le onzième supplément à la *Théorie des nombres* de Dirichlet, par Dedekind.

KUMMER [*Gedächtnissrede auf Lejeune-Dirichlet* (*Abhandl. der Königl. Akad. der Wiss. zu Berlin*, 1893, p. 1)] dit que l'application faite par Dirichlet de l'analyse à la théorie des nombres fait époque dans cette théorie en créant dans cette branche une nouvelle discipline mathématique comme le fit en Géométrie l'application de l'analyse par Descartes.

Antérieurement aux ouvrages de Kronecker, nous pouvons citer ici

Selling, qui [*Ueber die idealen Primfactoren welche aus den Wurzeln einer beliebigen irreductiblen Gleichung rational gebildet sind* (*Schlöm. Zeits.*, t. X, p. 17)] s'occupe de la réduction des racines $\rho_1, \rho_2, \ldots, \rho_n$ d'une équation algébrique irréductible

$$R_n = a_0 x^n + a_1 x^{n-1} + \ldots + a_n = 0,$$

où les a sont entiers, en facteurs premiers idéaux et suit une marche analogue à celle suivie par Kummer dans cette théorie, pour les nombres formés des racines de l'unité; Zolotareff, qui discuta des questions semblables dans la brochure *Sur la théorie des nombres complexes* (*Journal de Liouville*, 3e série, t. VI, p. 51 et p. 129).

Ceux qui s'occupèrent de la théorie des congruences supérieures et dont les recherches semblent avoir été utiles à Kronecker sont Schönemann (1) et Serret (2).

Après Gauss le grand maître dans la théorie des nombres fut Kronecker. Il semble qu'il ait voulu en faire la base de toute la Science mathématique.

Ce fut Kronecker qui généralisa les principes de Kummer et qui sentit la nécessité de définir les facteurs premiers idéaux pour les quantités algébriques les plus générales, en comprenant à la fois dans ces quantités les nombres algébriques et les quantités algébriques définies à la page 7. Frobenius, dans sa *Gedächtnissrede auf Leopold Kronecker* (*Abhandl. der Königl. Akad. der Wiss. zu Berlin*, 1893, p. 1), dit : « Par la manière dont le génie de Gauss traita les nombres cyclotomiques l'Algèbre fut redevable à l'Arithmétique, et la force conquérante de Jacobi déposa à ses pieds (de l'Arithmétique) les immenses trésors de formules de la théorie des fonctions elliptiques et au service de Dirichlet elle s'introduisit dans les méthodes les plus subtiles de l'analyse. Ce sera toujours la gloire de Kronecker d'avoir rendu cette science, qui se suffisait à elle-même, utile à la fois à l'Algèbre et à la

(1) SCHÖNEMANN, *Allgemeine Sätze über Congruenzen, etc.* (*Journal de Crelle*, t. 19, p. 231 et p. 289).

SCHÖNEMANN, *Grundzüge einer allgemeinen Theorie der höheren Congruenzen, etc.* (*Journal de Crelle*, t. 31, p. 269).

(2) SERRET, *Comptes rendus*, 1865, p. 913, et Chapitre III de son *Cours d'Algèbre supérieure*, t. II, 1866.

Théorie des fonctions; » et Kronecker, dans ses *Antrittsrede* à l'Académie de Berlin, dit : « *Die Verknupfung dieser drei Zweige der Mathematik erhöht den Reiz und die Fruchtbarkeit der Untersuchung.* »

Les recherches sur les nombres complexes formés des racines des équations abéliennes conduisirent Kronecker au problème algébrico-arithmétique de la formation de toutes les équations abéliennes pour un domaine quelconque de rationalité. Il communiqua la solution de ce problème à l'Académie de Berlin en 1853.

Depuis cette époque on attribua à Kronecker une habileté toute spéciale à traiter les questions d'Algèbre à un point de vue arithmétique et, en s'occupant de ces problèmes, il conçut l'idée d'étendre la notion, due à Gauss, de congruences ayant pour module un entier à la notion de congruences ayant un système arbitraire de modules, notion dont Schönemann et Serret avaient déjà eu tous deux une première idée.

Hensel, dans la préface du premier Volume des *Kronecker's Werke,* écrit, sous le nom d'*Arithmétique générale :* « Kronecker étendait l'application des conceptions et des méthodes de la théorie des nombres à la recherche des fonctions rationnelles d'un certain nombre de variables. Ce très vaste champ de recherches embrasse l'étude des systèmes de nombres entiers, la théorie des nombres dans son entier, les recherches sur les systèmes linéaires, la théorie des déterminants, les formes bilinéaires et quadratiques et finalement la théorie générale des nombres algébriques et des fonctions d'une et de plusieurs variables. » La théorie générale permettant de traiter ces questions fut présentée par Kronecker sous une forme condensée et excessivement difficile, à l'occasion du cinquantième anniversaire du doctorat de Kummer dans les *Grundzüge einer arithmetischen Theorie der algebraischen Grössen.*

Dans cet ouvrage, Kronecker employa systématiquement la méthode des coefficients indéterminés dans la définition des quantités idéales et, en se servant de plusieurs variables dans la mise en formules de ces fonctions, surmonta les difficultés et évita les imperfections rencontrées dans l'emploi d'une seule variable.

Au lieu d'associer des espèces plus élevées d'irrationnelles algébriques, il élargit la dimension du domaine initial en associant des

formes de plusieurs indéterminées et donna surtout de nouveaux points de vue pour les domaines de rationalité qui contiennent non seulement des nombres et des fonctions d'une variable mais encore de plusieurs variables indépendantes. Au moyen d'un nombre fini de quantités algébriques entières il peut exprimer toutes les quantités de cette sorte qui appartiennent au domaine. Le plus grand commun diviseur de plusieurs quantités entières n'est pas la seule chose commune à ces quantités, c'est seulement un diviseur commun de première espèce (*Stufe*); elles peuvent avoir aussi des diviseurs communs d'espèce supérieure.

Dedekind fit à la même époque des recherches semblables et indépendantes de celles de Kronecker, qui le conduisirent à une théorie générale du calcul des nombres algébriques. Dans ses idéaux premiers il a trouvé, pour les nombres algébriques généraux, les éléments extrêmes comme Kummer l'a fait dans le cas plus spécial des nombres algébriques qui sont formés avec les racines de l'unité. Dans le onzième Supplément à la *Dirichlet's Zahlentheorie* et dans d'autres ouvrages cités dans ce volume, Dedekind a fondé pour la théorie générale des nombres algébriques de véritables *Disquisitiones arithmeticæ*.

Domaine de rationalité.

Une fonction donnée de degré n

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n,$$

où $a_0, a_1, \ldots, a_n$ sont des nombres rationnels, peut toujours être décomposée en n facteurs linéaires, de sorte que l'on ait

$$f(x) = a_0 (x - x_1)(x - x_2) \ldots (x - x_n),$$

$x_0, x_2, \ldots, x_n$ étant les n racines de l'équation $f(x) = 0$.

Cette décomposition en facteurs n'est plus possible si nous assujettissons les coefficients à certaines conditions; par exemple, si nous voulons que les coefficients des facteurs en lesquels la fonction $f(x)$ doit être décomposée soient aussi des nombres réels, $f(x)$ ne pourra en général être décomposée qu'en facteurs du premier et du second degré puisqu'un trinome du second degré à discriminant négatif

ne peut pas être décomposé en deux facteurs linéaires à coefficients réels.

Nous pouvons aussi nous proposer de décomposer une fonction $F(x)$ à coefficients entiers en des facteurs qui aient aussi leurs coefficients entiers. Nous savons que cela est souvent impossible.

Nous appellerons *domaine* (1) un système de nombres ou de quantités en nombre infini; par exemple, nous avons le domaine de tous les entiers, le domaine de tous les nombres rationnels, qui comprend tous les entiers et toutes les fractions; etc.

Nous avons déjà dit que les nombres rationnels fournissent des nombres rationnels en les faisant entrer dans des opérations rationnelles. Ceci est encore vrai pour les nombres algébriques, c'est-à-dire qu'une fonction rationnelle d'un certain nombre de nombres algébriques est un nombre algébrique. Nous appelons *domaine de rationalité* (2) un système de quantités tel que toutes les quantités du système aient la propriété de se reproduire par des opérations rationnelles de sorte que, par exemple, la somme, la différence, le produit ou le quotient de deux nombres quelconques du système soient un nombre appartenant au système.

Soient $R^{(1)}$, $R^{(2)}$, $R^{(3)}$, ..., des quantités, où le terme *quantité* doit être pris dans le sens arithmétique et algébrique le plus large. Le domaine de rationalité de ces quantités comprend toutes les fonctions rationnelles de ces quantités dont les coefficients sont des nombres rationnels. On peut le désigner par $P = (R^{(1)}, R^{(2)}, R^{(3)}, \ldots)$. Après avoir fixé le domaine de rationalité nous pouvons supposer que les coefficients d'une fonction entière d'un certain nombre de variables appartiennent (3) à ce domaine. Cette fonction est dite *décomposable* en facteurs, lorsqu'elle est égale au produit de deux ou plusieurs fonctions entières de deux variables dont les coefficients appartiennent au même domaine de rationalité; sinon la fonction est dite *irréductible*.

---

(1) Je traduis le mot de Kronecker *Bereich* par le mot *domaine*, parce que ce mot éveille moins l'idée d'espace que tout autre mot (*voir* KRONECKER, t. II, p. 249).

(2) Ce qui correspond à ce que Dedekind appelle *Körper von Zahlen* ou *Zahlkörper* et Kronecker, *Rationalitätsbereich*.

(3) Une quantité appartient à un domaine lorsqu'elle est l'une des quantités qui constituent ce domaine.

Soit $P = (R^{(1)}, R^{(2)}, \ldots)$ un domaine de rationalité déterminé (1). La quantité ξ est dite *quantité algébrique* (ou fonction algébrique des quantités $R^{(1)}, R^{(2)}, \ldots$ *dérivée* du domaine P si ξ satisfait à une équation algébrique dont les coefficients appartiennent au domaine P. Toutes les quantités algébriques qui sont dérivées d'un domaine P forment elles-mêmes un autre domaine de rationalité.

A chaque quantité algébrique ξ correspond une équation irréductible $f(\xi) = 0$ qui est satisfaite par cette quantité. Si la fonction $f(\xi)$ est de degré n, les $n - 1$ autres racines $\xi^{(1)}, \xi^{(2)}, \ldots, \xi^{(n-1)}$ sont appelées *racines conjuguées* de ξ. Ce n'est donc là qu'une notion relative, puisqu'elle se rapporte au domaine P. Nous pouvons appeler P le domaine fondamental (*Stammbereich*). Nous dirons que le domaine P est le domaine *naturel* de rationalité lorsque les R sont tous indépendants. Dans ce cas, les fonctions entières de $R^{(1)}, R^{(2)}, \ldots$, à coefficients entiers constituent un système de quantités qui forment une partie ou un *diviseur* du domaine P. Le domaine formé par ces quantités entières est appelé *domaine d'intégrité* et est désigné par $[R^{(1)}, R^{(2)}, \ldots]$.

Une quantité ξ est appelée *fonction algébrique entière* des quantités $R^{(1)}, R^{(2)}, \ldots$, ou *quantité algébrique entière,* lorsqu'elle satisfait à une équation dans laquelle le coefficient de la plus haute puissance de la variable est l'unité tandis que les autres coefficients sont des quantités appartenant à $(R^{(1)}, R^{(2)}, \ldots)$. Puisque les fonctions algébriques entières des quantités algébriques entières sont des quantités algébriques entières, il en résulte que toutes les quantités algébriques entières qui sont dérivées du domaine d'intégrité $[R^{(1)}, R^{(2)}, \ldots]$ forment elles-mêmes un autre domaine d'intégrité.

Il existe un domaine de rationalité qui ne comprend que la quantité zéro. Nous ne considérerons pas ce cas trivial et nous supposerons toujours que le domaine comprend au moins une quantité a différente de zéro. Il comprendra donc toutes les quantités que l'on déduit de cette quantité par des opérations rationnelles, et par conséquent la quantité $\frac{a}{a} = 1$. Par suite tous les entiers positifs et négatifs ainsi que

(1) Nous écrirons *domaine* au lieu de *domaine de rationalité* quand il ne pourra pas en résulter de confusion.

les fractions appartiennent à ce domaine. L'ensemble de ces nombres rationnels forme un domaine de rationalité que Kronecker appelle le *domaine absolu* de rationalité. Ce domaine est contenu comme diviseur dans tout autre domaine, sauf dans le domaine trivial que nous venons de mentionner.

Si, au domaine de rationalité

$$P = (R^{(1)}, R^{(2)}, \ldots),$$

nous *adjoignons* une quantité ξ dérivée de ce domaine, nous avons un nouveau domaine

$$P(\xi) = (\xi, R^{(1)}, R^{(2)}, \ldots).$$

Toute fonction rationnelle de ξ, c'est-à-dire de la forme $\frac{h(\xi)}{g(\xi)}$, peut, au moyen de l'équation irréductible du $n^{\text{ième}}$ degré $f(\xi) = 0$, qui détermine ξ, être transformée en une fonction entière de ξ dont le degré est, au plus, $n - 1$ (*voir* l'*Algèbre* de Weber, t. I, p. 498). Par suite, nous aurons toutes les quantités appartenant au domaine $P(\xi)$ si, dans l'expression

$$a_0 + a_1\xi + a_2\xi^2 + \ldots + a_{n-1}\xi^{n-1},$$

nous prenons pour les a toutes les quantités du domaine P, et chacune des quantités de $P(\xi)$ est obtenue une fois seulement lorsque l'on substitue ces valeurs dans la forme linéaire.

$P(\xi)$ peut donc être appelé un *domaine du $n^{\text{ième}}$ degré*. Si $\xi^{(1)}$, $\xi^{(2)}, \ldots, \xi^{(n-1)}$ sont les racines conjuguées de ξ, $P(\xi^{(1)})$, $P(\xi^{(2)}), \ldots,$ $P(\xi^{(n-1)})$ s'appellent les *domaines conjugués de* $P(\xi)$, et le produit des domaines $P(\xi)$, $P(\xi^{(1)}), \ldots, P(\xi^{(n-1)})$ s'appelle le *norme* du domaine $P(\xi)$.

Lorsque toutes les quantités appartenant à l'un des domaines se trouvent aussi dans un autre domaine, on dit que ce dernier domaine *contient* le premier domaine et le premier est appelé un *diviseur* du second.

Par exemple, le domaine d'intégrité $[R^{(1)}, R^{(2)}, \ldots]$ est un diviseur du domaine $(R^{(1)}, R^{(2)}, \ldots)$ et le domaine $P(\xi)$ contient le *domaine fondamental* P. Toutes ces quantités algébriques, qui appartiennent au domaine $P(\xi)$, forment un *genus* (*Gattung*) de quantités algé-

briques, et le domaine $P(\xi)$ peut s'appeler le *genus* ξ lorsqu'on veut le distinguer d'un autre domaine.

Plus petit commun multiple ou produit de plusieurs domaines.

Soient $\xi, \eta, \zeta, \ldots$, des quantités algébriques dérivées du domaine

$$P = (R^{(1)}, R^{(2)}, \ldots)$$

et qui satisfont, par conséquent, aux équations algébriques

$$f(x) = 0, \qquad g(y) = 0, \qquad h(z) = 0, \qquad \ldots,$$

respectivement de degré $a, b, c, \ldots$, et dont les coefficients sont des quantités appartenant au domaine P. Formons les domaines $P(\xi)$, $P(\eta)$, $P(\zeta)$, ... Le plus petit commun multiple de ces domaines est un domaine composé du système de nombres le plus petit possible qui contienne tous les nombres appartenant à ces domaines; c'est-à-dire que c'est le domaine qui contient la totalité des fonctions rationnelles de $\xi, \eta, \zeta, \ldots$. Nous pouvons donc dire que $P(\xi, \eta, \zeta, \ldots)$ est le plus petit commun multiple ou le produit de ces domaines $P(\xi)$, $P(\eta)$, $P(\zeta)$, ...

Si maintenant il est possible de déduire une quantité ω telle que ω soit une fonction rationnelle de toutes les quantités $\xi, \eta, \zeta, \ldots$ et, en même temps, que chacune des quantités $\xi, \eta, \zeta, \ldots$ soit une fonction rationnelle de ω, le domaine $P(\xi, \eta, \zeta, \ldots)$ est identique au domaine $P(\omega) = \Omega$.

Pour montrer que l'on peut avoir une fonction telle que ω, il suffit de choisir pour ω une fonction rationnelle de $\xi, \eta, \zeta, \ldots$, telle que les $a.\ b.\ c.\ldots$ valeurs que ω prend lorsque nous remplaçons $\xi, \eta, \zeta, \ldots$ par leurs valeurs conjuguées, soient toutes différentes.

Le cas le plus simple d'une telle fonction est l'expression linéaire

$$w = \xi + p\eta + q\zeta + \ldots,$$

où, d'après la méthode de Cantor (*Math. Ann.*, t. V, p. 133), les quantités $p, q, \ldots$ ont été choisies de manière à remplir les conditions voulues. La proposition peut être alors démontrée, par exemple, par la méthode de Weber (*Alg.*, t. I, p. 500).

Conception plus précise d'un domaine du $n^{\text{ième}}$ degré. Domaines algébriques ou finis.

Nous dirons que n quantités $\xi_0, \xi_1, \ldots, \xi_{n-1}$ du domaine $P(\xi)$ sont linéairement indépendantes quand il n'est pas possible de trouver n quantités $a_0, a_1, \ldots, a_{n-1}$ du domaine P telles que l'on ait

$$a_0\xi_0 + a_1\xi_1 + \ldots + a_{n-1}\xi_{n-1} = 0.$$

Un domaine est dit *fini du $n^{\text{ième}}$ degré* lorsqu'il contient n quantités linéairement indépendantes, mais que $n+1$ quantités *quelconques* du domaine sont linéairement dépendantes.

Par exemple, les quantités $1, \xi, \xi^2, \xi^3, \ldots, \xi^{n-1}$ du domaine $P(\xi)$ sont linéairement indépendantes, mais une autre quantité η du domaine $P(\xi)$ peut être exprimée par une expression de la forme

$$\eta = a_0 + a_1\xi + a_2\xi^2 + \ldots + a_{n-1}\xi^{n-1},$$

où $a_0, a_1, \ldots, a_{n-1}$ sont des nombres du domaine P.

Dans un domaine du $n^{\text{ième}}$ degré, chaque système de n quantités linéairement indépendantes forme une *base* du domaine. Si l'on multiplie par tous les nombres rationnels les n quantités d'une base d'un domaine et si l'on ajoute les résultats, on a toutes les quantités du domaine, et chacune d'elles n'est obtenue qu'une fois.

Nous pouvons donc ainsi définir le degré d'un domaine à l'aide du domaine lui-même sans employer la quantité particulière ξ de ce domaine.

Relativement aux domaines infinis, nous ne pouvons donner que des résultats négatifs comme, du reste, leur définition, qui doit s'énoncer d'une manière négative.

Un domaine fini peut ne contenir que des nombres algébriques; un tel domaine sera, en conséquence, appelé un *domaine algébrique*. Le seul domaine du premier degré est le domaine des nombres rationnels. Nous le désignerons par $P(1)$ ou P. Ce domaine est contenu dans tous les autres et peut être nommé le *domaine absolu* P.

Si nous adjoignons au domaine P les racines d'une équation irréductible, le domaine qui en résulte est fini, et *nous obtenons tous les*

domaines finis possibles si nous adjoignons à P *les racines de toutes les équations irréductibles possibles.*

Pour démontrer ce théorème, il nous suffit de montrer que dans tout domaine fini A de degré n il existe une quantité algébrique au moyen de laquelle le domaine algébrique est complètement déterminé.

Si u est une quantité arbitraire du domaine A, elle satisfait à une équation irréductible de degré p, par exemple, dont les coefficients appartiennent au domaine P. Nous pouvons former le nouveau domaine $P(u)$ qui contient les p quantités linéairement indépendantes $1, u, \ldots, u^{p-1}$. Si $n > p$, le domaine A contient au moins une autre quantité u' qui est linéairement indépendante des quantités $1, u, \ldots, u^{p-1}$. Nous adjoignons cette quantité au domaine $P(u)$ et nous avons $P(u, u') = P(v)$, par exemple, où v satisfait à une équation irréductible de degré $q \leqq n$. Si $q < n$, nous continuerons à opérer de même jusqu'à ce que finalement nous arrivions, par un nombre fini d'opérations, à un domaine $P(x)$ du $n^{\text{ième}}$ degré.

Il peut y avoir plusieurs de ces quantités x, et qui soient différentes. Soit y une autre de ces quantités qui vérifie aussi une équation irréductible du $n^{\text{ième}}$ degré.

On voit par la manière même dont ces quantités ont été formées que x et y peuvent être exprimées rationnellement en fonction l'une de l'autre. De telles quantités sont appelées quantités *primitives* dans le domaine A qu'elles déterminent complètement. Le domaine $P(x)$ est identique à $P(y)$. La méthode suivante, donnée par le professeur Frobenius, peut être employée pour rechercher si la quantité y du domaine $P(x)$ est primitive ou non.

Soient $x^{(1)}, x^{(2)}, \ldots, x^{(n-1)}$ les quantités conjuguées de x. Soit $y = \varphi(x)$ où φ désigne une fonction rationnelle, et formons l'expression suivante, dans laquelle t est une quantité variable :

$$[t - \varphi(x)][t - \varphi(x')]\ldots[t - \varphi(x_1^{(n-1)})] = g(t);$$

$g(t)$ est une fonction entière de t dont les coefficients appartiennent au domaine P, puisque les fonctions symétriques élémentaires de x, x', ... peuvent être exprimées en fonction des coefficients de l'équation irréductible à laquelle x satisfait. En posant

$$y = \varphi(x), \quad y' = \varphi(x'), \quad \ldots, \quad y^{n-1} = \varphi(x^{n-1}),$$

l'équation ci-dessus devient

$$(t-y)(t-y')\ldots(t=y^{n-1})=g(t),$$

équation du $n^{\text{ième}}$ degré qui a y pour racine. Si y est une quantité primitive, elle satisfait à une équation irréductible du n^{ieme} degré; et dans ce cas les $n-1$ fonctions $\varphi(x')\ldots\varphi(x^{(n-1)})$ peuvent donner $n-1$ valeurs différentes $y^{(1)}, y^{(2)}, \ldots, y^{(n-1)}$, conjuguées de y.

Il est clair que les domaines $(x, R^{(1)}, R^{(2)}, \ldots)$, $(y, R_0^{(1)}, R_0^{(1)}, \ldots)$ sont identiques puisque les éléments de l'un des domaines peuvent s'exprimer rationnellement en fonction des éléments de l'autre et que, inversement, les éléments du second domaine peuvent s'exprimer rationnellement en fonction des éléments du premier. De plus, une fonction rationnelle des éléments d'un domaine peut être adjointe au domaine sans l'altérer, et, puisqu'un élément d'un domaine de rationalité peut s'exprimer rationnellement en fonction des autres éléments, on peut l'écarter du domaine.

Diviseurs d'un domaine donné.

Nous pouvons énoncer le lemme suivant :

LEMME. — *Si $f(x)$ est une fonction entière irréductible de x dont les coefficients appartiennent au domaine de rationalité déterminé* P, *et si $g(x)$ est une autre fonction de x dont les coefficients appartiennent aussi à un domaine* P, *je dis que, si $g(x)$ a avec $f(x)$ une racine commune, chaque racine de $f(x)$ est une racine de $g(x)$ et, par conséquent, que $g(x)$ est divisible par $f(x)$ si nous négligeons un facteur constant.*

Il en résultera aussi que :

1° Une équation irréductible ne peut avoir aucune racine commune avec une équation de degré inférieur;

2° Une équation irréductible ne peut pas avoir de racines multiples;

3° Deux équations irréductibles ne peuvent pas avoir de racines communes;

4° Lorsque le produit de deux fonctions entières est divisible par

une fonction irréductible, un des facteurs est divisible par cette fonction;

5° Une fonction réductible ne peut être décomposée en facteurs irréductibles que d'une seule manière.

Soit $h(z)$ une équation irréductible de degré c dont les coefficients appartiennent au domaine fondamental P, et soient z', $z^{(2)}$, ..., $z^{(c-1)}$ les quantités conjuguées de z. Formons le genre z,

$$\Gamma = P(z),$$

et soit x une quantité appartenant à ce dernier domaine, de telle sorte que, cependant, x soit une fonction rationnelle de z, soit $x = \varphi(z)$, et formons les expressions

$$\begin{aligned} x &= \varphi(z), \\ x^1 &= \varphi(z^1), \\ x^{(2)} &= \varphi(z^{(2)}), \\ &\cdots\cdots\cdots, \\ x^{(c-1)} &= \varphi(z^{(c-1)}). \end{aligned}$$

Nous allons maintenant former la fonction

$$F(t) = (t-x)(t-x^1)\ldots(t-x^{(c-1)}),$$

ou

$$F(t) = [t-\varphi(z)][t-\varphi(z^1)]\ldots[t-\varphi(z^{(c-1)})],$$

fonction entière de degré c dont les coefficients appartiennent au domaine P.

Je dis que $F(t)$ *est, soit une fonction irréductible, soit une puissance d'une fonction irréductible.*

Car si $F(t)$ est résoluble, soit $f(t)$ un de ses facteurs irréductibles de degré a, qui devient nul pour $t = \varphi(z)$ par exemple; on a

$$f[\varphi(z)] = 0.$$

Cette équation a donc une racine commune avec l'équation irréductible $h(z) = 0$; par conséquent,

$$f[\varphi(z^1)] = 0, \quad f[\varphi(z^{(2)})] = 0, \quad \ldots, \quad f[\varphi(z^{(c-1)})] = 0,$$

de sorte que chaque racine de l'équation $F(t) = 0$ satisfait à l'équation irréductible $f(t) = 0$.

Dès lors, en négligeant un facteur constant, on a

$$F_c(t) = [f_a(t)]^n,$$

où n est un entier positif.

Formons maintenant le *genus* x,

$$A = P(x),$$

où x satisfait à une équation irréductible $f(x) = 0$ de degré a, dont les coefficients appartiennent à P. Puisque x est aussi une quantité appartenant au domaine Γ, nous voyons que x est une fonction rationnelle de z, et nous dirons que le domaine A est un *diviseur* du domaine Γ. De la relation $c = a.n$, on déduit que le degré du domaine A est un *diviseur* du degré du domaine Γ, lorsque A est un diviseur de Γ. Si $n = 1$, la fonction $F(t)$ est irréductible, et toutes les racines x, $x', \ldots, x^{(c-1)}$ de $F(t) = 0$ sont différentes. Dès lors, x satisfait à une équation irréductible de degré n, et les quantités $1, x, x^2, \ldots, x^{c-1}$ sont c quantités indépendantes appartenant au domaine Γ. Donc toute autre quantité z du domaine Γ peut être exprimée rationnellement en fonction de x, de sorte que l'on a $z = \chi(x)$, où χ désigne une fonction rationnelle. Dans ce cas, les domaines A et Γ sont identiques.

Si $n \neq 1$, les c quantités $\varphi(z), \varphi(z'), \ldots, \varphi(z^{(c-1)})$ peuvent être distribuées par groupes, dans chacun desquels il y a n quantités égales, de sorte que

$$\begin{aligned}
x &= \varphi(z) = \varphi(z_1) = \varphi(z_2) = \ldots = \varphi(z_{n-1}),\\
x' &= \varphi(z') = \varphi(z'_1) = \varphi(z'_2) = \ldots = \varphi(z'_{n-1}),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
x^{(a-1)} &= \varphi(z^{(a-1)}) = \varphi(z_1^{(a-1)}) = \varphi(z_2^{(a-1)}) = \ldots = \varphi(z_{n-1}^{(a-1)}),
\end{aligned}$$

les quantités $\varphi(z_k^{(i)})$ désignant les quantités $\varphi(z), \ldots, \varphi(z^{(c-1)})$, quel que soit leur ordre.

Formons maintenant la fonction $\psi(t, x) = \varphi(t) - x$, fonction qui s'annule pour les n valeurs $t = z, z_1, \ldots, z_{n-1}$.

Soit

$$g(t, x) = (t - z)(z - z_1)\ldots(t - z_{n-1}),$$

le plus grand commun diviseur de la fonction $\psi(t, x)$ et de la fonction

de degré c, $h(t)$, de sorte que, dans le domaine $A = P(x)$, z satisfait à une équation $g(t)$ de degré $n = \frac{c}{a}$.

Nous pouvons montrer que, dans le domaine $P(x)$, la fonction $g(t)$ est irréductible. En effet, si $g(t)$ était réductible, supposons que le facteur irréductible de $g(t)$ qui contient la racine z soit $G(t, x)$. Puisque $x = \varphi(z)$, on a

$$G[z, \varphi(z)] = 0.$$

Mais, comme les coefficients de cette équation appartiennent au domaine P, l'équation $G = 0$ s'annule aussi pour les autres valeurs $t = z_1, \ldots, t = z_{n-1}$ pour lesquelles $g(x)$ s'annule, et, par conséquent, à un facteur constant près, $G(x) = g(x)$, et $g(t)$ est irréductible dans le domaine $P(x)$.

Ainsi, le degré de Γ *relativement au domaine* A *est* $\frac{c}{a}$, *s'il était* c *relativement au domaine* P.

Soit y une seconde quantité appartenant au domaine Γ, et formons le *genus* $P(y) = B$. Supposons qu'il y ait une nouvelle distribution des quantités c correspondant au domaine Γ, soit

$$\begin{array}{lllll}
y & = \psi(z) & = \psi(z_1) & = \psi(z_2) & = \ldots = \psi(z_{n-1}), \\
y' & = \psi(z') & = \psi(z'_1) & = \psi(z'_2) & = \ldots = \psi(z'_{n-1}), \\
\ldots & \ldots & \ldots & \ldots & \ldots \\
y^{(a-1)} & = \psi(z^{(a-1)}) & = \psi(z_1^{(a-1)}) & = \psi(z_2^{(a-1)}) & = \ldots = \psi(z_{n-1}^{(a-1)}).
\end{array}$$

On peut montrer que y est une fonction rationnelle de x dont les coefficients appartiennent au domaine P. Si, de plus, les quantités y, y', $\ldots$, $y^{(a-1)}$ sont toutes différentes, x est aussi une fonction rationnelle de y dont les coefficients sont aussi des quantités du domaine P, et les domaines A et B sont identiques. Nous avons ainsi la notion de l'*identité* de deux *genera* $P(x)$ et $P(y)$ qui tous deux sont diviseurs du *genus* $P(z)$.

Nous avons vu que, si le degré a d'un domaine diviseur A est plus petit que le degré c du domaine Γ, il correspond à ce diviseur une distribution des c quantités x, $x^{(1)}$, $\ldots$, $x^{(c-1)}$, en un groupe de n quantités égales. Mais les c ne peuvent être distribués en un système de n parties égales que d'un nombre fini de manières. Il peut se faire qu'à plusieurs de ces distributions il ne corresponde aucune division du

domaine Γ; mais à chaque division il correspondra une seule distribution.

Donc un domaine algébrique n'a qu'un nombre fini de divisions différentes; et l'on peut voir, réciproquement, que, si un domaine n'a qu'un nombre fini de divisions, il est algébrique (*voir*, par exemple, BACHMANN, *Math. Ann.*, t. XVIII, p. 449).

Réduction d'un domaine de rationalité lorsque, au lieu du domaine fondamental P, on prend pour domaine de rationalité un autre domaine $P(y)$ dérivé du domaine fondamental.

La quantité x étant une quantité primitive de $P(x) = A$ satisfait à une équation irréductible $f_a(x) = 0$ de degré a. Soit y une quantité dérivée de P et une quantité primitive du domaine $P(y) = B$ de degré b. Soit, de plus,

$$\Gamma = P(x) \times P(y) = P(z)$$

de degré c le plus petit commun multiple de A et B.

Dès lors, puisque A est un diviseur de Γ, $x = \varphi(z)$ est une fonction rationnelle de z et l'on a $c = a.n$ où n est un entier; de même $c = b.m$ où m est un entier.

De plus, puisque $P(z) = P(x, y)$, z est une fonction rationnelle de x et de y telle que $z = \chi(x, y)$, par exemple.

Si maintenant nous adjoignons y au domaine fondamental, dans le domaine résultant, en vertu des équations $x = \varphi(z)$, $z = \chi(x, y)$, x sera une fonction rationnelle de z et aussi z sera une fonction rationnelle de x. Il résulte par suite que, puisque z est une fonction primitive du domaine $\frac{\Gamma}{B}$, x est aussi une quantité primitive de ce domaine et satisfait à une équation irréductible de degré $\frac{c}{b}$ que nous avons appelée

$$G_{\frac{c}{b}}(u, y) = 0.$$

Dès lors, si P est le domaine de rationalité, le domaine A est de degré a. Mais si $P(y) = B$ est choisi pour domaine de rationalité, A est de degré $a' = \frac{c}{b}$; et dans ce dernier cas A peut être représenté par une

expression de la forme

$$\beta_0 + \beta_1 x + \ldots + \beta_{a'-1} x^{a'-1},$$

où les β sont les quantités rationnelles du domaine $P(y)$. Si, d'autre part, A était ajouté au domaine fondamental P, le degré de B serait

$$b' = \frac{c}{a}.$$

Dès lors, b' et a' sont reliés par la relation $c = ab' = ba'$. Soit $B = P(y)$ un domaine dans lequel y est une quantité primitive, et soit y' une quantité conjuguée de y. Si $F(u, y)$, $G(u, y)$, sont deux fonctions telles que $F(u, y)$ soit divisible par $G(u, y)$, il en résulte que $F(u, y')$ est divisible par $G(u, y')$.

Nous avons dit plus haut que, dans le domaine P, x satisfait à l'équation irréductible $f(u) = 0$, et que, dans le domaine $P(y)$, x satisfait à l'équation irréductible $G_{\frac{c}{b}}(u, y) = 0$. Il en résulte que $f_a(u)$ est divisible par $G_{\frac{c}{b}}(u, y)$ et, par conséquent, aussi par $G_{\frac{c}{b}}(u, y')$, puisque $f_a(u)$ reste invariable quand y' est remplacé par y.

Dès lors, chacune des quantités $G(u, y)$, $G(u, y')$, ..., $G(u, y^{(b-1)})$ contient au moins une des racines de $f(u)$. Et puisque les coefficients du produit de ces fonctions appartiennent au domaine P, il en résulte que ce produit est égal à une puissance de $f(u)$ et par suite à la puissance $\frac{c}{a}$.

Plus grand commun diviseur de deux ou plusieurs domaines.

Soient A et B deux domaines dérivés du domaine fondamental P. Ces deux domaines ont, en général, en plus des quantités qui appartiennent au domaine P, d'autres quantités en commun. Toutes les quantités qui sont communes aux deux domaines forment un autre domaine qu'on appelle le *plus grand commun diviseur* des deux domaines. Si A et B sont des domaines finis, D est aussi fini; et si t est une quantité primitive de D telle que $D = P(t)$, t est une fonction rationnelle de x et y

$$t = \varphi(x), \qquad t = \psi(y).$$

Considérons les quatre domaines définis plus haut A, B, Γ, D de degrés respectivement égaux à a, b, c et d.

La quantité $u = x$ satisfait à l'équation irréductible $f_a(u) = 0$ relativement au domaine P et à l'équation irréductible $G_{\frac{c}{b}}(u, y) = 0$ relativement au domaine $P(y)$. Soit maintenant D le domaine de rationalité donné. Dès lors, relativement à ce domaine, $u = x$ satisfait à l'équation $H_{\frac{a}{d}}(u, t) = 0$, où les coefficients appartiennent au domaine D et, puisque D est un diviseur de B, aussi au domaine B. Par suite, x satisfait dans B à l'équation $H_{\frac{a}{d}}(u, t) = 0$ et, comme nous l'avons dit plus haut, x satisfait aussi dans B à l'équation irréductible $G_{\frac{c}{b}}(u, y) = 0$. Dès lors $H_{\frac{a}{d}}(u, t)$ considéré comme fonction de u doit être divisible par $G_{\frac{c}{b}}(u, y)$ et par conséquent

$$\frac{a}{d} \geq \frac{c}{b}.$$

Sous certaines conditions, $cd = ab$, par exemple dans le cas des *domaines normaux* (Galois) (*voir* C. JORDAN, *Math. Ann.*, t. I, p. 141, ou BACHMANN, *Math. Ann.*, t. XVIII, p. 460).

Si A est un domaine normal, d'après la définition d'un tel domaine les racines $x^{(1)}$, $x^{(2)}$, ..., $x^{(a-1)}$ de l'équation irréductible $f_a(u) = 0$ peuvent s'exprimer rationnellement en fonction de x, quantité primitive à laquelle, dans ce domaine, elles sont conjuguées.

$G(u, y)$, étant un diviseur de $f(u)$, contient quelques-unes des racines de $f(u)$, de sorte que, par conséquent,

$$G(u, y) = (u - x)(u - x')(u - x'')\ldots.$$

Les coefficients de $G(u, y)$ appartiennent au domaine B; mais puisque x', x'', ..., sont des fonctions rationnelles de x, ces coefficients appartiennent aussi au domaine A et, par conséquent aussi à D, le plus grand commun diviseur de A et B. Mais dans D la quantité $u = x$ satisfait à l'équation irréductible $H(u) = 0$; dès lors G est divisible par H et, puisque, d'après ce qui précède, H était divisible par G, il en résulte que $G = H$ ou $ab = cd$.

Égalité relative de deux domaines.

Supposons que du domaine fondamental P on ait dérivé le domaine $P(x) = A$ dans lequel la quantité primitive x satisfait à l'équation irréductible $f_a(u) = 0$, de sorte que chaque quantité appartenant au domaine A peut être mise sous la forme

$$R_0 + R_1 x + R_2 x^2 + \ldots + R_{a-1} x^{a-1},$$

les quantités R appartenant au domaine P.

Supposons maintenant que d'un autre domaine fondamental P′ on ait dérivé le domaine $P'(x) = A'$ dans lequel la quantité primitive x satisfait à la même équation irréductible $f_a(u) = 0$, de sorte que les coefficients de cette équation appartiennent aussi au domaine P′.

Nous dirons que les deux domaines A et A′ sont *relativement égaux*. Les coefficients de $f_a(u) = 0$ appartenant aux deux domaines P et P′ appartiennent au plus grand commun diviseur de ces domaines. Dès lors, toutes les quantités du domaine A′ peuvent être mises sous la forme

$$R_0^1 + R_1^1 x + \ldots + R_{a-1}^1 x^{a-1},$$

où les quantités $R_0^1, \ldots$ appartiennent au domaine diviseur. Nous pouvons maintenant établir comme il suit le théorème démontré plus haut.

Si $cd = ab$, les deux domaines $\frac{\Gamma}{B}$ et $\frac{A}{D}$ sont *relativement égaux*.

Car dans $\frac{A}{D}$ la quantité x est une quantité primitive qui satisfait à l'équation irréductible $H_{\frac{a}{d}}(u) = 0$, et x est aussi une quantité primitive du domaine $\frac{\Gamma}{B}$ satisfaisant à l'équation irréductible $G_{\frac{c}{b}}(u, y) = 0$.

De plus, puisque $G_{\frac{c}{b}}(u, y) = H_{\frac{a}{d}}(u)$, comme nous l'avons montré plus haut, il en résulte que les domaines $\frac{\Gamma}{B}$ et $\frac{A}{D}$ sont relativement équivalents.

Sur les *domaines relatifs de rationalité*, voir HILBERT, *Jahresbericht der Deuts. Math. Vereinigung*, t. IV, p. 203.

Extension de la notion de division. Modules et idéaux.

Nous pouvons dire qu'un nombre entier algébrique μ appartenant au domaine Ω est décomposable en facteurs, s'il existe dans Ω deux entiers algébriques μ_1 et μ_2 différents des unités algébriques de Ω tels que

$$\mu = \mu_1 \mu_2.$$

Cette définition correspond à la définition de la divisibilité des entiers rationnels.

Car si $\mu = \mu_1 \mu_2$, si, de plus, nous désignons le norme de μ par m, et si nous écrivons $N(\mu_1) = m_1$, $N(\mu_2) = m_2$, on a $m = m_1 m_2$, de sorte que la divisibilité de μ par les deux facteurs μ_1 et μ_2 correspond à la décomposition de l'entier rationnel m en deux facteurs qui sont ici m_1 et m_2; aussi, correspondant au cas où les normes sont des nombres premiers, il est clair qu'il existe des entiers algébriques qui ne sont pas décomposables en facteurs.

Mais ici nous rencontrons une difficulté : *La décomposition d'un nombre algébrique en facteurs irréductibles n'est pas unique*. Prenons, par exemple, le domaine $\Omega = P(\theta)$, où

$$\theta^2 + 5 = 0.$$

Dans ce domaine $6 = 2.3 = (1+\theta)(1-\theta)$ et, dans les deux cas, les facteurs sont irréductibles [*voir* DEDEKIND (1), p. 451].

Pour surmonter la difficulté, nous ferons usage de la notion de division généralisée comme il suit par Kummer.

Dans le domaine des nombres rationnels P, nous savons ce que l'on appelle *le plus grand commun diviseur* de plusieurs nombres a, b, c, ... Ce diviseur d peut être mis sous la forme

$$d = ax + by + cz + \ldots,$$

où $x, y, z, \ldots$ sont des entiers déterminés.

---

(1) Nous n'indiquerons que le nom de M. Dedekind lorsque l'on devra se reporter à la *Dirichlet's Zahlentheorie*, par Dedekind, 4e édition.

Nous pourrons dire qu'un nombre rationnel m est divisible par le complexe $a, b, c, \ldots$, lorsque nous pourrons déterminer des entiers $x', y', z', \ldots$ tels que

$$m = ax' + by' + cz' + \ldots.$$

Mais il est clair que, tant que nous resterons dans le domaine P, cette conception de la divisibilité sera superflue, puisque tout nombre divisible par le complexe $a, b, c, \ldots$ est divisible par le plus grand commun diviseur d des nombres $a, b, c, \ldots$, et tout nombre qui est divisible par d est divisible aussi par le complexe $a, b, c, \ldots$. Dès lors, tant que nous resterons dans le domaine des nombres rationnels, la notion de divisibilité par le complexe $a, b, c, \ldots$ est identique à celle de la divisibilité par d.

L'entier m est divisible par d s'il existe un entier x tel que $m = dx$.

Nous avons encore le théorème suivant : *Si le produit de plusieurs entiers est divisible par un nombre premier p, au moins l'un de ses facteurs est divisible par p*; de là, il résulte que tout entier est décomposable en un produit d'un nombre fini de facteurs entiers et cela d'une seule manière.

Mais si le domaine Ω est un domaine algébrique arbitraire, on dit encore qu'un nombre algébrique μ de ce domaine est divisible par un entier algébrique δ appartenant à Ω si l'on peut déterminer dans Ω un entier algébrique ξ tel que l'on ait $\mu = \delta\xi$.

On dit de même que le nombre algébrique μ est divisible par le complexe formé des nombres algébriques $\alpha, \beta, \gamma, \ldots$ de Ω si l'on peut déterminer dans Ω des entiers algébriques $\xi, \eta, \zeta, \ldots$ tels que

$$\mu = \alpha\xi + \beta\eta + \gamma\zeta + \ldots.$$

Cette conception n'est plus superflue. Car supposons que δ soit un autre nombre algébrique par lequel les nombres algébriques $\alpha, \beta, \gamma, \ldots$ soient divisibles, chaque nombre qui est divisible par le complexe $\alpha, \beta, \gamma, \ldots$ est aussi divisible par δ. Mais la proposition inverse n'est pas vraie; tout nombre qui est divisible de δ n'est pas forcément divisible par le complexe $\alpha, \beta, \gamma, \ldots$; car, dans ce cas, δ doit avoir la forme

$$\delta = \alpha\xi' + \beta\eta' + \gamma\zeta' + \ldots,$$

où $\xi', \eta', \zeta', \ldots$ sont des entiers algébriques de Ω, et, dans cette hypothèse, δ est divisible par chaque diviseur commun aux nombres α, β, γ, ... et doit être, par conséquent, le plus grand commun diviseur de ces nombres dans le sens qu'on lui donne ordinairement dans la théorie des entiers rationnels.

Mais, dans ce sens, le plus grand commun diviseur des nombres algébriques $\alpha, \beta, \gamma, \ldots$ n'existe que tant que nous restons dans le domaine infini des entiers algébriques. Si nous ne considérons plus le domaine Ω, il existe quelque chose qui est l'analogue du plus grand commun diviseur des nombres rationnels. D'autre part, à moins que nous ne prenions un domaine fini de rationalité déterminée auquel toutes nos quantités doivent appartenir, il n'existe rien d'analogue au nombre premier, et la notion de décomposition unique d'un entier en facteurs premiers n'existe plus. En effet, tant que nous resterons dans le domaine infini de tous les nombres algébriques, si α est un entier algébrique, $\alpha = \sqrt{\alpha}\sqrt{\alpha}$ et $\sqrt{\alpha}$ est aussi un nombre algébrique. Par conséquent tout entier algébrique est décomposable en facteurs *ad infinitum*.

Dès lors, la notion de divisibilité par le complexe des nombres algébriques $\alpha, \beta, \gamma, \ldots$ n'est plus superflue lorsque nous nous limitons à un domaine fini déterminé Ω; et nous pouvons, par conséquent, dire qu'*un nombre algébrique* μ *est divisible par le complexe* $\alpha, \beta, \gamma, \ldots$ *s'il est possible de déterminer des entiers algébriques* $\xi, \eta, \zeta, \ldots$ *tels que*

$$\mu = \alpha\xi + \beta\eta + \gamma\zeta + \ldots,$$

où toutes les quantités introduites appartiennent au domaine Ω.

Par cette définition, nous arrivons à la théorie des formes linéaires

$$\alpha\xi + \beta\eta + \gamma\zeta + \ldots,$$

où les variables $\xi, \eta, \zeta, \ldots$, sont des entiers algébriques de Ω, tandis que les *coefficients* de la forme linéaire $\alpha, \beta, \gamma, \ldots$ sont des nombres entiers ou fractionnaires du domaine Ω.

L'ensemble des nombres algébriques qui sont représentés par la forme linéaire

$$\alpha x + \beta y + \gamma z + \ldots,$$

où les coefficients sont des nombres de Ω et $x, y, z, \ldots$ des *entiers*

rationnels, est appelé par Dedekind (p. 494) *module* (1) et désigné par $[\alpha, \beta, \gamma, \ldots] = \mathfrak{a}$, par exemple. Les quantités $\alpha, \beta, \gamma, \ldots$ s'appellent les *éléments* du module.

La définition suivante du module est plus générale et plus abstraite en ce qu'elle ne fait pas intervenir la conception de la forme linéaire : *Un module est un système de nombres ayant la propriété suivante : la différence de deux nombres quelconques du système est un nombre qui appartient au système.*

Un nombre μ est divisible par le module $[\alpha, \beta, \gamma, \ldots]$, lorsque l'on peut déterminer des entiers rationnels $x, y, z, \ldots$, tels que

$$\mu = \alpha x + \beta y + \gamma z + \ldots;$$

et le module

$$\mathfrak{b} = (\beta_1, \beta_2, \beta_3, \ldots)$$

est divisible par le module

$$\mathfrak{a} = (\alpha_1, \alpha_2, \alpha_3, \ldots),$$

lorsque $\beta_i (i = 1, 2, 3, \ldots)$ est divisible par $\mathfrak{a}$, ou, ce qui revient au même, lorsque tout nombre divisible par $\mathfrak{b}$ est aussi divisible par $\mathfrak{a}$.

Si tous les nombres divisibles par le module $\mathfrak{a}$ peuvent être mis sous la forme

$$\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n,$$

où $x_1, x_2, \ldots, x_n$ sont des entiers rationnels et les coefficients $\alpha_1, \alpha_2, \ldots, \alpha_n$ des nombres divisibles par le module $\mathfrak{a}$, le module $\mathfrak{a}$ est appelé *module fini* de *rang* n, et les quantités $\alpha_1, \alpha_2, \ldots, \alpha_n$ s'appellent *base* de ce module.

Le *produit* $\mathfrak{ab}$ de deux modules $\mathfrak{a}$ et $\mathfrak{b}$ peut être défini comme le complexe de nombres formés en ajoutant de toutes les façons possibles les produits $\alpha\beta$ où l'on doit prendre pour α tout nombre divisible par $\mathfrak{a}$ et pour β tout nombre divisible par $\mathfrak{b}$.

---

(1) Comme le fait Dedekind (p. 541), nous appellerons cet ensemble de nombres un *module* pour ne pas confondre avec le mot *modulus* de Gauss. Ces mots ont respectivement *modules* et *moduli* pour pluriels.

En particulier le produit de deux modules finis

$$\mathfrak{a} = (\alpha_1, \alpha_2, \ldots, \alpha_n) \qquad \text{et} \qquad \mathfrak{b} = (\beta_1, \beta_2, \ldots, \beta_m)$$

est

$$\mathfrak{ab} = (\alpha_1\beta_1, \alpha_1\beta_2, \ldots, \alpha_1\beta_m, \alpha_2\beta_1, \alpha_2\beta_2, \ldots, \alpha_2\beta_m, \ldots, \alpha_n\beta_1, \alpha_n\beta_2, \ldots, \alpha_n\beta_m).$$

Le quotient des deux modules $\mathfrak{a}$ et $\mathfrak{b}$ peut se définir comme étant le complexe $\mathfrak{k}$ de tous les nombres k, tels que $\mathfrak{ka} > \mathfrak{b}$ où, avec Dedekind (p. 495), nous emploierons $>$ comme symbole de la division; de sorte que $\mathfrak{ka} > \mathfrak{b}$ signifie que $\mathfrak{ka}$ *est divisible* par $\mathfrak{b}$.

Si l'on a $\mathfrak{ka} > \mathfrak{b}$, on a aussi $\mathfrak{k} > \frac{\mathfrak{b}}{\mathfrak{a}}$ et *vice versa :* si $\mathfrak{k} > \frac{\mathfrak{b}}{\mathfrak{a}}$ on a aussi $\mathfrak{ka} > \mathfrak{b}$.

Soit $\mathfrak{b}$ un module et désignons par $\mathfrak{a}^0$ le module $\frac{\mathfrak{a}}{\mathfrak{a}}$. Dès lors le module $\mathfrak{a}^0$ est formé de tous les nombres k qui sont tels que $\mathfrak{ka} > \mathfrak{a}$. Il est clair que l'unité est comprise parmi ces nombres et par conséquent

$$1 > \mathfrak{a}^0.$$

Si maintenant $\mathfrak{k}$ est un module et si $\mathfrak{ka} > \mathfrak{a}$, on a $\mathfrak{k} > \mathfrak{a}^0$; et si $\mathfrak{k} > \mathfrak{a}^0$, on a $\mathfrak{ka} > \mathfrak{a}$.

Sur le module $\mathfrak{a}^0$, on peut démontrer les théorèmes suivants

1° $\qquad \mathfrak{a}\mathfrak{a}^0 = \mathfrak{a},$

2° $\qquad \frac{\mathfrak{a}}{\mathfrak{a}^0} = \mathfrak{a},$

3° $\qquad \mathfrak{a}^0\mathfrak{a}^0 = \mathfrak{a}^0,$

4° $\qquad \frac{\mathfrak{a}^0}{\mathfrak{a}^0} = \mathfrak{a}^0.$

Un module ε qui a les deux propriétés

1° $\qquad \varepsilon\varepsilon > \varepsilon,$

2° $\qquad 1 > \varepsilon$

est appelé par Kronecker un *Art* ou *Species* (*Grundzüge*, p. 15); par Dedekind (p. 505) un *ordre* (*Ordnung*).

Puisque $1 > \varepsilon$, on voit que tous les entiers rationnels sont divisibles par un *species*.

Nous pouvons donc appeler $\mathfrak{a}^0$ le species de module $\mathfrak{a}$. Ce module $\mathfrak{a}^0$ a, pour le module $\mathfrak{a}$, les mêmes propriétés que l'*unité* dans le domaine des nombres rationnels.

Modules de rang n dans un domaine de degré n. — Les modules qui appartiennent à un domaine Ω de degré n peuvent être soit finis, soit infinis. Dedekind (p. 497) donne un exemple de module infini. Dans un domaine de degré n le rang d'un module fini ne peut être plus grand que n; sinon le domaine contiendrait plus de n quantités indépendantes. Si donc $\mathfrak{a} = [\alpha_1, \alpha_2, \ldots, \alpha_n]$ est un module dans Ω et de rang n, et si les éléments $\alpha_1, \alpha_2, \ldots, \alpha_n$ forment une base de ce module, tous les nombres qui appartiennent au module peuvent être mis sous la forme

$$\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n,$$

où les x sont des *entiers rationnels;* et tous les nombres appartenant au domaine Ω sont de la forme

$$\alpha_1 r_2 + \alpha_2 r_2 + \ldots + \alpha_n r_n,$$

où les r sont des *nombres rationnels*.

Supposons que β soit une quantité arbitraire du domaine Ω, telle que

$$\beta = \alpha_1 \rho_1 + \alpha_2 \rho_2 + \ldots + \alpha_n \rho_n$$

et supposons que l'entier ρ soit le plus grand commun diviseur des entiers qui entrent dans les dénominateurs de $\rho_1, \rho_2, \ldots, \rho_n$; on a

$$\rho\beta = \alpha_1 \rho_1 \rho + \alpha_2 \rho_2 \rho + \ldots + \alpha_n \rho_n \rho.$$

Puisque $\rho_1\rho, \rho_2\rho, \ldots, \rho_n\rho$ sont des entiers, il est clair que $\rho\beta$ est divisible par le module $\mathfrak{a}$. Dès lors, nous avons le théorème suivant:

Toute quantité appartenant au domaine Ω peut, en la multipliant par un entier rationnel, donner une quantité qui appartienne au module $\mathfrak{a}$.

Un domaine est un module de rang infini. Tous les entiers algébriques qui appartiennent a Ω (domaine de degré n) forment un *module fini de rang n.* Dedekind désigne ce module par o (p. 537). Si les n

entiers algébriques $\omega_1, \omega_2, \ldots, \omega_n$ forment une base du module φ, la forme linéaire

$$\omega_1 x_1 + \omega_2 x_2 + \ldots + \omega_n x_n$$

représente, pour des valeurs entières et rationnelles des variables $x_1, x_2, \ldots, x_n$ les entiers algébriques du domaine Ω, et tout entier algébrique de Ω peut être mis sous la forme

$$\omega_1 x_1 + \omega_2 x_2 + \ldots + \omega_n x_n,$$

où $x_1, x_2, \ldots, x_n$ sont des entiers rationnels.

Modules entiers. — Nous pouvons maintenant définir un module entier, *un module qui est divisible par le module* φ.

Puisque tout domaine, à l'exception du domaine trivial formé seulement de zéros, contient l'unité, il en résulte que le module φ est tel que

$$1 > \varphi$$

et, par conséquent, il en résulte aussi que les entiers rationnels sont divisibles par φ.

Puisque le produit et la somme d'entiers algébriques sont des entiers algébriques, nous avons aussi

$$(a) \qquad \varphi\varphi \quad \text{ou} \quad \varphi^2 > \varphi.$$

De plus, puisque $1 > \varphi$ et $\varphi > \varphi$, on a

$$(b) \qquad \varphi > \varphi^2,$$

et, de (a) et (b), nous déduisons

$$\varphi = \varphi^2.$$

Dès lors, φ est un *species*.

Puisque, de plus,

$$\varphi^0 = \frac{\varphi}{\varphi} = \varphi,$$

on voit que φ est son propre *species*.

Nous appellerons, par conséquent, φ le *species principal*. Kronecker se sert aussi du mot *Hauptart* (*Grundzüge*, p. 15).

Entiers algébriques. — Nous pouvons aussi donner une nouvelle et meilleure définition d'un entier algébrique : *Si η est un nombre algébrique tel qu'il existe un module fini* $\mathfrak{a}$, *tel que* $\eta\mathfrak{a} > \mathfrak{a}$, η *est un entier algébrique, et si* η *est un entier algébrique, il existe un module fini tel que* $\eta\mathfrak{a} > \mathfrak{a}$.

Étant donnée cette définition des entiers algébriques, on peut établir les théorèmes suivants :

1° *Si* α *et* β *sont des entiers algébriques, la somme, la différence et le produit de* α *et* β *sont des entiers algébriques;*

2° *Si* ω *satisfait a une équation algébrique dans laquelle le coefficient de la plus haute puissance de la variable est l'unité et les autres coefficients sont des entiers algébriques,* ω *est un entier algébrique.*

Soit Ω un domaine algébrique de degré n et soient μ, α, β, γ, ... des nombres arbitraires appartenant à ce domaine. On dit que μ est divisible par le complexe α, β, γ, ... lorsqu'il existe dans Ω des nombres algébriques ξ, η, ζ, ..., 1°, qui ont la propriété d'être des entiers algébriques et, 2°, qui sont tels que

$$\mu = \alpha\xi + \beta\eta + \gamma\zeta + \dots.$$

On voit que le système des nombres tels que μ, qui peuvent être représentés par l'expression ci-dessus, forment un module d'après la définition générale du module donnée p. 30.

De plus, si $\omega_1, \omega_2, \dots, \omega_n$ est une base du système ν d'entiers algébriques de Ω telle que

$$\begin{aligned}
\xi &= \omega_1 x_1^{(1)} + \omega_2 x_2^{(1)} + \dots + \omega_n x_n^{(1)},\\
\eta &= \omega_1 x_1^{(2)} + \omega_2 x_2^{(2)} + \dots + \omega_n x_n^{(2)},\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots,
\end{aligned}$$

μ a la forme

$$\begin{aligned}
\mu = \quad & \alpha\omega_1 x_1^{(1)} + \alpha\omega_2 x^{(1)} + \dots + \alpha\omega_n x_n^{(1)}\\
& + \beta\omega_1 x^{(2)} + \beta\omega_2 x^{(1)} + \dots + \beta\omega_n x_n^{(2)}\\
& + \dots\dots\dots\dots\dots\dots\dots\dots\dots.
\end{aligned}$$

Puisque $\alpha\omega_1, \alpha\omega_2, \dots$ sont des nombres appartenant au domaine Ω, on voit que μ peut être donnée par une forme linéaire d'un nombre fini d'entiers rationnels dont les coefficients appartiennent à Ω.

Comme ce nombre est fini, le rang de ce module ne peut être plus grand que le degré n de Ω et, de plus, puisque $\omega_1, \omega_2, \ldots, \omega_n$ sont indépendants, le rang n'est pas inférieur à n.

Dès lors, le module formé de tous ces nombres algébriques μ du domaine Ω, qui peuvent se mettre sous la forme

$$\alpha\xi + \beta\eta + \gamma\zeta + \ldots,$$

où les coefficients $\alpha, \beta, \gamma, \ldots$ sont des quantités entières ou fractionnaires de Ω et les nombres $\xi, \eta, \zeta, \ldots$ des entiers algébriques de Ω, est un module de rang n dans le domaine Ω de degré n.

Ce système de nombres s'appellera un *idéal* et sera désigné par $(\alpha, \beta, \gamma, \ldots)$. Si, dès lors, $\alpha, \beta, \gamma, \ldots$ sont des quantités de Ω, *l'idéal* $(\alpha, \beta, \gamma, \ldots)$ *est formé de tous les nombres contenus dans l'expression*

$$\alpha\xi + \beta\eta + \gamma\zeta + \ldots,$$

où $\xi, \eta, \zeta, \ldots$ *sont des entiers algébriques de* Ω, *tandis que le module* $[\alpha, \beta, \gamma, \ldots]$ *est formé de tous ceux de ces nombres qui sont contenus dans l'expression*

$$\alpha\xi + \beta\eta + \gamma\zeta + \ldots,$$

où $\xi, \eta, \zeta, \ldots$ *sont des nombres entiers rationnels.*

On voit en même temps (*voir* DEDEKIND, p. 551) que si

$$\mathfrak{a} = (\alpha, \beta, \gamma, \ldots),$$

$$\rho\mathfrak{a} = \mathfrak{a}, \qquad \frac{\mathfrak{a}}{\rho} = \mathfrak{a} \qquad \text{et aussi} \qquad \mathfrak{a}^0 = \rho.$$

De la dernière relation, il résulte que le *species* d'un idéal est le *species* principal. Nous pouvons alors définir les idéaux comme étant *ceux des modules finis dont le species est le species principal.*

Le *species* principal ρ est lui-même un idéal, puisque $\rho\rho = \rho$, et cet idéal ρ a la même place dans le domaine Ω que l'unité dans le domaine des nombres rationnels.

Un idéal est *entier* lorsqu'il ne renferme que des nombres entiers algébriques. Dans le présent Mémoire, nous n'aurons à considérer que des idéaux entiers, et la discussion qui va suivre se bornera aux idéaux de cette sorte.

Avec Dedekind (*note* de la p. 495), nous désignerons le plus grand commun diviseur de deux modules par le symbole + et par le symbole — le plus petit commun multiple de deux modules.

Deux idéaux $\mathfrak{a}$ et $\mathfrak{b}$ sont premiers entre eux lorsque

$$\mathfrak{a} + \mathfrak{b} = \mathfrak{o}.$$

Un idéal entier $\mathfrak{a}$, qui n'est divisible par aucun autre idéal entier, sauf par $\mathfrak{a}$ et $\mathfrak{o}$, s'appelle un idéal *premier;* et si $\mathfrak{a}$ n'a pas cette propriété, on l'appelle un idéal *composé*.

Système modulaire de Kronecker. Congruences supérieures.

Dans les *Disquisitiones Arithmeticæ* (Art. 1), Gauss donne la définition suivante : Si la différence de deux entiers rationnels a et b est divisible par l'entier rationnel m, les entiers a et b sont dits *congruents* relativement à m; nous appellerons m le *modulus* et chacun des entiers a et b est dit, dans le premier cas, un *résidu* de l'autre; dans le second cas, un *non-résidu*.

Plus loin (Art. 2), il montre que tous les résidus d'un nombre entier a, relativement au modulus m, sont contenus dans la formule

$$a + km,$$

où k est un entier indéterminé.

Dès lors, tous les entiers qui peuvent être mis sous la forme

$$\ldots, \quad a - 3m, \quad a - 2m, \quad a - m, \quad a, \quad a + m, \quad a + 2m \quad a + 3m, \quad \ldots,$$

seront dits *congruents, modulo m*, et la série des nombres $a + km$ est complètement déterminée par les deux quantités suivantes : le modulus donné m et un terme quelconque de la série.

Kronecker (*Werke*, t. III[1], p. 148, ou *Journal de Crelle*, t. 99, p. 330 et suiv.) dit que deux formes linéaires des variables x et x',

$$a + bx, \qquad a' + b'x'$$

sont *équivalentes*, si l'une peut se transformer en l'autre par les substitutions entières

$$x = \alpha x' + \beta, \qquad x' = \alpha' x + \beta'.$$

Les conditions nécessaires et suffisantes de cette équivalence sont donc

$$b = \pm b', \qquad a \equiv a' \pmod{b};$$

de sorte que la conception de la congruence de nombres $a \equiv a' \pmod{m}$ est entièrement identique à la conception de l'équivalence des formes linéaires $a + mx$ et $a' + m'x'$ (*voir* aussi KRONECKER, t. III¹, p. 114). Le passage naturel de la notion de congruence à un seul modulus à la notion plus générale de congruences relatives à un système de moduli s'impose immédiatement lorsque, au lieu de formes linéaires à une variable, nous considérons des formes linéaires d'un nombre quelconque de variables telles que

$$a + m_1 x_1 + m_2 x_2 + \ldots + m_\mu x_\mu,$$

où toutes les quantités introduites sont des entiers rationnels; et, comme plus haut, nous dirons que les deux formes

$$a + \sum_{h=1}^{h=\mu} m_h x_h, \qquad a' + \sum_{k=1}^{k=\nu} m'_k x'_k$$

sont équivalentes, lorsque l'une peut se transformer dans l'autre par les substitutions entières

$$x_h = c_{h0} + \sum_k c_{hk} x'_k, \qquad x'_k = c_{k0} + \sum_h c'_{kh} x_h$$
$$(h = 1, 2, \ldots, \mu;\ k = 1, 2, \ldots, \nu),$$

dans lesquels les c sont des entiers rationnels.

Dès lors, les conditions nécessaires et suffisantes pour que les formes

$$a + \sum_{h=1}^{h=\mu} m_h x_h \qquad \text{et} \qquad a' + \sum_{k=1}^{k=\nu} m'_k x'_k$$

soient équivalentes sont exprimées par les équations

$$(\mathrm{A}) \qquad a = a' + \sum_k c'_{k0} m'_k, \qquad a' = a + \sum_h c_{h0} m_h,$$

$$(\mathrm{B}) \qquad m_h = \sum_k c'_{kh} m'_k, \qquad m'_k = \sum_h c_{hk} m_h$$
$$(h = 1, 2, \ldots, \mu;\ k = 1, 2, \ldots, \nu).$$

Les coefficients entiers c et c' dans les équations (A) et (B) ont des valeurs particulières. Donnons-leur toutes les valeurs entières; comme dans le cas d'un seul module, l'*ensemble* des nombres qui peuvent se mettre sous la forme

$$a + \sum_{h=1}^{h=\mu} c_{h0} m_h$$

peut être caractérisé en disant qu'ils sont congruents l'un à l'autre, relativement au système modulaire $[m_1, m_2, \ldots, m_\mu]$.

Si nous tenons compte des relations (B), l'ensemble des nombres qui appartiennent à la forme

$$a + \sum_{h=1}^{h=\mu} c_{h0} m_h$$

est le même que celui des nombres qui appartiennent à la forme

$$a' + \sum_{k=1}^{k=\nu} c'_{k0} m'_k,$$

de sorte que la notion de l'équivalence des deux systèmes modulaires

$$(m_1, m_2, \ldots, m_\mu) \quad \text{et} \quad (m'_1, m'_2, \ldots, m'_\nu)$$

en est une conséquence naturelle. Ces équations (B) sont, par conséquent, *caractéristiques* de l'équivalence

$$(m_1, m_2, \ldots, m_\mu) \backsim (m'_1, m'_2, \ldots, m'_\nu).$$

Dès lors, les conditions nécessaires et suffisantes de l'équivalence des formes linéaires

$$a + \sum_{h=1}^{h=\mu} m_h x_h \qquad \text{et} \qquad a' + \sum_{k=1}^{k=\nu} m'_k x'_k$$

sont exprimées par la congruence

$$a \equiv a_1 \pmod{m_1, m_2, \ldots, m_\mu},$$

en même temps que l'équivalence

$$(m_1, m_2, \ldots, m_\mu) \backsim (m'_1, m'_2, \ldots, m'_\nu).$$

En procédant de même, nous pouvons étendre la notion de systèmes modulaires, dans le cas traité ci-dessus, au cas plus général où A, M_1, M_2, ..., M_μ; A', M'_1, M'_2, ..., M'_ν sont des quantités entières du domaine Ω.

Nous définirons l'équivalence des systèmes modulaires

$$(M_1, M_2, \ldots, M_\mu) \quad \text{et} \quad (M'_1, M'_2, \ldots, M'_\nu),$$

et la congruence de deux quantités A et A' relativement à l'un de ces systèmes modulaires par le système d'équations

$$(A) \qquad A = A' + \sum_k b'_{k0} M'_k, \qquad A' = A + \sum_h b_{h0} M_h,$$

$$(B) \qquad M_h = \sum_k b'_{kh} M'_k, \qquad M'_k = \sum_h b_{hk} M_h$$

$$(h = 1, 2, \ldots, \mu; \; k = 1, 2, \ldots, \nu),$$

dans lesquelles les b et les b' sont des quantités entières de Ω.

Ces mêmes équations servent aussi à définir l'équivalence des formes linéaires

$$A + \sum_{h=1}^{h=\mu} M_h X_h \quad \text{et} \quad A' + \sum_{k=1}^{k=\nu} M'_k X'_k,$$

puisque, à l'aide des équations (A) et (B), ces formes peuvent être transformées l'une dans l'autre par des substitutions à coefficients entiers appartenant à Ω; et l'équivalence de ces deux formes linéaires est *caractérisée* par la congruence

$$A \equiv A' \,(\mathrm{mod}\, M', M_2, \ldots, M_\mu),$$

en même temps que l'équivalence

$$(M_1, M_2, \ldots, M_\mu) \backsim (M'_1, M'_2, \ldots, M'_\nu).$$

Si les μ équations (B) sont vérifiées, c'est-à-dire si

$$M_h \equiv 0 \,(\mathrm{mod}\, M'_1, M'_2, \ldots, M'_\nu) \qquad (h = 1, 2, \ldots, \mu),$$

on dit que le système modulaire $(M_1, M_2, \ldots, M_\mu)$ *contient* le système $(M'_1, M'_2, \ldots M'_\nu)$, et si les deux systèmes se contiennent l'un et l'autre,

nous avons l'équivalence (1)

$$(M_1, M_2, \ldots, M_\mu) \backsim (M'_1, M'_2, \ldots, M'_\nu).$$

Dès lors, si nous nous servons de la notion de division déjà introduite, et si nous disons qu'une quantité k est divisible par le système modulaire

$$(M'_1, M'_2, \ldots, M'_\nu)$$

lorsque

$$k \equiv 0 \pmod{M'_1, M'_2, \ldots, M'_\nu},$$

nous voyons qu'un système modulaire *contient* un autre système modulaire lorsque chaque élément du premier système est divisible par le second système, c'est-à-dire si

$$(M_1, M_2, \ldots, M_\mu) \equiv 0 \pmod{M'_1, M'_2, \ldots, M'_\nu},$$

ou, en se servant du symbole de la division dû à Dedekind, si l'on a

$$(M_1, M_2, \ldots, M_\mu) > (M_1, M'_2, \ldots, M'_\nu).$$

De même si

$$(M'_1, M'_2, \ldots, M'_\nu) > (M_1, M_2, \ldots, M_\mu),$$

nous avons l'équivalence

$$(M_1, M_2, \ldots, M_\mu) \backsim (M'_1, M'_2, \ldots, M'_\nu).$$

De ce qui précède il résulte qu'un système modulaire contient un autre système modulaire lorsqu'il est divisible par ce système modulaire. Dès lors, les deux notions : *être divisible par* et *être contenu dans*, qui sont, dans le langage usuel, opposées l'une à l'autre, sont ici identiques.

Si, pour abréger, nous désignons le système modulaire

$$(M_1, M_2, \ldots, M_\mu)$$

par M, et si nous posons

$$(M'_1, M'_2, \ldots, M'_\nu) = M',$$

---

(1) *Voir* KRONECKER, *Journal de Crelle*, t. 99, p. 432, ou *Werke*, III^1, p. 151, et aussi *Journal de Crelle*, t. 92, p. 77, ou *Werke*, II, p. 334.

nous dirons que *le système modulaire* M *est divisible par le système modulaire* M′ *lorsque toute quantité divisible par* M *est aussi divisible par* M′.

Cette définition est en contradiction avec la notion habituelle de division; car ici la partie est divisible par le tout. Elle est aussi en contradiction avec la notion de divisibilité de deux domaines de rationalité, mais comme nous n'aurons guère à nous occuper des domaines de rationalité, qui, comme nous l'avons dit ci-dessus, ne sont pas des modules finis, nous ne risquons pas de faire de confusion.

Si M est divisible par M′, nous dirons que M′ est un *diviseur* de M et que M est un *multiple* de M′.

Si $M > M'$ et $M' > M''$, on a $M > M''$.

Les éléments $M_1, M_2, \ldots, M_\mu$; $M'_1, M'_2, \ldots, M'_\nu$ ont été définis comme étant des quantités entières du domaine Ω.

Nous prendrons pour les éléments $M_1, \ldots, M_\mu, M'_1, \ldots, M'_\nu$ des fonctions entières d'une ou de plusieurs variables dont les coefficients sont des entiers algébriques de Ω, et nous nous imposerons de plus la condition que μ et ν soient des entiers finis.

Il est évident que tout système $(M_1, M_2, \ldots, M_\mu)$ peut être transformé en un système équivalent en *ajoutant* ou en *retranchant* de chaque élément du système un ou plusieurs des autres éléments; et tout élément peut être ajouté à un système modulaire ou en être enlevé lorsque cet élément est divisible par les éléments qui restent (la divisibilité étant prise dans le sens que nous avons employé plus haut).

Supposons que

$$(I) \qquad [p, f_1(x), f_2(x), \ldots, f_n(x), h_1(x), h_2(x), \ldots, h_m(x)]$$

soit un système modulaire dans lequel p est un entier rationnel premier, $f_1(x), f_2(x), \ldots, f_n(x), h_1(x), h_2(x), \ldots, h_m(x)$ des fonctions entières en x à coefficients entiers rationnels, ou, comme nous dirons pour abréger, des fonctions qui appartiennent au domaine d'intégrité $[1, x]$; les entiers m et n sont finis. Le domaine général d'intégrité est ainsi limité au cas très spécial $[1, x]$, afin de pouvoir démontrer un théorème qui éclaircira plusieurs des principes fondamentaux déjà établis.

Nous dirons (*voir* aussi p. 29) qu'une fonction $f(x)$ est *divisible* par une fonction $g(x)$ relativement au modulus p, lorsque nous pourrons trouver dans le domaine d'intégrité $[1, x]$ deux fonctions $\varphi(x)$ et $\psi(x)$, telles que

$$f(x) = g(x)\,\varphi(x) + p\,\psi(x),$$

ou

$$f(x) = g(x)\,\varphi(x) \pmod p.$$

Lorsqu'on ne peut pas trouver de telles fonctions on dit que $f(x)$ est *irréductible* $(\mathrm{mod}\, p)$.

Nous allons démontrer le théorème suivant :

Si les m fonctions précédentes $h_1(x), h_2(x), \ldots, h_m(x)$ *dépendent linéairement des n fonctions linéairement indépendantes* $f_1(x), f_2(x), \ldots, f_n(x)$ $(\mathrm{mod}\, p)$, *le système* (I) *peut être remplacé par un système qui ne contient que n éléments qui sont linéairement indépendants* $(\mathrm{mod}\, p)$.

En effet, si $h_1(x)$ dépend linéairement des fonctions $f(x)$, nous avons

$$h_1(x)\,k(x) \equiv f_1(x)\,\varphi_1(x) + f_2(x)\,\varphi_2(x) + \ldots + f_n(x)\,\varphi_n(x),$$

où $k(x)$, $\varphi_1(x)$, $\varphi_2(x)$, $\ldots$, $\varphi_n(x)$ sont des fonctions de $[1, x]$.

De plus si

$$k(x) \equiv g_1(x)\,k_1(x) \pmod p,$$

où $g_1(x)$ est irréductible $(\mathrm{mod}\, p)$, il s'ensuit que

$$(1)\quad g_1(x)\,k_1(x)\,h_1(x) \equiv f_1(x)\,\varphi_1(x) + f_2(x)\,\varphi_2(x) + \ldots + f_n(x)\,\varphi_n(x) \pmod p,$$

et que toutes les fonctions $\varphi_1(x)$, $\varphi_2(x)$, $\ldots$, $\varphi_n(x)$ ne sont pas divisibles par $g_1(x)$ $(\mathrm{mod}\, p)$; sinon $g_1(x)$ pourrait être mis en facteur dans l'expression (1).

Supposons que $g_1(x)$ et $\varphi_1(x)$ n'aient pas de facteur commun $(\mathrm{mod}\ p)$, de sorte que nous puissions, par conséquent, par l'algorithme du plus grand commun diviseur, déterminer deux facteurs $G_1(x)$ et $\Phi_1(x)$ tels que

$$g_1(x)\,G_1(x) + \varphi_1(x)\,\Phi_1(x) \equiv 1 \pmod p.$$

En multipliant la congruence (1) par $G_1(x)$, nous avons

$$[1 - \varphi_1(x)\,\Phi_1(x)]\,k_1(x)\,h_1(x) \equiv G_1(x)\,[f_1(x)\,\varphi_1(x) + f_2(x)\,\varphi_2(x) + \ldots + f_n(x)\,\varphi_n(x)] \pmod p,$$

ou, si nous posons

$$(a) \qquad G_1(x) f_1(x) - \Phi_1(x) k_1(x) h_1(x) = f^{(1)}(x),$$

il s'ensuit que

$$(2) \quad k_1(x) h_1(x) \equiv \varphi_1(x) f^{(1)}(x) + G_1(x)[f_2(x)\varphi_2(x) + \ldots + f_n(x)\varphi_n(x)] \pmod{p};$$

De même, en multipliant (1) par $\Phi_1(x)$, nous avons

$$\Phi_1(x) g_1(x) k_1(x) h_1(x) \equiv f_1(x)[g_1(x) G_1(x) - 1] + \Phi_1(x)[f_2(x)\varphi_2(x) + \ldots + f_n(x)\varphi_n(x)] \pmod{p}$$

ou

$$(3) \quad f_1(x) \equiv g_1(x) f^{(1)}(x) + \Phi_1(x)[f_2(x)\varphi_2(x) + \ldots + f_n(x)\varphi_n(x)] \pmod{p}.$$

On voit, d'après la relation (a), que $f^{(1)}(x)$ peut être ajouté comme élément au système modulaire (I), et d'après (3) il s'ensuit que, lorsque cela aura été fait, nous pourrons enlever $f_1(x)$ de ce système.

Nous remarquerons de plus que $f^{(1)}(x), f_2(x), f_3(x), \ldots, f_n(x)$ sont linéairement indépendants et que les éléments $h_1(x), h_2(x), \ldots, h_m(x)$ peuvent s'exprimer linéairement en fonction de ces éléments.

En comparant les relations (1) et (2), on voit que, dans le premier cas :

$g_1(x) k_1(x) h_1(x)$ peut s'exprimer linéairement en fonction de $f_1(x), f_2(x), \ldots, f_n(x)$, et dans le second cas que $k_1(x) h_1(x)$ peut s'exprimer linéairement en fonction de $f^{(1)}(x), f_2(x), \ldots, f_n(x)$.

Mais, dans le second cas, nous avons fait disparaître un des facteurs irréductibles $(\mathrm{mod}\, p)$ $g_1(x)$ de $k(x)$.

En continuant de la sorte, nous pouvons arriver à faire disparaître, l'un après l'autre, tous les facteurs irréductibles de $k(x)$ et, par conséquent, $k(x)$ lui-même. Nous aurons donc finalement exprimé $h_1(x)$ par une fonction linéaire de n variables indépendantes qui remplace $f_1(x), f_2(x), \ldots, f_n(x)$ dans un autre système, sans que le système initial cesse de rester équivalent à lui-même. L'élément $h_1(x)$ peut être supprimé du système. Nous pouvons, de la même manière, enlever tous les éléments $h_2(x), \ldots, h_m(x)$, et nous avons encore un système qui est équivalent au système modulaire (I).

En employant les méthodes qui ont été données ensuite, on peut démontrer ce même théorème pour les systèmes modulaires qui ont pour éléments des fonctions entières de plusieurs variables dont les coefficients sont des entiers algébriques de Ω.

Plus petit commun multiple de deux systèmes modulaires.

Si

$$\mathrm{L} = (\mathrm{L}_1, \mathrm{L}_2, \ldots, \mathrm{L}_\lambda),$$
$$\mathrm{M} = (\mathrm{M}_1, \mathrm{M}_2, \ldots, \mathrm{M}_\mu),$$
$$\mathrm{N} = (\mathrm{N}_1, \mathrm{N}_2, \ldots, \mathrm{N}_\nu)$$

sont trois systèmes modulaires dans lesquels les éléments sont des fonctions entières d'un nombre quelconque de variables et dont les coefficients sont des entiers algébriques de Ω et si, de plus,

$$\mathrm{L} > \mathrm{M} \quad \text{et} \quad \mathrm{L} > \mathrm{N},$$

L est un multiple de M et de N.

Toutes les quantités qui sont divisibles par L sont divisibles à la fois par M et par N. Il peut y avoir d'autres quantités qui sont divisibles à la fois par M et par N et qui ne le sont pas par L, et il peut se faire encore qu'il n'y ait aucune quantité divisible à la fois par M et N.

Dès lors, s'il existe un plus petit commun multiple L des deux systèmes M et N, il jouit des propriétés suivantes :

1° Il est divisible à la fois par M et par N;

2° Un autre multiple commun à M et N est divisible par L.

Avec Dedekind (note de la p. 495), nous écrirons

$$\mathrm{L} = \mathrm{M} - \mathrm{N} = \mathrm{N} - \mathrm{M}.$$

Il s'ensuit immédiatement que, si M, N et P sont trois systèmes modulaires qui ont un plus petit commun multiple,

$$(\mathrm{M} - \mathrm{N}) - \mathrm{P} = \mathrm{M} - (\mathrm{N} - \mathrm{P}) = (\mathrm{M} - \mathrm{P}) - \mathrm{N}.$$

Plus grand commun diviseur de deux ou plusieurs systèmes modulaires.

Soient

$$D = (D_1, D_2, \ldots, D_\delta),$$
$$M = (M_1, M_2, \ldots, M_\mu),$$
$$N = (N_1, N_2, \ldots, N_\nu),$$

trois systèmes modulaires et supposons que l'on ait

$$M > D \quad \text{et} \quad N > D.$$

D sera alors un diviseur commun à la fois à M et N.

Si D est le plus grand commun diviseur de ces deux systèmes, il a les deux caractéristiques suivantes :

1°

$$M > D \quad \text{et} \quad N > D;$$

2° Un autre diviseur commun K à M et à N est un diviseur de D.

En employant la notation de Dedekind, nous écrirons

$$D = M + N.$$

On voit immédiatement que

$$D = (M_1, M_2, \ldots, M_\mu, N_1, N_2, \ldots, N_\nu),$$

car 1°

$$(M_1, M_2, \ldots, M_\mu, N_1, N_2, \ldots, N_\nu)$$

est un diviseur des deux systèmes M et N;

Et 2° si K est un diviseur de M et N, de sorte que l'on ait

$$M > K \quad \text{et} \quad N > K,$$

on a

$$(M_1, M_2, \ldots, M_\mu, N_1, N_2, \ldots, N_\nu) > K.$$

Dans le domaine des nombres rationnels, deux entiers sont dits *premiers entre eux* lorsque leur plus grand commun diviseur est l'unité.

Dans le même domaine, deux systèmes modulaires M et N sont dits

premiers entre eux lorsque $M + N = 1$, c'est-à-dire lorsque

$$(M_1, M_2, \ldots, M_\mu, N_1, N_2, \ldots, N_\nu) = 1.$$

Lorsque cette condition est remplie on voit que l'unité est un élément qui peut être adjoint au système

$$(M_1, M_2, \ldots, M_\mu, N_1, N_2, \ldots, N_\nu).$$

Par exemple, les systèmes $(2, x^2)$, $(2, 1 + x)$ sont premiers entre eux. Car on a

$$(2, x^2, 1 + x) \backsim [2, x^2 - x(1 + x), 1 + x] \backsim (2, -x, 1 + x) \backsim (2, -x, 1) \backsim 1.$$

Dans le cas général, c'est-à-dire lorsque deux systèmes modulaires appartenant à un domaine quelconque d'intégrité sont premiers entre eux, *voir* pages 36 et 55.

Digression sur la théorie des équations.

Nous avons déjà considéré des domaines de rationalité d'un certain *degré*, des modules d'un certain rang; nous allons maintenant introduire la notion de l'*espèce* d'un système modulaire [*Stufe* (1), voir *Kronecker's Grundzüge*, p. 70; ou *Werke*, t. II, p. 326].

Dans la théorie des équations, nous pouvons avoir m équations contenant n quantités $x_1, x_2, \ldots, x_n$ où $m \leqq n$; par exemple, les m équations peuvent être mises sous la forme de

$$(1) \quad \begin{cases} c_{11}(x_1 - a_1) + c_{12}(x_2 - a_2) + \ldots + c_{1n}(x_n - a_n) + \gamma_1 = 0, \\ c_{21}(x_1 - a_1) + c_{22}(x_2 - a_2) + \ldots + c_{2n}(x_n - a_n) + \gamma_2 = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ c_{m1}(x_1 - a_1) + c_{m2}(x_2 - a_2) + \ldots + c_{mn}(x_n - a_n) + \gamma_m = 0, \end{cases}$$

où les c sont des constantes déterminées et $\gamma_1, \gamma_2, \ldots, \gamma_m$ des séries en

$$x_1 - a_1, \quad x_2 - a_2, \quad \ldots, \quad x_n - a_n,$$

(1) Dans le *Quarterly Journal*, vol. XXVII, p. 163, je traduis le mot *Stufe* par le mot anglais *Kind*.

dans lesquelles chaque terme est de dimension (1) plus grande que un. Les quantités $a_1, a_2, \ldots, a_n$ forment un système déterminé de valeurs des variables qui satisfait aux m équations.

Si maintenant un des déterminants, soit

$$\begin{vmatrix} c_{11}, & c_{12}, & \ldots, & c_{1m} \\ c_{21}, & c_{22}, & \ldots, & c_{2m} \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ c_{m1}, & c_{m2}, & \ldots, & c_{mm} \end{vmatrix},$$

est différent de zéro, nous pouvons écrire

$$\begin{aligned} x_1 - a_1 &= c'_{11}(x_{m+1} - a_{m+1}) + c'_{12}(x_{m+2} - a_{m+2}) + \ldots + c'_{1,n-m}(x_n - a_n) + \chi'_1, \\ x_2 - a_2 &= c'_{21}(x_{m+1} - a_{m+1}) + c'_{22}(x_{m+2} - a_{m+2}) + \ldots + c'_{2,n-m}(x_n - a_n) + \chi'_2, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_m - a_m &= c'_{m1}(x_{m+1} - a_{m+1}) + c'_{m2}(x_{m+2} - a_{m+2}) + \ldots + c'_{m,n-m}(x_n - a_n) + \chi'_m, \end{aligned}$$

où les c' sont des constantes déterminées.

A l'aide de ces équations, nous pouvons exprimer

$$x_1 - a_1, \quad x_2 - a_2, \quad \ldots, \quad x_m - a_m$$

à l'aide de $n - m$ différences restantes.

Le procédé régulier de développement de la série est le suivant : Nous posons

$$\chi'_1 = 0, \qquad \chi'_2 = 0, \qquad \ldots, \qquad \chi'_m = 0,$$

et nous avons pour $x_1 - a_1$, $x_2 - a_2$, ..., $x_m - a_m$ des expressions qui sont les premières valeurs approchées. Nous substituons ces premières valeurs approchées dans $\chi'_1, \chi'_2, \ldots, \chi'_m$ et négligeant les termes de dimension supérieure ou égale à la troisième, nous obtenons les secondes valeurs approchées. En continuant ainsi, nous pouvons obtenir les séries cherchées.

Weierstrass dit que les équations (I) contenant les n quantités x_1, x_2, ..., x_n, définissent une *structure* ou *configuration* (*analytisches*

(1) On appelle *dimension d'un terme* la somme des exposants des variables qui y entrent et *dimension d'une fonction* la dimension du terme qui a la plus grande dimension.

Gebilde) de $(n-m)^{\text{ième}}$ espèce (*Stufe*) dans le domaine des n quantités $x_1, x_2, \ldots, x_n$.

Nous pouvons dire que le système des équations (I) est un système d'équations de $m^{\text{ième}}$ espèce dans le domaine des quantités $x_1, x_2, \ldots, x_n$.

En particulier, si $m = n$, un système d'équations de $n^{\text{ième}}$ espèce définit une structure analytique d'espèce o dans le domaine des quantités $x_1, x_2, \ldots, x_n$.

Supposons maintenant que

$$\text{(II)} \qquad \begin{cases} f_1(x_1, x_2, \ldots, x_n) = 0, \\ f_2(x_1, x_2, \ldots, x_n) = 0, \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ f_m(x_1, x_2, \ldots, x_n) = 0, \end{cases}$$

soient m équations algébriques entières par rapport aux variables $x_1, x_2, \ldots, x_n$, les coefficients étant des entiers de Ω respectivement de dimensions $d_1, d_2, \ldots, d_m$.

Nous ferons d'abord, dans les équations (II), les substitutions

$$\begin{aligned} x_1 &= a_{11} z_1 + a_{12} z_2 + \ldots + a_{1n} z_n, \\ x_2 &= a_{21} z_1 + a_{22} z_2 + \ldots + a_{2n} z_n, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots, \\ x_n &= a_{n1} z_1 + a_{n2} z_2 + \ldots + a_{nn} z_n, \end{aligned}$$

où nous pouvons choisir les entiers algébriques a_{ij}, de telle sorte

1° Que l'on ait

$$\Delta = |a_{ij}| \neq 0;$$

2° Que, dans les équations obtenues,

$$\text{III)} \qquad \begin{cases} g_1(z_1, z_2, \ldots, z_n) = 0, \\ g_2(z_1, z_2, \ldots, z_n) = 0, \\ \cdots\cdots\cdots\cdots\cdots\cdots, \\ g_m(z_1, z_2, \ldots, z_n) = 0, \end{cases}$$

le degré en chacune des variables soit égal à la dimension de la fonction.

Nous évitons ainsi les difficultés que l'on rencontrerait autrement dans les résultants, telles que l'introduction de valeurs infinies

parmi les racines, c'est-à-dire les systèmes de quantités telles que $(\xi_1, \xi_2, \ldots, \xi_n)$ qui, substituées aux variables dans (III), rendent simultanément nulles ces équations; et de même, en donnant les valeurs $\xi_1, \xi_2, \ldots, \xi_{n-1}$ aux $n-1$ variables $x_1, x_2, \ldots, x_{n-1}$, il ne pourra y avoir ici un nombre infini de valeurs ξ_n pour x_n. De plus, un facteur de l'une quelconque des équations (III) contient toutes les variables.

Nous pouvons faire maintenant la transformation de Liouville

$$z = u_1 z_1 + u_2 z_2 + \ldots + u_n z_n,$$

où $u_1, u_2, \ldots, u_n$ sont des quantités entières indéterminées de Ω.

Multiplions chacune des équations (III) par $u_n^{d_i}$ $(i = 1, 2, \ldots, m)$ et dans ces équations écrivons à la place de $u_n z_n$ l'expression

$$z - u_1 z_1 - u_2 z_2 - \ldots - u_{n-1} z_{n-1}.$$

Les résultats de ces transformations seront désignés par les quantités

$$k_i(z_1, z_2, \ldots, z_{n-1}; u_1, u_2, \ldots, u_n) = 0 \quad (i = 1, 2, \ldots, m) \tag{IV}$$

qui sont des polynomes entiers de degré d_i $(i = 1, 2, \ldots, m)$ en chacune des lettres $z_1, z_2, \ldots, z_{n-1}, z$ et homogènes et de ce degré par rapport aux lettres $u_1, u_2, \ldots, u_n, z$.

Soit d'abord $m = n$, de sorte que dans (IV) il y ait autant d'équations que d'inconnues.

Soit $R(z)$ le résultat de l'élimination des variables $z_1, z_2, \ldots, z_{n-1}$ entre ces m équations.

Si $R(z)$ ne s'annule pas identiquement, les racines du système (IV) forment une variété (*Mannigfaltigkeit*) de dimension o, et le système d'équations est de $n^{\text{ième}}$ espèce.

Si $R(z)$ s'annule identiquement, c'est-à-dire s'il y a un nombre infini de systèmes de valeurs qui satisfont aux équations (IV), tous les coefficients de $R(z)$ sont nuls quelles que soient les valeurs des u. Dès lors, nous avons aussi $R(z_n) = 0$ et nous pouvons par conséquent donner à z_n une valeur arbitraire et déterminer un système de valeurs qui lui soit associé et qui satisfasse au système d'équations (IV).

Nous pouvons donc laisser z_n indéterminé et écrire

$$z^{(1)} = u_1 z_1 + u_2 z_2 + \ldots + u_{n-1} z_{n-1}.$$

A la place de $u_{n-1}z_{n-1}$ nous écrirons

$$z^{(1)} - u_1 z_1 - u_2 z_2 - \ldots - u_{n-2} z_{n-2}$$

dans chacune des équations (IV).

Entre $n-1$ de ces équations nous éliminerons $z_1, z_2, \ldots, z_{n-2}$, et nous pourrons en déduire les n résultants

$$R^{(1)}(z^{(1)}, z_n), \quad R^{(2)}(z^{(1)}, z_n), \quad \ldots, \quad R^{(n)}(z^{(1)}, z_n),$$

dans lesquels nous pouvons donner à z_n une valeur arbitraire.

Si l'un de ces résultants $R^{(i)}(z^{(1)}, z_n)$ ne s'annule pas identiquement, les racines du système (IV) forment une variété de dimension 1, et le système est dit *d'espèce* $n-1$.

A l'aide de la solution relative à $z^{(1)}$ de l'équation

$$R^{(i)}(z^{(1)}, z_n) = 0,$$

nous pouvons déterminer toutes les racines du système (IV).

Si $R^{(i)}(z^{(1)}, z_n)$ ne contient pas de facteur indépendant de z_n, les racines de (IV) sont toutes des fonctions de z_n, et le système d'équations (IV) s'appelle un *système pur* de $(m-1)^{\text{ième}}$ espèce.

Si, cependant, $R^{(i)}(z^{(1)}, z_n)$ contient des facteurs indépendants de z_n, les racines du système (IV) correspondant aux valeurs de $z^{(1)}$, qui sont obtenues en égalant ces facteurs à 0, forment une variété de dimension zéro. Dans ce cas, le système (IV) est dit *système mixte* d'espèce $m-1$, car il est mêlé à un système de $m^{\text{ième}}$ espèce.

Si les n résultants

$$R^{(1)}(z^{(1)}, z_n), \quad R^{(2)}(z^{(1)}, z_n), \quad \ldots, \quad R^{(n)}(z^{(1)}, z_n)$$

sont identiquement nuls, il est vrai aussi que

$$R^{(\nu)}(z_{n-1}, z_n) = 0 \qquad (\nu = 1, 2, \ldots, n).$$

Nous pouvons, par suite, laisser z_{n-1} et z_n indéterminés dans le système (IV), et nous ferons alors la substitution

$$z^{(2)} = u_1 z_1 + u_2 z_2 + \ldots + u_{n-2} z_{n-2},$$

c'est-à-dire qu'à la place de $u_{n-2}z_{n-2}$ nous écrirons

$$z^{(2)} - u_1 z_1 - u_2 z_2 - \ldots - u_{n-2} z_{n-2}$$

dans les équations (IV) et, à l'aide de $n-2$ de ces équations, nous éliminerons les variables $z_1, z_2, \ldots, z_{n-3}$.

Nous pourrons ainsi former les $k = \frac{n(n-1)}{2}$ résultants

$$R^{(1)}(z^{(2)}, z_{n-1}, z_n), \quad R^{(2)}(z^{(2)}, z_{n-1}, z_n), \quad \ldots, \quad R^{k}(z^{(2)}, z_{n-1}, z_n).$$

Si l'un de ces éléments n'est pas identiquement nul, les racines des équations (IV) forment une variété de dimension 2, et le système d'équations (IV) est un système de $(n-2)^{\text{ième}}$ espèce, qui peut être pur ou mêlé à des systèmes de $(n-1)^{\text{ième}}$ ou de $n^{\text{ième}}$ espèce selon que le résultant n'a pas de facteur indépendant des deux paramètres z_{n-1}, z_n, ou a un facteur qui contient un de ces paramètres, ou enfin a un facteur indépendant des deux paramètres.

Si tous les résultants ci-dessus s'annulent identiquement, nous pouvons continuer comme précédemment et déterminer les systèmes de troisième espèce et ainsi de suite (*Cf.* KRONECKER, *Grundzüge*, § 21, ou *Algèbre de Netto*, t. II, p. 95).

Systèmes modulaires de différentes espèces.

En vertu de la congruence

$$G(z^{(1)}, z_1, \ldots, z_{n-1}) \equiv 0 \qquad (\mathrm{mod}\, k_1, k_2, \ldots, k_n),$$

où $k_1, k_2, \ldots, k_n$ sont les fonctions qui se trouvent dans le membre de gauche du système d'équations (IV), nous voyons que $G(z^{(1)}, z_1, \ldots, z_{n-1})$ peut s'exprimer par une forme linéaire des éléments $k_1, k_2, \ldots, k_n$ dans laquelle les coefficients sont aussi des fonctions entières de $z^{(1)}, z_1, \ldots, z_{n-1}$ à coefficients constants appartenant à un domaine d'intégrité donné, de sorte que

$$G = k_1 Z_1 + k_2 Z_2 + \ldots + k_n Z_n,$$

où $Z_1, Z_2, \ldots, Z_n$ sont des fonctions entières des z à coefficients entiers.

En vertu de cette équation, la dimension de la variété du système d'équations

$$(IV') \qquad k_1 = 0, \quad k_2 = 0, \quad \ldots, \quad k_n = 0 \qquad (n = m)$$

est diminuée d'une unité et, d'après les notions données plus haut, nous pouvons dire que l'espèce est augmentée d'une unité.

Dès lors, si le système d'équations (IV) *est de* $n^{ième}$ *espèce, nous pouvons dire que le système modulaire, relativement aux fonctions linéaires formées avec ses éléments, est un système de* $(n+1)^{ième}$ *espèce.*

Donc, si le domaine d'intégrité est $[o_1, z_1, z_2, \ldots, z_n]$ nous pouvons y trouver des systèmes modulaires de première, deuxième, ..., $(n+1)^{ième}$ espèce, les systèmes de première espèce ne contenant que des entiers algébriques, ceux de seconde espèce des fonctions entières d'une variable, etc.

Revenons au système d'équations (IV).

Supposons que $R_1(z_1, z_2, \ldots, z_{n-1}, z; u_1, u_2, \ldots, u_n)$ soit le plus grand commun diviseur des fonctions $k_i (i = 1, 2, \ldots, m)$ et posons

$$k_i(z_1, z_2, \ldots, z_{n-1}, z; u_1, u_2, \ldots, u_n) = R_1(z_1, z_2, \ldots, z_{n-1}, z; u_1, u_2, \ldots, u_n) L_i(z_1, z_2, \ldots, z_{n-1}, z; u_1, u_2, \ldots, u_n) \quad (i = 1, 2, \ldots, m).$$

En négligeant la multiplicité des racines, on voit que ce système des solutions de

$$L_i(z_1, z_2, \ldots, z_{n-1}, z; u_1, u_2, \ldots, u_n) = 0 \quad (i = 1, 2, \ldots, m)$$

est le même que le système des solutions de

$$k_i(z_1, z_2, \ldots, z_{n-1}, z; u_1, u_2, \ldots, u_n) = 0 \quad (i = 1, 2, \ldots, m), \tag{IV}$$

si nous ajoutons aussi les solutions de

$$R_1(z_1, z_2, \ldots, z_{n-1}, z; u_1, u_2, \ldots, u_n) = 0.$$

A l'aide des coefficients indéterminés $U_1, U_2, \ldots, U_m$; $V_1, V_2, \ldots, V_n$ formons les deux fonctions

$$\sum_{i=1}^{i=m} U_i L_i \quad \text{et} \quad \sum_{i=1}^{i=m} V_i L_i$$

et formons le résultant de ces fonctions relativement à z_{n-1}. Ordonnons ce résultant suivant les puissances de U et V et représentons les coefficients par $S_1, S_2, S_3, \ldots$.

Le système des solutions des équations

$$S_1 = 0, \quad S_2 = 0, \quad S_3 = 0, \quad \ldots$$

est le même que le système des solutions des équations

$$L_1 = 0, \quad L_2 = 0, \quad \ldots, \quad L_m = 0.$$

Dès lors si

$$S_1 = R_2 H_1, \quad S_2 = R_2 H_2, \quad S_3 = R_2 H_3, \quad \ldots$$

et si nous négligeons la multiplicité des racines, le système des solutions des équations (IV) est le même que le système des solutions de

$$H_1 = 0, \quad H_2 = 0, \quad H_3 = 0, \quad \ldots,$$

si nous ajoutons les solutions de $R_1 . R_2 = 0$.

En continuant à opérer de même, nous formerons l'*équation résolvante*

$$R_1 . R_2 \ldots R_m = 0$$

du système d'équations (IV).

Lorsque nous posons $R_1 = 0$, on voit que z_n est par là même exprimé à l'aide d'une fonction algébrique de $z_1, z_2, \ldots, z_{n-1}$, de sorte que les racines de (IV) qui proviennent de $R_1 = 0$ forment une variété de dimension $n - 1$.

Les racines de (IV) qui proviennent de $R_2 = 0$ forment une variété de dimension $n - 2$, puisque dans ce cas z_n, z_{n-1} sont des fonctions algébriques des autres variables, et ainsi de suite.

En considérant R_1 comme un diviseur des éléments du système modulaire

$$[k_1, k_2, \ldots, k_m] = K,$$

puisque ce diviseur contient toutes les variables $z^{(1)}, z_1, z_2, \ldots, z_{n-1}$, c'est une structure analytique de $n^{\text{ième}}$ espèce.

Nous pouvons dire que R_1 est un diviseur de première espèce du système modulaire K, R_2 étant un diviseur de seconde espèce, etc.

Cf. Molk, *Sur une Notion qui comprend, etc.*, Chap. IV, § 2 (*Act. Math.*, vol. VI), et Borel et Drach, *Introduction à l'étude de la Théorie des nombres, etc.*, p. 218.

Multiplication ou composition de deux systèmes modulaires

$$M = (M_1, M_2, \ldots, M_\mu), \qquad N = (N_1, N_2, \ldots, N_\nu).$$

La composition de deux formes linéaires

$$M_1 X_1 + M_2 X_2 + \ldots + M_\mu X_\mu, \qquad N_1 Y_1 + N_2 Y_2 + \ldots + N_\nu Y_\nu,$$

où les X et les Y sont comme les M et les N des fonctions entières d'une ou de plusieurs variables à coefficients entiers appartenant au domaine Ω, se fait par multiplication directe et, comme la multiplication de deux systèmes modulaires M et N, produit un nouveau système modulaire T dont les éléments sont constitués par les $\mu\nu$ produits $M_h N_k (h = 1, 2, \ldots, m; k = 1, 2, \ldots, \nu)$.

Lorsque T peut s'exprimer par une forme linéaire de ces $\mu\nu$ produits, il est évident que la forme linéaire du produit de deux systèmes modulaires est le produit des formes linéaires des systèmes initiaux.

Les systèmes M et N peuvent être appelés les *facteurs du système* T.

Le système modulaire

$$(M.M', M_1, M_2, \ldots, M_\mu)$$

est le produit des deux systèmes

$$(M, M_1, M_2, \ldots, M_\mu) \quad \text{et} \quad (M', M_1, M_2, \ldots, M_\mu),$$

si $(M, M') \backsim 1$.

Par exemple

$$(21, M_1, M_2) \backsim (7, M_1, M_2)(3, M_2, M_2).$$

Nous dirons que le système

$$(M.M', M_1, M_2, \ldots, M_\mu)$$

est formé par la *composition* de deux systèmes

$$(M, M_1, M_2, \ldots, M_\mu) \quad \text{et} \quad (M', M_1, M_2, \ldots, M_\mu).$$

Un système qui n'est pas équivalent à un système qui peut être formé par la composition de deux autres systèmes est appelé *système irréductible* (*dans le sens de l'équivalence*).

Par exemple, le système (x^2+p, p^2), où p est un entier premier, est un système irréductible. Mais ce système contient le système (x, p), puisque chacun de ses éléments x^2+p, p^2 peut être exprimé par une fonction linéaire des éléments de (x, p), dont les coefficients appartiennent au domaine d'intégrité $[1, x]$.

Ces systèmes modulaires irréductibles, qui ne contiennent pas d'autres systèmes modulaires de la même espèce, sont appelés par Kronecker (*Werke*, t. III, p. 158), *systèmes modulaires premiers*.

Ces systèmes modulaires premiers ont, dans la théorie des systèmes modulaires, les propriétés caractéristiques qui appartiennent aux nombres premiers dans la théorie ordinaire des nombres. Par exemple, si le produit de deux systèmes modulaires est divisible par un système modulaire premier, l'un des facteurs est divisible par ce système modulaire.

Nous montrerons dans la suite que ces *systèmes modulaires* premiers ont aussi les mêmes propriétés caractéristiques dans les domaines d'intégrité dans lesquels ils entrent, que les entiers premiers rationnels dans le domaine d'intégrité rationnel.

SECONDE PARTIE.

RÉDUCTION DES SYSTÈMES MODULAIRES DANS LESQUELS LES COEFFICIENTS DES ÉLÉMENTS SONT DES ENTIERS ALGÉBRIQUES DU DOMAINE Ω.

Systèmes modulaires de première espèce.

Dans le domaine des nombres rationnels, le système

$$(6, 15) \backsim (6, 15-2.6) \backsim (6, 3) \backsim (3).$$

En général, le plus grand commun diviseur d des entiers a_1, a_2, ..., a_n peut être mis sous la forme

$$d = a_1 x_1 + a_2 x_2 + \ldots + a_n x_n,$$

où $x_1, x_2, \ldots, x_n$ sont des entiers déterminés. Dès lors nous pouvons ajouter l'élément d au système modulaire $[a_1, a_2, \ldots, a_n]$, qui devient alors $[d, a_1, a_2, \ldots, a_n]$; et puisque $a_1, a_2, \ldots, a_n$ sont tous des multiples de d, ces éléments peuvent être supprimés du système modulaire, et il reste

$$(a_1, a_2, \ldots a_n) \backsim (d).$$

Considérons maintenant le système modulaire

$$(\alpha_1, \alpha_2)$$

où α_1, α_2 sont des entiers algébriques du domaine Ω, c'est-à-dire des quantités appartenant au domaine d'intégrité $[\nu]$, puisque tous les entiers de Ω sont divisibles par ν.

Puisque l'on peut ajouter un élément quelconque au système modulaire pourvu que cet élément soit divisible par les éléments de ce système, on voit que

$$(\alpha_1, \alpha_2) \backsim (\alpha_1, \alpha_2, \xi_1\alpha_1, \xi_2\alpha_2),$$

où ξ_1 et ξ_2 sont des entiers quelconques de Ω.

De même

$$(\alpha_1, \alpha_2) \backsim (1\alpha_1, 1\alpha_2, \rho\alpha_1, \rho\alpha_2),$$

ρ étant l'*idéal principal* qui contient tous les entiers algébriques de Ω. De plus, puisque $1 > \rho$, il en résulte que

$$(\alpha_1, \alpha_2) \backsim (\rho\alpha_1, \rho\alpha_2).$$

Un idéal ρ peut être décomposé en facteurs premiers d'une seule manière. Soit

$$\rho\alpha = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\ldots,$$

où $\mathfrak{p}_1, \mathfrak{p}_2, \ldots$ sont des idéaux premiers.

Si deux idéaux $\rho\beta_1$ et $\rho\beta_2$ sont premiers entre eux, leur plus grand commun diviseur (*voir* p. 36) est ρ, de sorte que

$$\rho\beta_1 + \rho\beta_2 = \rho.$$

On voit immédiatement, d'après ce qui précède, que le système $(\rho\alpha_1, \rho\alpha_2)$ est équivalent au système $(\mathfrak{p}^k.\mathfrak{q}^l\ldots)$, où le produit des

idéaux $\mathfrak{p}^k$, $\mathfrak{q}^l$, ... est commun aux deux idéaux $\varphi\alpha_1, \varphi\alpha_2$; car si l'on a

$$\varphi\alpha_1 = \mathfrak{p}^k \mathfrak{q}^l \ldots \mathfrak{n}_1$$

et

$$\varphi\alpha_2 = \mathfrak{p}^k \mathfrak{q}^l \ldots \mathfrak{n}_2,$$

où $\mathfrak{n}_1$ et $\mathfrak{n}_2$ sont des idéaux premiers entre eux

$$(\varphi\alpha_1, \varphi\alpha_2) \backsim (\mathfrak{p}^k \mathfrak{q}^l \ldots \mathfrak{n}_1, \mathfrak{p}^k \mathfrak{q}^l \ldots \mathfrak{n}_2, \mathfrak{p}^k \mathfrak{q}^l \ldots \mathfrak{n}_1 + \mathfrak{p}^k \mathfrak{q}^l \ldots \mathfrak{n}_2)$$
$$\backsim (\mathfrak{p}^k \mathfrak{q}^l \ldots \mathfrak{n}_1, \mathfrak{p}^k \mathfrak{q}^l \ldots \mathfrak{n}_2, \mathfrak{p}^k \mathfrak{q}^l \ldots \varphi) \backsim (\mathfrak{p}^k \mathfrak{q}^l \ldots \varphi) \backsim (\mathfrak{p}^l \mathfrak{q}^l \ldots).$$

Il en résulte immédiatement que le système modulaire

$$(\alpha_1, \alpha_2, \ldots, \alpha_n),$$

où les éléments α_1, α_2, ..., α_n sont des quantités entières du domaine $[\varphi]$, est équivalent au système

$$(\mathfrak{p}_1^{h_1} \mathfrak{p}_2^{h_2} \ldots),$$

où h_1, h_2 sont des entiers rationnels et où les idéaux premiers $\mathfrak{p}_1$, $\mathfrak{p}_2$, ... entrent avec ces puissances dans chacun des éléments

$$\varphi\alpha_1, \quad \varphi\alpha_2 \quad \ldots, \quad \varphi\alpha_n.$$

En particulier, s'il n'y a pas d'idéal commun à tous les éléments $\varphi\alpha_1$, $\varphi\alpha_2$, ..., $\varphi\alpha_n$, on a

$$(\alpha_1, \alpha_2, \ldots, \alpha_n) \backsim (\varphi).$$

La propriété analogue dans le domaine des nombres rationnels est que

$$(\alpha_1, \alpha_2, \ldots, \alpha_n) \backsim (1),$$

s'il n'y a pas de diviseur commun à tous les entiers α_1, α_2, ... α_n autre que l'unité.

Systèmes modulaires de seconde espèce.

Les quantités entières qui apparaissent comme éléments dans ces systèmes sont de la forme

$$\alpha_0 x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n,$$

où α_0, α_1, ..., α_n sont des entiers algébriques du domaine Ω; nous

pouvons donc dire que ces quantités appartiennent au domaine d'intégrité $[\rho, x]$,

Considérons d'abord, dans le domaine d'intégrité $[1, x]$ le système modulaire

$$(ax^2 + cx + e,\ bx + d),$$

où a, c, e, b, d sont des entiers rationnels.

S'il y avait un facteur commun à $ax^2 + cx + e$ et $bx + d$, ce facteur pourrait être supprimé comme facteur du système modulaire. Nous pouvons donc supposer que les deux éléments $ax^2 + cx + e$ et $bx + d$ n'ont pas de facteur commun.

En vertu de la relation identique

$$(ax^2 + cx + e)\, b^2 = (abx + bc - ad)(bx + d) + b^2 e - bcd + ad^2,$$

on voit que l'entier positif ou négatif

$$m = b^2 e - bcd + ad^2 \equiv 0 \pmod{ax^2 + cx + e,\ bx + d}$$

peut être ajouté comme un élément au système

$$(ax^2 + cx + e,\ bx + d)$$

sans qu'il cesse d'être équivalent à lui-même.

Considérons maintenant le même système dans le domaine $[\rho, x]$, de sorte que maintenant a, c, e, b, d sont des entiers algébriques de Ω. Si, comme ci-dessus, nous supposons que les éléments $ax^2 + cx + e$, $bx + d$ n'ont pas de facteur commun dans ce domaine, l'entier algébrique

$$\mu = b^2 e - bcd + ad^2$$

est différent de zéro.

Puisque, d'autre part,

$$\mu = 0 \pmod{ax^2 + cx + e,\ bx + d},$$

on voit que μ peut être ajouté comme un élément au système modulaire donné, qui devient alors

$$(\mu,\ ax^2 + cx + e,\ bx + d).$$

De plus, puisque le système reste équivalent à lui-même lorsque nous multiplions chaque élément par ρ, on voit que nous pouvons con-

sidérer les coefficients des éléments soit comme étant les nombres entiers a, c, e, b, d, soit comme étant les entiers idéaux $\wp a$, $\wp c$, $\wp e$, $\wp b$, $\wp d$ puisque (*voir* DEDEKIND, t. III, p. 542) la divisibilité du nombre entier λ par l'entier algébrique μ est identique à la divisibilité de l'idéal $\wp\lambda$ par l'idéal $\wp\mu$.

Supposons que l'idéal $\mathfrak{q}$ soit un facteur commun des idéaux $\wp a$, $\wp b$, $\wp c$, de sorte que

$$\wp a x^2 + \wp c x + \wp c = \mathfrak{q}(\wp a' x^2 + \wp c' x + \wp e');$$

on peut montrer que, si $\mathfrak{q}$ n'est pas un diviseur de l'idéal $\wp\mu$ (diviseur qui soit un facteur de $\wp\mu$ dans le sens employé lorsqu'on a affaire au domaine des nombres rationnels), l'élément $\mathfrak{q}(\wp a' x^2 + \wp c' x + \wp c')$ peut être remplacé dans le système modulaire par l'élément $\delta(\wp a' x^2 + \wp c' x + \wp c')$, où δ est un idéal déterminé diviseur de $\wp\mu$ et que, par ce changement des éléments, le système reste équivalent à lui-même. Pour le prouver, soit δ un idéal qui soit le plus grand commun diviseur des idéaux $\mathfrak{q}$ et $\wp\mu$, de sorte que

$$\delta = \mathfrak{q} + \wp\mu.$$

Le système

$$[\wp\mu, \mathfrak{q}(\wp a' x^2 + \wp c' x + \wp e'), bx + d]$$

est, en raison de la présence de l'élément $\wp\mu$, équivalent à

$$\begin{aligned}&[\wp\mu, \mathfrak{q}(\wp a' x^2 + \wp c' x + \wp e'), \wp\mu(\wp a' x^2 + \wp c' x + \wp e'), bx + d]\\ &\quad \backsim (\wp\mu, \mathfrak{q})(\wp a' x^2 + \wp c' x + \wp e'), (\mathfrak{q} + \wp\mu)(\wp a' x^2 + \wp c' x + \wp e'), bx + d]\\ &\quad \backsim (\wp\mu, \mathfrak{q}(\wp a' x^2 + \wp c' x + \wp e'), \delta(\wp a' x^2 + \wp c' x + \wp e'), bx + d],\end{aligned}$$

et ce système, puisque $\mathfrak{q}$ est multiple de δ, est équivalent à

$$[\wp\mu, \delta(a' x^2 + c' x + e'), bx + d].$$

Dans le système modulaire

$$(\wp\mu, ax^2 + cx + c, bx + d)$$

supposons que $\wp\mu = \mathfrak{p}_1 . \mathfrak{p}_2$, où $\mathfrak{p}_1$ et $\mathfrak{p}_2$ soient des idéaux premiers entre eux; et, pour abréger, posons

$$\begin{aligned}f_1(x) &= ax^2 + bx + e,\\ f_2(x) &= bx + d.\end{aligned}$$

Nous dirons que le système

$$[\varphi\mu, f_1(x), f_2(x)]$$

est équivalent au produit des deux systèmes

$$[\mathfrak{p}_1, f_1(x), f_2(x)] \quad \text{et} \quad [\mathfrak{p}_2, f_1(x), f_2(x)],$$

car le produit de ces deux systèmes est

$$[\mathfrak{p}_1\mathfrak{p}_2, \mathfrak{p}_1 f_1(x), \mathfrak{p}_2 f_1(x), \mathfrak{p}_1 f_2(x), \mathfrak{p}_2 f_2(x), f_1(x)^2, f_2(x)^2, f_1(x)\cdot f_2(x)].$$

En raison de la présence des deux éléments $\mathfrak{p}_1 f_1(x)$ et $\mathfrak{p}_2 f_1(x)$, nous pouvons ajouter $(\mathfrak{p}_1+\mathfrak{p}_2) f_1(x)$ ou $\varphi f_1(x)$ au système. Comme $\varphi f_1(x) = f_1(x)$, nous pouvons ajouter $f_1(x)$ et, de même, $f_2(x)$, au système, qui se réduit alors immédiatement à

$$[\mathfrak{p}_1\mathfrak{p}_2, f_1(x), f_2(x)].$$

Nous pouvons donc considérer au lieu du système modulaire

$$[\varphi\mu, f_1(x, f_2(x)]$$

des systèmes de la forme

$$[\mathfrak{p}, f_1(x), f_2(x)],$$

où $\mathfrak{p}$ est un idéal premier ou une puissance d'un idéal premier.

Ce qui vient d'être démontré pour les valeurs spéciales données à $f_1(x)$ et $f_2(x)$ peut encore l'être dans le cas plus général où l'on prend pour $f_1(x)$ et $f_2(x)$ des fonctions entières quelconques de x à coefficients entiers appartenant au domaine Ω.

Si nous supposons qu'il n'y a pas de facteur commun à ces deux fonctions (puisqu'un tel facteur peut être immédiatement supprimé comme facteur du système modulaire), nous pouvons, par la méthode ordinaire du plus grand commun diviseur, déterminer un entier algébrique μ appartenant au domaine Ω qui puisse être ajouté au système en le laissant équivalent à lui-même.

En général, si nous supposons que, dans le système modulaire

$$[f_1(x), f_2(x), \ldots, f_n(x)]$$

les éléments sont des fonctions entières en x dont les coefficients appar-

tiennent au domaine $[\rho]$ *et, de plus, qu'il n'y a pas de diviseur commun à tous les éléments, la méthode ordinaire du plus grand commun diviseur nous permet de déterminer un entier algébrique appartenant aussi à* $[\rho]$, *qui peut se mettre sous la forme d'une fonction linéaire des éléments du système modulaire et qui peut, par conséquent, être ajouté comme élément au système modulaire en le laissant équivalent à lui-même.*

Le système devient alors

$$[\mu, f_1(x), f_2(x), \ldots, f_n(x)].$$

De même, comme dans le cas particulier considéré plus haut, si

$$\rho\mu = \mathfrak{p}_1^{e_1} \cdot \mathfrak{p}_2^{e_2} \cdot \ldots,$$

où $\mathfrak{p}_1$, $\mathfrak{p}_2$, ... sont des idéaux premiers et e_1, e_2, ... des entiers rationnels, nous pouvons considérer, au lieu du système donné au début, les systèmes

$$[\mathfrak{p}_1^{e_1}, f_1(x), f_2(x), \ldots, f_n(x)], \quad [\mathfrak{p}_2^{e_2}, f_1(x), f_2(x), \ldots, f_n(x)], \ldots,$$

dont le produit est équivalent au système initial.

Considérons le système

$$[\mathfrak{p}_1^{e_1}, f_1(x), f_2(x), \ldots, f_n(x)].$$

Si les coefficients de l'un quelconque des éléments, par exemple $f_1(x)$, ont un facteur commun, puisque l'élément peut être remplacé par un autre dans lequel le facteur est un diviseur de $\mathfrak{p}_1^{e_1}$, on voit que le système modulaire doit être de la forme

$$[\mathfrak{p}_1^{e_1}, \mathfrak{p}_1^{d_1} g_1(x), \mathfrak{p}_1^{d_2} g_2(x), \ldots, \mathfrak{p}_n^{d_n} g_n(x)],$$

où les nombres d_1, d_2, ..., d_n sont ou zéro ou des diviseurs de e_1, sans en excepter l'unité. Nous pouvons, de plus, supposer que les coefficients d'aucun des éléments $g_i(x)\,(i = 1, 2, \ldots, n)$ n'ont de facteur commun.

Dedekind (p. 636) démontre le théorème suivant : *Si* $\mathfrak{p}$ *est un entier rationnel premier et si l'on a*

$$\rho\mathfrak{p} = \mathfrak{p}_1^{k_1} \cdot \mathfrak{p}_2^{k_2} \cdot \ldots \cdot \mathfrak{p}_r^{k_r},$$

où $\mathfrak{p}_1$, $\mathfrak{p}_2$, ..., $\mathfrak{p}_r$ *sont des idéaux premiers; si, de plus, un des entiers* k_1,

$k_2, \ldots, k_r$ *est plus grand que l'unité, le discriminant* D *de* Ω (DEDEKIND, p. 538) *est toujours divisible par* p.

Le théorème suivant est également vrai : *Si* vp *contient un idéal premier* $\mathfrak{p}$ *à la* $k^{ième}$ *puissance,* D *contient le facteur premier* p *à la* $(k-1)^{ième}$ *puissance, excepté dans le cas où* k *est divisible par* p; *dans ce cas,* D *contient* p *au moins à la* $k^{ième}$ *puissance.*

Soit m le plus petit entier divisible par $v\mu$ et supposons *d'abord* que D ne soit divisible par aucun des facteurs de m, de sorte qu'aucun des exposants $e_1, e_2, \ldots$ de l'élément constant

$$v\mu = \mathfrak{p}_1^{e_1} \cdot \mathfrak{p}_2^{e_2} \cdot \ldots,$$

qui entre dans le système modulaire ci-dessus, ne puisse être plus grand que l'unité.

Ce système peut alors prendre la forme

$$[\mathfrak{p}, g_1(x), g_2(x), \ldots, g_n(x)].$$

Considérons maintenant la forme plus simple

$$[\mathfrak{p}, g_1(x), g_2(x)],$$

où

$$g_1(x) = \alpha_0 x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n,$$
$$g_2(x) = \beta_0 x^m + \beta_1 x^{m-1} + \ldots + \beta_m,$$
$$n \geqq m.$$

Nous pouvons supposer qu'aucun des coefficients

$$\alpha_0, \quad \alpha_1, \quad \ldots, \quad \alpha_n; \quad \beta_0, \quad \beta_1, \quad \ldots, \quad \beta_m$$

n'est divisible par $\mathfrak{p}$, puisque, dans ce cas, les termes contenant un tel coefficient peuvent être supprimés de la fonction, et le système modulaire reste équivalent à lui-même.

Dans le domaine des nombres rationnels, les entiers

$$0, \quad 1, \quad 2, \quad \ldots, \quad p-1$$

forment un système de résidus incongrus (mod$p$) et, par conséquent, tous les entiers du domaine peuvent être distribués en classes où

chaque entier appartenant à une classe donnée est congru (mod$p$) à un, et à un seulement, des entiers

$$0, \quad 1, \quad 2, \quad \ldots, \quad p-1.$$

De même, les entiers de Ω peuvent être distribués en $(\varphi, \mathfrak{p})$ classes (DEDEKIND, p. 509). Désignons ce nombre de classes par k, de sorte que $k = (\varphi, \mathfrak{p})$. Un entier quelconque d'une classe peut être choisi comme *représentatif* de cette classe. Dès lors, si nous choisissons un entier de chacune des $k = (\varphi, \mathfrak{p})$ classes, nous avons un système d'entiers qui peut être appelé le *système représentatif* des entiers du domaine Ω relativement au module $\mathfrak{p}$. Chaque entier de Ω est congru (mod$\mathfrak{p}$) à un des entiers relatifs à ces k classes.

Le *système représentatif* est donc caractérisé par les trois propriétés suivantes :

1° Les nombres représentatifs du système sont tous divisibles par φ;

2° La différence de deux représentatifs est divisible par $\mathfrak{p}$;

3° Tout entier algébrique de Ω est congru (mod$\mathfrak{p}$) à un des représentatifs.

L'entier 1, étant un des entiers de Ω, appartient à une des k classes et nous le prendrons comme représentatif de la classe à laquelle il appartient, et comme représentatif des $k-1$ autres classes, nous prendrons les entiers dont les normes sont inférieurs au norme de $\mathfrak{p}$.

Ces représentatifs seront désignés par

$$\rho_1 = 1, \quad \rho_2, \quad \ldots, \quad \rho_k.$$

Puisque le norme d'un idéal $\mathfrak{m}$ (DEDEKIND, p. 564) est égal à $(\varphi, \mathfrak{m})$, on voit que

$$N(\mathfrak{p}) = (\varphi, \mathfrak{p}) = k.$$

Par conséquent, les entiers rationnels $N(\rho_1)$, $N(\rho_2)$, $N(\rho_k)$ sont tous moindres que k.

Si maintenant une fonction $f(x)$ entière en x dont les coefficients sont des entiers de Ω, est multipliée successivement par tous les entiers de Ω, les différentes fonctions qui en résultent peuvent à leur tour être classées, relativement au modulus $\mathfrak{p}$, en $k = (\varphi, \mathfrak{p})$ différents

groupes et les k représentatifs qui en résultent sont obtenus en multipliant la fonction $f(x)$ par les k entiers algébriques qui constituent les représentatifs des k classes.

De plus, chacune des fonctions représentatives peut être employée à la place de la fonction $f(x)$, comme il est évident qu'une telle fonction, multipliée à son tour par chacun des k entiers algébriques qui constituent ce système représentatif donnera le système de fonctions représentatives que nous avons déjà trouvé plus haut.

Si donc

$$g_1(x) = \alpha_0 x^n + \alpha^{n-1} + \ldots + \alpha_n,$$

il est certain que l'un des systèmes représentatifs des entiers algébriques, soit, par exemple, ρ_i, est tel que

$$\rho_i \alpha_0 \equiv 1 \pmod{\mathfrak{p}}.$$

Dès lors, nous pouvons remplacer la fonction $g_1(x)$ dans le système modulaire

$$[\mathfrak{p}, g_1(x), g_2(x)]$$

par l'élément

$$G_1(x) = \rho_i g_1(x) \equiv x^n + \overline{\alpha_1} x^{n-1} + \overline{\alpha_2} x^{n-2} + \ldots + \overline{\alpha_n} \pmod{\mathfrak{p}},$$

où $\overline{\alpha_1}$, $\overline{\alpha_2}$, ..., $\overline{\alpha_n}$ sont des entiers algébriques que l'on trouve parmi les entiers ρ_1, ρ_2, ..., ρ_k.

Nous appellerons $G_1(x)$ l'*élément réduit* de $g_1(x)$.

Soit $G_2(x)$ l'élément réduit de $g_2(x)$. On voit que

$$[\mathfrak{p}, g_1(x), g_2(x)] \backsim [\mathfrak{p}, G_1(x), G_2(x)].$$

Puisque le degré de $G_2(x)$ en x est égal ou inférieur au degré de $G_1(x)$, nous avons par division

$$\frac{G_1(x)}{G_2(x)} = Q_1(x) + \frac{R_1(x)}{G_2(x)},$$

où les coefficients de $Q_1(x)$ et de $R_1(x)$ sont des entiers algébriques de Ω et où le degré de $R_1(x)$ en x est moindre que le degré de $G_1(x)$ et de $G_2(x)$.

De la relation qui précède il résulte que

$$G_1(x) = Q_1(x) G_2(x) + R_1(x),$$

et, par conséquent, puisque

$$R_1(x) \equiv o\,[\mathrm{mod}\,G_1(x), G_2(x)],$$

et

$$G_1(x) \equiv o\,[\mathrm{mod}\,G_2(x), R_1(x)],$$

nous voyons que nous pouvons adjoindre l'élément $R_1(x)$ au système

$$[\mathfrak{p}, G_1(x), G_2(x)]$$

et en retrancher $G_1(x)$ sans qu'il cesse d'être équivalent à lui-même, c'est-à-dire de telle façon que l'on ait

$$[\mathfrak{p}, G_1(x), G_2(x)] \backsim [\mathfrak{p}, G_2(x), R_1(x)].$$

Soit $H_3(x)$ l'élément réduit de $R_1(x)$, et comme plus haut écrivons la relation

$$G_2(x) = Q_2(x)H_3(x) + R_2(x).$$

Adjoignons $R_2(x)$ au système, et supprimons-en $G_2(x)$. Le système que nous avons à considérer est

$$[\mathfrak{p}, R_1(x), R_2(x)] :$$

Comme les degrés des nouveaux éléments qui sont adjoints au système vont continuellement en décroissant et ne peuvent pas devenir négatifs, on voit que si nous continuons à procéder de la même façon nous devrons finalement avoir

$$[\mathfrak{p}, H_{\nu-1}(x), H_\nu(x)]$$

et ici, ou bien $H_{\nu-1}(x)$ est divisible par $H_\nu(x)$ $(\mathrm{mod}\mathfrak{p})$ ou bien $H_\nu(x)$ est un entier algébrique premier avec $\mathfrak{p}$. Dans le premier cas le système modulaire $[\mathfrak{p}, H_{\nu-1}(x), H_\nu(x)]$ est équivalent à $[\mathfrak{p}, H_\nu(x)]$; dans le second cas il est équivalent à $[\rho]$, et cela n'est plus d'aucun intérêt.

Exactement de la même manière le système modulaire le plus général écrit plus haut

$$[\mathfrak{p}, g_1(x), g_2(x), g_3(x), \ldots, g_n(x)]$$

se réduit ou au système de la forme

$$[\mathfrak{p}, F(x)],$$

ou à

$$[\rho].$$

Ce dernier cas étant sans intérêt, nous étudierons maintenant de plus près le système

$$[\mathfrak{p}, F(x)],$$

où l'élément $F(x)$ peut être mis sous la forme

$$F(x) = x^\tau + \gamma_1 x^{\tau-1} + \gamma_2 x^{\tau-2} + \ldots + \gamma_\tau,$$

où $\gamma_1, \gamma_2, \ldots, \gamma_\tau$ sont prises parmi les quantités $\rho_1, \rho_2, \ldots, \rho_k$.

Supposons que par quelque autre méthode le système modulaire initial $[\mathfrak{p}, g_1(x), g_2(x), \ldots, g_n(x)]$ ait été réduit à la forme

$$[\mathfrak{p}, F_1(x)],$$

où l'élément $F_1(x)$ est un élément réduit $(\mathrm{mod}\,\mathfrak{p})$, c'est-à-dire un élément dans lequel le coefficient de la plus haute puissance de x est l'unité, tandis que les autres coefficients sont pris parmi les nombres $\rho_1, \rho_2, \ldots, \rho_k$. Nous allons voir maintenant que $F_1(x)$ est identique à $F(x)$.

En vertu de l'équivalence

$$[\mathfrak{p}_1, F(x)] \backsim [\mathfrak{p}_1, F_1(x)],$$

nous avons d'une part

$$F(x) = \mathfrak{p}\Pi_1(x) + F_1(x)\,\overline{F_1(x)}, \tag{1}$$

et d'autre part

$$F_1(x) = \mathfrak{p}\Pi(x) + F(x)\,\overline{F(x)}, \tag{2}$$

où les quantités $\Pi_1(x)$, $\Pi(x)$, $\overline{F_1(x)}$, $\overline{F(x)}$ sont des fonctions entières en x dont les coefficients sont des entiers algébriques de Ω, ou, comme nous dirons pour abréger, des quantités appartenant au domaine $[\rho, x]$.

Les relations (1) et (2) peuvent s'écrire :

$$F(x) = F_1(x)\,\overline{F_1(x)} \pmod{\mathfrak{p}}, \tag{1'}$$

$$F_1(x) = F(x)\,\overline{F(x)} \pmod{\mathfrak{p}}. \tag{2'}$$

Multiplions ces congruences membre à membre, nous avons

$$F(x)\,F_1(x) = F(x)\,F_1(x)\,\overline{F_1(x)}\,\overline{F(x)} \pmod{\mathfrak{p}}.$$

Puisque ni $F(x)$ ni $F_1(x)$ ne sont divisibles par $\mathfrak{p}$, il s'ensuit que

$$1 \equiv \overline{F_1(x)}\,\overline{F(x)} \pmod{\mathfrak{p}},$$

et comme $\overline{F_1(x)}$ et $\overline{F(x)}$ sont des quantités de $[\rho, x]$, cette congruence peut seulement avoir lieu si $\overline{F_1(x)}$ et $\overline{F(x)}$ sont des unités de Ω.

Dès lors de (1′) nous tirons

$$F(x) \equiv F_1(x) \pmod{\mathfrak{p}},$$

et puisque $F(x)$ et $F_1(x)$ sont tous deux réduits $(\mathrm{mod}\,\mathfrak{p})$, il s'ensuit que $F(x)$ doit être égal à $F_1(x)$.

Le système $[\mathfrak{p}, F(x)]$ est ce que j'ai appelé une *forme canonique* (*voir* le *Journal de Crelle*, t. 119, p. 148) du système modulaire

$$[\mathfrak{p}, g_1(x), g_2(x), \ldots, g_n(x)].$$

C'est ainsi que, quelle que soit la réduction du système

$$[\mathfrak{p}, g_1(x), g_2(x), \ldots, g_n(x)]$$

que l'on ait opérée, la forme finale, qui est équivalente à la forme canonique, lui est identique.

Dans le système $[\mathfrak{p}, F(x)]$ la fonction $F(x)$ est de la forme

$$F(x) = x^\tau + \gamma_1 x^{\tau-1} + \gamma_2 x^{\tau-2} + \ldots + \gamma_\tau,$$

où les γ peuvent prendre des valeurs $\rho_1, \rho_2, \ldots, \rho_k$.

Dès lors les résidus (quantités incongrues) du système modulaire ci-dessus ont la forme

$$R(x) = \beta_0 + \beta_1 x + \beta_2 x^2 + \ldots + \beta_{\tau-1} x^{\tau-1},$$

où les β peuvent prendre des valeurs $\rho_1, \ldots, \rho_k$.

Le nombre des fonctions de cette forme est donc par conséquent k^τ, et puisque l'une de ces fonctions est divisible par le système modulaire, le nombre total des résidus du système modulaire est $\mu = k^\tau - 1$.

On peut voir comme il suit que ces μ résidus $R_1, R_2, \ldots, R_\mu$ sont incongrus $[\mathrm{mod}\,\mathfrak{p}, F(x)]$: supposons que $R_i(x)$ et $R_h(x)$ sont deux des résidus dont nous venons de parler et supposons qu'ils soient congrus $[\mathrm{mod}\,\mathfrak{p}, F(x)]$.

La différence de ces résidus peut s'écrire

$$R_i(x) - R_h(x) = \beta_0^{(i)} - \beta_0^{(h)} + (\beta_1^{(i)} - \beta_1^{(h)})\, x + (\beta_2^{(i)} - \beta_2^{(h)})\, x^2 + \ldots + (\beta_{n-1}^{(i)} - \beta_{n-1}^{(h)})\, x^{n-1},$$

où les $\beta^{(i)}$ et les $\beta^{(h)}$ sont pris parmi les entiers $\rho_1, \ldots, \rho_k$.

Puisque $R_i(x) - R_h(x)$ est divisible par le système modulaire $[\mathfrak{p}, F(x)]$, il s'ensuit que

$$(a) \qquad R_i(x) - R_h(x) = H\mathfrak{p} + F'(x)\, F(x),$$

où H et $F'(x)$ sont des quantités de $[o, x]$. De plus, puisque $F(x)$ est de degré τ en x et est de la forme

$$F(x) = x^\tau + \gamma_1 x^{\tau-1} + \ldots + \gamma_\tau,$$

et puisque le degré de $R_i(x) - R_h(x)$ est au plus $\tau - 1$, il en résulte que $F'(x)$ doit être divisible par $\mathfrak{p}$ afin que la relation (a) soit vraie, et par conséquent nous devons avoir

$$R_i(x) - R_h(x) = H\mathfrak{p},$$

où H est une quantité entière de Ω.

Mais puisque les différences $\beta_0^{(i)} - \beta_0^{(h)}$, $\beta_1^{(i)} - \beta_1^{(h)}$, ..., $\beta_{n-1}^{(i)} - \beta_{n-1}^{(h)}$ ne sont divisibles par $\mathfrak{p}$ que si $\beta_0^{(i)} = \beta_0^{(h)}$, $\beta_1^{(i)} = \beta_1^{(h)}$, ..., $\beta_{n-1}^{(i)} = \beta_{n-1}^{(h)}$, la relation (a) ne peut avoir lieu que si $R_i(x) = R_h(x)$.

On voit aussi que les produits

$$R_i R_1,\ R_i R_2,\ R_i R_3, \ldots, R_i R_\mu \qquad (i = 1, 2, \ldots, \mu),$$

sont incongrus $[\mathrm{mod}\, \mathfrak{p}\, F(x)]$.

Nous aurons par conséquent

$$(1) \qquad \prod_{k=1}^{k=\mu} (x - R_i R_k) \equiv \prod_{k=1}^{k=\mu} (x - R_k) \ [\mathrm{mod}\, \mathfrak{p}, F(x)] \qquad (i = 1, 2, \ldots, \mu),$$

et aussi

$$(2) \qquad \prod_{k=1}^{k=\mu} (R_i R_k) \equiv \prod_{k=1}^{k=\mu} R_k \ [\mathrm{mod}\, \mathfrak{p}, F(x)],$$

u

$$R_i^{\nu} \prod_{k=1}^{k=\mu} R_k \equiv \prod_{k=1}^{k=\mu} R_k \ [\mathrm{mod}\,\mathfrak{p}, F(x)] \qquad (i = 1, 2, \ldots, \mu).$$

Puisque, de plus, $\prod_{k=1}^{k=\mu} R_k$ n'est pas divisible par le système modulaire $\mathfrak{p}, F(x)]$ il s'ensuit que

$$R_i^{\nu} \equiv 1 \ [\mathrm{mod}\,\mathfrak{p}, F(x)] \qquad (i = 1, 2, \ldots, \mu),$$

ce qui est une *forme générale du théorème de Fermat.*

En remplaçant μ par sa valeur $k^{\tau} - 1$, on voit que

$$R_i^{k^{\tau}} \equiv R_i [\mathrm{mod}\,\mathfrak{p}, F(x)] \qquad (i = 1, 2, \ldots, \mu),$$

et par conséquent aussi

$$x^{k^{\tau}} - x \equiv F(x)\,\varphi(x) \ (\mathrm{mod}\,\mathfrak{p}),$$

où $\varphi(x)$ est une quantité de $[\mathfrak{p}, x]$; *dès lors* $(\mathrm{mod}\,\mathfrak{p})$ *la fonction* $x^{k^{\tau}} - x$ *est divisible par la fonction* $F(x)$ (*voir* SERRET, *Cours d'Algèbre supérieure*, t. II, Chap. III, p. 131; 1866).

Avec Serret nous dirons que la fonction $F(x)$ est *décomposable* en ces facteurs $\varphi(x)$, $\psi(x)$ $(\mathrm{mod}\,\mathfrak{p})$, qui appartiennent à $[\mathfrak{p}, x]$ s'il est possible de déterminer une fonction $\chi(x)$ appartenant aussi à $[\mathfrak{p}, x]$ et telle que

$$\varphi(x)\chi(x) = F(x) + \mathfrak{p}\chi(x);$$

dans le cas contraire, la fonction $F(x)$ peut être appelée *irréductible* $(\mathrm{mod}\,\mathfrak{p})$. Les résultats trouvés ci-dessus sont vrais, que $F(x)$ soit ou ne soit pas irréductible $(\mathrm{mod}\,\mathfrak{p})$.

Prenons pour exemple, dans le domaine des nombres rationnels, le système modulaire

$$[5, (x-1)(x-2)];$$

on a l'équivalence

$$(5, x^2 - 3x + 2) \backsim (5, x^2 + 2x + 2).$$

Multiplions chacun des résidus $(\mathrm{mod}\,5)$ de $x^2 + 2x + 2$ par le ré-

sidu $x+1$, par exemple; nous avons

0 multiplié par $x+1 \equiv$	0,	$2x+3$ multiplié par $x+1 \equiv$	$4x+1$,
1 » » $\equiv$	$x+1$,	$2x+4$ » » $\equiv$	$3x$,
2 » » $\equiv$	$2x+2$,	$3x$ » » $\equiv$	$3x+1$,
3 » » $\equiv$	$3x+3$,	$3x+1$ » » $\equiv$	$2x$,
4 » » $\equiv$	$4x+4$,	$2x+2$ » » $\equiv$	$x+4$,
x » » $\equiv$	$x+2$,	$3x+3$ » » $\equiv$	3,
$x+1$ » » $\equiv$	1,	$3x+4$ » » $\equiv$	$4x+2$,
$x+2$ » » $\equiv$	$4x$,	$4x$ » » $\equiv$	$4x+3$,
$x+3$ » » $\equiv$	$3x+4$,	$4x+1$ » » $\equiv$	$3x+2$,
$x+4$ » » $\equiv$	$2x+3$,	$4x+2$ » » $\equiv$	$2x+1$,
$2x$ » » $\equiv$	$2x+4$,	$4x+3$ » » $\equiv$	x ,
$2x+1$ » » $\equiv$	$x+3$,	$4x+4$ » » $\equiv$	4,
$2x+2$ » » $\equiv$	2,		

$$[\text{mod } 5,\ x^2+2x+2],$$

De là il résulte que

$$(x+1)^{24} \equiv 1\ [\text{mod } 5,\ x^2+2x+2].$$

Revenons au système

$$[\mathfrak{p},\ F(x)],$$

et supposons que

$$F(x) = \varphi(x)\psi(x) + \mathfrak{p}\chi(x),$$

de sorte

$$[\mathfrak{p},\ F(x)] \backsim [\mathfrak{p},\ \varphi(x).\psi(x)].$$

Supposons de plus que $\varphi(x)$ et $\psi(x)$ n'aient pas de facteur commun (mod $\mathfrak{p}$).

Nous pouvons écrire alors

$$[\mathfrak{p},\ F(x)] \backsim [\mathfrak{p},\ \varphi(x)]\,[\mathfrak{p},\ \psi(x)],$$

car le produit que nous venons d'écrire est équivalent à

$$[\mathfrak{p}^2,\ \mathfrak{p}\psi(x),\ \mathfrak{p}\varphi(x),\ \varphi(x).\psi(x)].$$

Mais puisque $\varphi(x)$ et $\psi(x)$ sont premiers entre eux, leur plus grand commun diviseur est ν et peut s'écrire

$$\nu = \psi(x) + \varphi(x).$$

Dès lors nous avons les équivalences

$$[\mathfrak{p}^2, \mathfrak{p}\psi(x), \mathfrak{p}\varphi(x), \varphi(x)\psi(x)] \backsim [\mathfrak{p}^2, \mathfrak{p}\psi(x), \mathfrak{p}\varphi(x), \mathfrak{p}\psi(x) + \mathfrak{p}\varphi(x), \varphi(x)\psi(x)]$$
$$\backsim [\mathfrak{p}^2, \mathfrak{p}\psi(x), \mathfrak{p}\varphi(x), \mathfrak{p}, \varphi(x)\psi(x)] \backsim [\mathfrak{p}, \varphi(x)\psi(x)].$$

Nous pouvons donc considérer maintenant un système de la forme

$$[\mathfrak{p}, \varphi(x)],$$

où $\varphi(x)$ est une fonction irréductible (mod $\mathfrak{p}$).

Ce système correspond à ce que nous avons appelé un *système modulaire premier* (p. 55).

Supposons que $\varphi(x)$ ait la forme

$$\varphi(x) = x^\lambda + \gamma_1 x^{\lambda-1} + \gamma_2 x^{\lambda-2} + \ldots + \gamma_\lambda,$$

où $\gamma_1, \gamma_2, \ldots, \gamma_\lambda$ sont pris parmi les quantités $\rho_1, \rho_2, \ldots, \rho_k$.

Il y a, par conséquent, $m = k^\lambda - 1$ résidus du système $[\mathfrak{p}, \varphi(x)]$, que nous désignerons par $r_1, r_2, \ldots, r_m$.

Nous aurons donc, comme plus haut,

$$r_i^{k^\lambda - 1} \equiv 1 \,[\mathrm{mod}\ \mathfrak{p}, \varphi(x)] \qquad (i = 1, 2, \ldots, m).$$

Lemme. — *Si r désigne un quelconque des résidus dont nous venons de parler et si*

$$G(r) = A_0 r^m + A_1 r^{m-1} + \ldots + A_m \equiv 0 \qquad [\mathrm{mod}\ \mathfrak{p}, \varphi(x)],$$

où $A_0, A_1, \ldots, A_m$ sont des fonctions entières en x dont les coefficients appartiennent au domaine $[\rho]$ et $A_0 \not\equiv 0$ [mod $\mathfrak{p}$, $\varphi(x)$], la congruence précédente ne peut avoir plus de m racines.

Nous démontrerons d'abord ce lemme pour le cas particulier de $m = 1$. Considérons la congruence

$$A_0 r + A_1 \equiv 0 \qquad [\mathrm{mod}\ \mathfrak{p}, \varphi(x)],$$

où $A_0 \not\equiv 0$ [mod $\mathfrak{p}$, $\varphi(x)$], et supposons que r_1 et r_2 soient deux racines de cette congruence, de sorte que l'on ait, par suite,

$$A_0 r_1 + A_1 \equiv 0 \qquad [\mathrm{mod}\ \mathfrak{p}, \varphi(x)],$$

et

$$A_0 r_2 + A_1 \equiv 0 \qquad [\mathrm{mod}\ \mathfrak{p}, \varphi(x)].$$

Par soustraction nous avons

$$A_0(r_1 - r_2) \equiv 0 \qquad [\text{mod } \mathfrak{p}, \varphi(x)],$$

et puisque A_0 n'est pas divisible par le système modulaire premi $[\mathfrak{p}, \varphi(x)]$, il s'ensuit que

$$r_1 \equiv r_2 \qquad [\text{mod } \mathfrak{p}, \varphi(x)].$$

Donc une congruence du premier degré peut avoir au plus une r cine incongrue $[\text{mod } \mathfrak{p}, \varphi(x)]$.

Revenons au cas général et supposons que r_i est une des racines de la congruence

$$G(r) \equiv 0 \qquad [\text{mod } \mathfrak{p}, \varphi(x)],$$

de sorte que, par suite,

$$G(r) - G(r_i) \equiv (r - r_i) G_1(r) \equiv 0 \qquad [\text{mod } \mathfrak{p}, \varphi(x)],$$

où $G_1(r)$ est une fonction de même nature que $G(r)$ et est au plus de degré $m - 1$.

Dès lors, par induction, en supposant le lemme démontré pour le degré $m - 1$, de sorte que $G_1(r) \equiv 0 [\text{mod } \mathfrak{p}, \varphi(x)]$ ne peut avoir plus de $m - 1$ racines, comme, d'après ce qui précède, $r - r_i \equiv 0$ $[\text{mod } \mathfrak{p}, \varphi(x)]$ ne peut pas avoir plus d'une racine, le théorème est démontré dans le cas général.

Supposons maintenant que la congruence

$$G(r) \equiv 0 \qquad [\text{mod } \mathfrak{p}, \varphi(x)]$$

ait exactement m racines incongrues $[\text{mod } \mathfrak{p}, \varphi(x)]$, et soient r_1, r_2, ..., r_m ces racines; posons encore

$$G(r) = A_0 r^m + A_1 r^{m-1} + \ldots + A_m$$

et formons la congruence

$$A_0 r^m + A_1 r^{m-1} + \ldots + A_m - A_0(r - r_1)(r - r_2) \ldots (r - r_m) \equiv 0 \qquad [\text{mod } \mathfrak{p}, \varphi(x)].$$

Cette congruence est au plus du $(m-1)^{\text{ième}}$ degré, puisque les d termes $A_0 r^m$ se détruisent. Elle a pourtant plus de $m - 1$ raci

congruentes [mod $\mathfrak{p}$, $\varphi(x)$], puisqu'elle est satisfaite par les m racines $r_1, r_2, \ldots, r_m$. Dès lors tous les coefficients de cette congruence doivent être divisibles par le système modulaire [$\mathfrak{p}$, $\varphi(x)$].

Il s'ensuit que la congruence

$$A_0 r^m + A_1 r^{m-1} + \ldots + A_m - A_0 (r - r_1)(r - r_2)\ldots(r - r_m) \equiv 0 \quad [\text{mod } \mathfrak{p}, \varphi(x)]$$

doit être satisfaite *identiquement*, et nous devons avoir

$$\begin{aligned}
-A_1 &\equiv r_1 + r_2 + \ldots + r_m && [\text{mod } \mathfrak{p}, \varphi(x)],\\
+A_2 &\equiv r_1 r_2 + r_1 r_2 + \ldots + r_{m-1} r_m && [\text{mod } \mathfrak{p}, \varphi(x)],\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
(-1)^m A_m &\equiv r_1 r_2 r_3 \ldots r_m && [\text{mod } \mathfrak{p}, \varphi(x)].
\end{aligned}$$

Si donc la congruence de degré m

$$G(r) \equiv 0 \qquad [\text{mod } \mathfrak{p}, \varphi(x)]$$

a exactement m racines $r_1, r_2, \ldots, r_m$, nous avons identiquement la congruence

$$G(r) \equiv A_0 \prod_{i=1}^{i=m} (r - r_i) \qquad [\text{mod } \mathfrak{p}, \varphi(x)].$$

Revenant maintenant à la congruence

$$r^{k^\lambda - 1} - 1 \equiv 0 \qquad [\text{mod } \mathfrak{p}, \varphi(x)],$$

on a vu que cette congruence a $m = k^\lambda - 1$ racines $r_1, r_2, \ldots, r_m$, ces racines étant les résidus du système [$\mathfrak{p}$, $\varphi(x)$], dans lequel l'élément $\varphi(x)$ a la forme

$$\varphi(x) = x^\lambda + \gamma_1 x^{\lambda-1} + \gamma_2 x^{\lambda-2} + \ldots + \gamma_\lambda.$$

Les résidus sont, par conséquent, de la forme

$$\delta_1 x^{\lambda-1} + \delta_2 x^{\lambda-2} + \ldots + \delta_\lambda,$$

où $\delta_1, \delta_2, \ldots, \delta_\lambda$ peuvent prendre des valeurs quelconques parmi les valeurs $\rho_1, \rho_2, \ldots, \rho_k$ de la page 63.

Dès lors on voit que

$$r^{k^\lambda - 1} - 1 \equiv \prod [r - (\delta_1 x^{\lambda-1} + \delta_2 x^{\lambda-2} + \ldots + \delta_\lambda)] \, [\text{mod } \mathfrak{p}, \varphi(x)],$$

où le produit s'étend à la totalité des fonctions que nous avions obtenues en prenant successivement pour chacun des δ les k valeurs ρ_1, ρ_2, ..., ρ_k, excepté le seul cas particulier où chacun des δ est remplacé par la quantité ρ, qui est $\equiv 0 \pmod{\mathfrak{p}, \varphi(x)}$.

Égalant les coefficients des mêmes puissances de r dans les deux membres de la congruence ci-dessus, on a la *forme très générale du théorème de Wilson*

$$-1 = \prod (\delta_1 x^{\lambda-1} + \delta_2 x^{\lambda-2} + \ldots + \delta_\lambda),$$

où le produit s'étend à la totalité des fonctions dans lesquelles les δ ont les valeurs que nous venons d'indiquer.

Nous avons posé $m = k^\lambda - 1$, où $k = (\nu, \mathfrak{p}) = \mathrm{N}(\mathfrak{p}) = p^f$, où p est le plus petit entier divisible par $\mathfrak{p}$ et où l'entier positif f est le *degré* (Dedekind, p. 565) de l'idéal premier $\mathfrak{p}$.

Dès lors $m = p^{\lambda f} - 1$, et la congruence ci-dessus peut s'écrire

$$r^{p^{\lambda f}-1} - 1 \equiv 0 \qquad \pmod{\mathfrak{p}, \varphi(x)}.$$

Considérons la série de fonctions

$$[\psi(x)]^{p^0}, \quad [\psi(x)]^{p^1}, \quad [\psi(x)]^{p^2}, \quad \ldots,$$

où $\psi(x)$ est une fonction entière et arbitraire de x dont les coefficients sont des entiers de Ω.

Dans cette série, nous devons finalement avoir la fonction $[\psi(x)]^{p^s}$ qui est congrue à $[\psi(x)]^{p^0} \pmod{\mathfrak{p}, \varphi(x)}$; car, si cela n'arrive pas avant, cela est certainement vrai pour $s = \lambda f$.

Nous appellerons HAUTEUR (Dedekind, p. 571) de la fonction $\psi(x)$ le plus petit entier rationnel h, différent de zéro, qui satisfait à la congruence

$$[\psi(x)]^{p^h} \equiv \psi(x) \qquad \pmod{\mathfrak{p}, \varphi(x)}.$$

En élevant les deux membres de la congruence précédente à la puissance p^h, nous avons

$$[\psi(x)]^{p^h p^h} \equiv [\psi(x)^{p^h}] \equiv \psi(x) \qquad \pmod{\mathfrak{p}, \varphi(x)},$$

et, par conséquent, aussi

$$[\psi(x)]^{p^{kh+t}} \equiv [\psi(x)]^{p^t} \qquad \pmod{\mathfrak{p}, \varphi(x)}.$$

Si donc $t \equiv s \pmod h$, on a

$$[\psi(x)]^{p^r} \equiv [\psi(x)]^{p^t} \qquad [\bmod \mathfrak{p}, \varphi(x)];$$

et, réciproquement, si l'on a

$$[\psi(x)]^{p^r} \equiv [\psi(x)]^{p^t} \qquad [\bmod \mathfrak{p}, \varphi(x)],$$

on a aussi

$$t \equiv s \qquad (\bmod h).$$

Nous avons aussi démontré les théorèmes suivants d'une manière indirecte :

I. *Si s est incongru à $t \pmod h$, $[\psi(x)]^{p^r}$ est aussi incongru à $[\psi(x)]^{p^t} [\bmod \mathfrak{p}, \varphi(x)]$.*

II. *Si $[\psi(x)]^{p^t}$ est incongru à $[\psi(x)]^{p^r}$, s est incongru à $t \pmod h$.*

Considérons maintenant la série de fonctions en nombre illimité

$$[\psi(x)]^{p^0}, \quad [\psi(x)]^{p^1}, \quad [\psi(x)]^{p^2}, \quad [\psi(x)]^{p^3}, \quad \ldots,$$

relatives au système modulaire $[\mathfrak{p}, \varphi(x)]$.

Les h premières de ces fonctions, h étant la hauteur de la fonction $\psi(x)$, sont incongrues $(\bmod \mathfrak{p}, \varphi(x)]$. Les h suivantes sont les h premières répétées dans le même ordre; par conséquent, nous pouvons (Cf. Dedekind, p. 871) appeler les h fonctions

$$[\psi(x)]^{p^0}, \quad [\psi(x)]^{p^1}, \quad [\psi(x)]^{p^2}, \quad \ldots, \quad [\psi(x)]^{p^{h-1}},$$

la *période* de la fonction $\psi(x)$ relative au système modulaire $[\mathfrak{p}, \varphi(x)]$. Il est clair que la période d'une quelconque des fonctions $[\psi(x)]^{p^t}$, où t est un entier rationnel, contient les mêmes fonctions relativement au système modulaire $[\mathfrak{p}, \varphi(x)]$, comme la période de la fonction $\psi(x)$.

Supposons maintenant que dans la congruence

$$[\psi(x)]^{p^{\lambda f-1}} - 1 \equiv 0 \qquad [\bmod \mathfrak{p}, \varphi(x)],$$

on ait $f = 1$, et considérons la congruence

$$[\psi(x)]^{p^\lambda} \equiv \psi(x) \qquad [\bmod \mathfrak{p}, \varphi(x)].$$

Prenons d'abord dans le domaine des nombres rationnels le système modulaire

$$[p, \Phi(x)],$$

dans lequel p est l'entier rationnel premier qui est divisible par $\mathfrak{p}$; $\Phi(x)$ est de la forme

$$\Phi(x) \equiv x^\lambda + g_1 x^{\lambda-1} + g_2 x^{\lambda-2} + \ldots g_\lambda,$$

où $g_1, g_2, \ldots, g_\lambda$ peuvent prendre tous les valeurs, 0, 1, 2, $\ldots, p-1$. Il y a, par conséquent, $p^\lambda - 1$ résidus du système modulaire $[p, \Phi(x)]$. Dès lors, si $\psi(x)$ est une fonction quelconque de x dont les coefficients soient des entiers rationnels, nous avons

$$[\psi(x)]^{p^\lambda} \equiv \psi(x) \pmod{p, \Phi(x)}.$$

Posons de plus, comme plus haut,

$$\varphi(x) = x^\lambda + \gamma_1 x^{\lambda-1} + \gamma_2 x^{\lambda-2} + \ldots + \gamma_\lambda.$$

Supposons que

$$\begin{aligned} g_1 &\equiv \gamma_1 \pmod{\mathfrak{p}}, \\ g_2 &\equiv \gamma_2 \pmod{\mathfrak{p}}, \\ &\ldots\ldots\ldots\ldots\ldots, \\ g_\lambda &\equiv \gamma_\lambda \pmod{\mathfrak{p}}; \end{aligned}$$

c'est-à-dire que les quantités g_1 et γ_1, g_2 et γ_2, $\ldots$, g_λ et γ_λ soient des entiers algébriques appartenant respectivement aux mêmes classes dans la distribution que nous avons faite à la page 63.

Il s'ensuit immédiatement que le système modulaire $[p, \Phi(x)]$ est divisible par le système modulaire $[\mathfrak{p}, \varphi(x)]$, et que, par conséquent,

$$[\psi(x)]^{p^\lambda} \equiv \psi(x) \quad [\mathrm{mod}\, \mathfrak{p}, \varphi(x)].$$

De là il résulte que *toute fonction entière en x à coefficients entiers a, relativement au système modulaire* $[\mathfrak{p}, \varphi(x)]$, *une hauteur égale au degré de la fonction* $\varphi(x)$.

Nous allons montrer maintenant que *toute fonction de hauteur* λ *relativement au système modulaire* $[\mathfrak{p}, \varphi(x)]$ *est congrue* $[\mathrm{mod}\, \mathfrak{p}, \varphi(x)]$ *à une fonction entière de x, de degré inférieur ou égal à* $\lambda - 1$ *et dont les coefficients sont des entiers rationnels.*

Conformément au théorème précédent, la congruence

$$r^{p^\lambda} - r \equiv 0 \quad [\mathrm{mod}\, \mathfrak{p}, \varphi(x)]$$

est satisfaite par les p^λ fonctions

$$g_1 x^{\lambda-1} + g_2 x^{\lambda-2} + \ldots + g_\lambda,$$

où les g prennent les valeurs 0, 1, 2, ..., $p-1$ et de plus ces p^λ fonctions sont toutes incongrues $[\text{mod } \mathfrak{p}, \varphi(x)]$.

Dès lors, la congruence

$$r^{p^\lambda} - r \equiv 0 \qquad [\text{mod } \mathfrak{p}, \varphi(x)]$$

a un nombre de racines incongrues $[\text{mod } \mathfrak{p}, \varphi(x)]$ égal au degré $d = p^\lambda$ de la fonction, et, par conséquent, d'après le théorème donné page 73, si $r_1, r_2, \ldots, r_{d-1}, r_d = 0$ sont les racines de cette congruence, nous avons la congruence identique

$$r^{p^\lambda} - r \equiv r(r-r_1)(r-r_2)\ldots(r-r_{d-1}) \equiv 0 \qquad [\text{mod } \mathfrak{p}, \varphi(x)].$$

Si maintenant $\chi(x)$ est une fonction de hauteur λ relativement au système modulaire $[\mathfrak{p}, \varphi(x)]$, nous devons avoir

$$[\chi(x)]^{p^\lambda} - \chi(x) \equiv 0 \qquad [\text{mod } \mathfrak{p}, \varphi(x)];$$

et, par conséquent,

$$\chi(x)[\chi(x)-r_1][\chi(x)-r_2]\ldots[\chi(x)-r_{d-1}] \equiv 0 \qquad [\text{mod } \mathfrak{p}, \varphi(x)].$$

Il résulte de ceci que l'on a

$$\chi(x) \equiv r \qquad [\text{mod } \mathfrak{p}, \varphi(x)],$$

où r est une des fonctions entières $r_1, r_2, \ldots, r_{d-1}, r_d = 0$, dont le degré en x est inférieur ou égal à $\lambda - 1$ et dont les coefficients sont des entiers rationnels mod p.

Réciproquement, si $\chi(x)$ est congru $[\text{mod } \mathfrak{p}, \varphi(x)]$ à r, r étant une fonction entière en x dont les coefficients sont des entiers rationnels, de sorte que

$$\chi(x) = r \qquad [\text{mod } \mathfrak{p}, \varphi(x)],$$

on a aussi

$$[\chi(x)]^{p^\lambda} \equiv r^{p^\lambda} \qquad [\text{mod } \mathfrak{p}, \varphi(x)].$$

Mais puisque

$$r^{p^\lambda} \equiv r \qquad [\text{mod } \mathfrak{p}, \varphi(x)],$$

il s'ensuit que

$$[\chi(x)]^{p^\lambda} \equiv r \qquad [\mathrm{mod}\, \mathfrak{p}, \varphi(x)],$$

et

$$[\chi(x)]^{p^\lambda} \equiv \chi(x) \qquad [\mathrm{mod}\, \mathfrak{p}, \varphi(x)].$$

Nous avons donc le théorème suivant :

Toute fonction entière en x dont les coefficients appartiennent à Ω qui est congrue $[\mathrm{mod}\, \mathfrak{p}, \varphi(x)]$ *à une fonction entière en x dont les coefficients sont des entiers rationnels, a pour hauteur λ relativement au système modulaire* $[\mathfrak{p}, \varphi(x)]$; *et toute fonction entière en x dont les coefficients appartiennent à Ω, qui a pour hauteur λ relativement au système modulaire* $[\mathfrak{p}, \varphi(x)]$, *est congrue, relativement à ce système, à une fonction entière en x de degré inférieur ou égal à $\lambda - 1$, et à coefficients entiers et rationnels réduits* mod p.

Nous savons que, si $\mathrm{R}(\alpha, \beta, \gamma, \ldots) = l\alpha^n + l_1\alpha^{n-1}\beta + \ldots$ est une fonction entière par rapport aux quantités $\alpha, \beta, \gamma, \ldots$ et si $l, l_1, \ldots$ sont des entiers rationnels, on a

$$[\mathrm{R}(\alpha, \beta, \gamma, \ldots)]^p \equiv \mathrm{R}(\alpha^p, \beta^p, \gamma^p, \ldots) \qquad (\mathrm{mod}\, p),$$

où p est un entier premier. Dès lors, si p est divisible par l'idéal premier $\mathfrak{p}$, nous avons

$$[\mathrm{R}(\alpha, \beta, \gamma, \ldots)]^p \equiv \mathrm{R}(\alpha^p, \beta^p, \gamma^p, \ldots) \qquad (\mathrm{mod}\, \mathfrak{p}).$$

Supposons maintenant que $\psi(x)$, fonction quelconque du domaine $[(\varphi, x)]$, soit de hauteur h et formons la fonction symétrique

$$\sigma = \mathrm{S}\left([\psi(x)],\ [\psi(x)]^p,\ [\psi(x)]^{p^2},\ [\psi(x)]^{p^{h-1}}\right),$$

de sorte que, par conséquent, σ est une fonction entière en x dont les coefficients sont des entiers de Ω.

On voit que

$$\begin{aligned}
\sigma^p &\equiv \mathrm{S}\left([\psi(x)],\ [\psi(x)]^p,\ [\psi(x)]^{p^2}, \ldots, [\psi(x)^{p^{h-1}}]\right)^p \\
&\equiv \mathrm{S}\left([\psi(x)]^p, [\psi(x)]^{p^2}, [\psi(x)]^{p^3}, \ldots, [\psi(x)^{p^h}]\right) \\
&\equiv \mathrm{S}\left([\psi(x)]^p, [\psi(x)]^{p^2}, [\psi(x)]^{p^3}, \ldots, [\psi(x)]\right) \qquad (\mathrm{mod}\, \mathfrak{p}),
\end{aligned}$$

ou

$$\sigma^p \equiv \sigma \qquad (\mathrm{mod}\, \mathfrak{p}),$$

puisque

$$\sigma^{p^2} \equiv \sigma^p \equiv \sigma \pmod{\mathfrak{p}},$$

il s'ensuit aussi que

$$\sigma^{p^h} \equiv \sigma \quad [\mathrm{mod}\,\mathfrak{p}, \varphi(x)].$$

Il résulte de là que, puisque la hauteur de la fonction σ relativement au système modulaire $[\mathfrak{p}, \varphi(x)]$ est λ, la fonction σ est congrue $[(\mathrm{mod}\,\mathfrak{p}, \varphi(x)]$ à une fonction entière en x de degré inférieur ou égal à $\lambda - 1$, dont les coefficients sont des entiers rationnels réduits mod p.

De la même manière, on peut prouver que *toute fonction entière symétrique des h fonctions*

$$[\psi(x)], \quad [\psi(x)]^p, \quad [\psi(x)]^{p^2}, \quad \ldots, \quad [\psi(x)]^{p^{h-1}}$$

est congrue $[\mathrm{mod}\,\mathfrak{p}, \varphi(x)]$ *à une fonction entière de x de degré inférieur ou égal à* $\lambda - 1$ *et dont les coefficients sont des entiers rationnels réduits* $(\mathrm{mod}\,p)$.

Formons maintenant le produit

$$[r - \psi(x)] \cdot \{r - [\psi(x)]^p\} \cdot \{r - [\psi(x)]^{p^2}\} \ldots \{r - [\psi(x)]^{p^{h-1}}\},$$

que nous désignerons par $\mathrm{P}(r, x)$.

En développant ce produit suivant les puissances de r, nous avons

$$\mathrm{P}(r, x) \equiv r^h + c_1 r^{h-1} + c_2 r^{h-2} + \ldots + c_h,$$

où $c_1, c_2, \ldots, c_h$ sont des fonctions entières symétriques des fonctions

$$\psi(x), \quad [\psi(x)]^p, \quad [\psi(x)]^{p^2}, \quad \ldots, \quad [\psi(x)]^{p^{h-1}}.$$

La fonction $\mathrm{P}(r, x)$ *est donc congrue* $[(\mathrm{mod}\,\mathfrak{p}, \varphi(x)]$ *à une fonction entière de degré h en r, dont les coefficients sont des fonctions entières en x de degré inférieur ou égal à* $\lambda - 1$, *et les coefficients de ces fonctions de x sont des entiers rationnels réduits* $(\mathrm{mod}\,p)$.

La fonction $\mathrm{P}(r, x)$ peut être appelée une *fonction première* (Dedekind, p. 571); car on peut prouver aisément qu'il n'est pas possible de déterminer deux fonctions $f(r, x)$, $g(r, x)$ entières en r et en x, telles que

$$\mathrm{P}(r, x) \equiv f(r, x)\, g(r, x) \quad [\mathrm{mod}\,\mathfrak{p}, \varphi(x)].$$

Revenons à la congruence

$$[\psi(x)]^{p^{\lambda f}} \equiv \psi(x) \qquad [\mathrm{mod}\ \mathfrak{p}, \varphi(x)];$$

nous voyons que si h est la hauteur de la fonction $\psi(x)$ relativement au système modulaire $[\mathfrak{p}, \varphi(x)]$, on a

$$[\psi(x)]^{p^h} \equiv \psi(x) \qquad [\mathrm{mod}\ \mathfrak{p}, \varphi(x)].$$

Dès lors il s'ensuit que

$$[\psi(x)]^{p^h} \equiv [\psi(x)]^{p^0} \qquad [\mathrm{mod}\ \mathfrak{p}, \varphi(x)].$$

De cette congruence (*voir* p. 75), nous pouvons aussi déduire la congruence

$$h \equiv \lambda f \qquad (\mathrm{mod}\ h),$$

et par conséquent λf doit être divisible par h. Nous avons ainsi le théorème suivant : *La hauteur d'une fonction quelconque relativement au système modulaire* $[\mathfrak{p}, \varphi(x)]$ *est un diviseur de* λf *où* f *est le degré de* $\mathfrak{p}$, *et* λ *le degré de la fonction* $\varphi(x)$ *en* x.

Nous allons montrer maintenant que, *si* h *est un diviseur de* λf, *il existe des fonctions de hauteur* h *relativement au système modulaire* $[\mathfrak{p}, \varphi(x)]$.

S'il existe de telles fonctions, par exemple $\psi(x)$, il en existe évidemment h, savoir

$$\psi(x), \quad [\psi(x)]^p, \quad [\psi(x)]^{p^2}, \quad \ldots, \quad [\psi(x)]^{p^{h-1}}.$$

Dès lors en supposant qu'il existe des fonctions de hauteur h relativement au système modulaire $[\mathfrak{p}, \varphi(x)]$, on voit que l'on peut partager toutes ces fonctions en groupes, et qu'il y aura h fonctions dans chaque groupe.

Désignons le nombre de groupes par γ_h et par conséquent le nombre des fonctions incongrues de hauteur h relativement du système modulaire $[\mathfrak{p}, \varphi(x)]$ par $h\gamma_h$.

Puisque λf est divisible par h, nous pouvons poser

$$\lambda f = hg,$$

où g est un entier rationnel.

Or, puisque

$$\frac{p^{\lambda f}-1}{p^h-1}=1+p^h+p^{2h}+\ldots+p^{(g-1)h},$$

de sorte que $\frac{p^{\lambda f}-1}{p^h-1}$ est un entier positif, il s'ensuit que

$$\frac{[\psi(x)]^{p^{\lambda f-1}}-1}{[\psi(x)]^{p^h-1}-1}=\mathfrak{G}(x),$$

où $\mathfrak{G}(x)$ est une fonction entière en x de degré $p^{\lambda f}-p^h$ à coefficients entiers appartenant au domaine Ω.

Dès lors

$$[\psi(x)]^{p^{\lambda f}}-\psi(x)\equiv\{[\psi(x)]^{p^h}-\psi(x)\}\mathfrak{G}(x)\equiv 0 \qquad [\text{mod } \mathfrak{p}, \varphi(x)].$$

Puisque

$$[\psi(x)]^{p^{\lambda f}}-\psi(x)\equiv 0 \qquad [\text{mod } \mathfrak{p}, \varphi(x)]$$

a $p^{\lambda f}$ racines incongrues $[\text{mod } \mathfrak{p}, \varphi(x)]$, et puisque $\mathfrak{G}(x)$ ne peut pas avoir plus de $p^{\lambda f}-p^h$ racines incongrues, il s'ensuit que

$$[\psi(x)]^{p^h}-\psi(x)\equiv 0 \qquad [\text{mod } \mathfrak{p}, \varphi(x)]$$

doit avoir au moins p^h de ces racines. Puisque cette congruence ne peut pas avoir un nombre plus grand de racines incongrues

$$[\text{mod } \mathfrak{p}, \varphi(x)],$$

il en résulte que la congruence

$$[\psi(x)]^{p^h}-\psi(x)=0 \qquad [\text{mod } \mathfrak{p}, \varphi(x)]$$

a p^h racines incongrues $[\text{mod } \mathfrak{p}, \varphi(x)]$.

Si maintenant nous avons une fonction $\varpi(x)$ de hauteur h relativement au système modulaire $[\mathfrak{p}, \varphi(x)]$, elle satisfait à la congruence

$$(1) \qquad [\omega(x)]^{p^h}\equiv\omega(x) \qquad [\text{mod } \mathfrak{p}, \varphi(x)],$$

et réciproquement, si la fonction $\varpi(x)$ satisfait à la congruence (1) elle est de hauteur h ou de hauteur d, d étant un diviseur de h.

Dès lors, nous voyons que chacune des racines incongrues

$$[\text{mod } \mathfrak{p}, \varphi(x)],$$

qui satisfait à la congruence (1), est ou de hauteur h ou de hauteur d, d étant un diviseur de h.

Si d est un diviseur de h, le nombre des fonctions incongrues de hauteur d relativement au système modulaire $[\mathfrak{p}, \varphi(x)]$ est, en employant la notation précédente, égal à $d\chi_d$.

Il en résulte donc que le nombre des fonctions incongrues de hauteur h ou de hauteur d, d étant un diviseur de h relativement au système modulaire $[\mathfrak{p}, \varphi(x)]$, est

$$\Sigma d\chi_d,$$

où la sommation s'étend à tous les diviseurs de h, y compris h. Puisque ce nombre est aussi égal à p^h, il s'ensuit que

$$\Sigma d\chi_d = p^h.$$

Nous avons vu p. 73 que

$$(\mathrm{I}) \qquad r^{p^h} - r \equiv \Pi(r - r_i) \qquad [\mathrm{mod}\,\mathfrak{p}, \varphi(x)],$$

où le produit doit être étendu à un système de p^h fonctions incongrues de hauteur h ou de hauteur d, d étant un diviseur de h, relativement au système modulaire $[\mathfrak{p}, \varphi(x)]$.

Si une des racines, r_k, par exemple, de la congruence précédente est de hauteur h relativement au système modulaire $[\mathfrak{p}, \varphi(x)]$, le produit

$$(r - r_k)(r - r_k^p)(r - r_k^{p^2}) \ldots (r - r_k^{p^{h-1}})$$

entre comme facteur dans (I).

Nous pouvons écrire, au lieu de ce produit, la fonction $\mathrm{P}(r, x)$ qui est entière en r et x, de degré h en r et en x, de degré inférieur ou égal à $\lambda - 1$ et dont ces coefficients sont des entiers rationnels réduits $(\mathrm{mod}\, p)$.

De la même manière, si d est un diviseur de h, il entre comme facteur, dans (I), le produit

$$(r - r_\nu)(r - r_\nu^p)(r - r_\nu^{p^2}) \ldots (r - r_\nu^{p^{d-1}}),$$

où r_ν est une fonction de hauteur d relativement au système modulaire.

Nous pouvons donc remplacer le produit par une autre fonction première entière en r et x, de degré d en r et en x, de degré inférieur ou égal à $\lambda - 1$, dont les coefficients sont des entiers rationnels réduits $(\mathrm{mod}\, p)$.

Il est ainsi évident que l'on a

$$r^{p^h} - r \equiv \Pi P(r, x) \qquad [\text{mod } \mathfrak{p}, \varphi(x)],$$

où le produit doit être étendu à un certain nombre de fonctions premières.

De telles fonctions, dans lesquelles les coefficients des plus hautes puissances de r sont l'unité, sont dites *fonctions premières primaires*.

Je ne calculerai pas le nombre de ces fonctions qui sont de degré h en r ou qui ont pour degré un diviseur de h.

Si nous désignons par ω_k le nombre des fonctions premières primaires de hauteur h relativement au système modulaire $[\mathfrak{p}, \varphi(x)]$, on peut montrer que

$$\Sigma d\omega_d = \Sigma d\chi_d = p^h.$$

Par conséquent, *le produit précédent doit s'étendre à toutes les fonctions premières primaires* $P(r, x)$ *possibles dont le degré en* r *est* h *ou un diviseur de* h *et, en* x, *est inférieur à* $\lambda - 1$ *et dont les coefficients sont des entiers rationnels réduits* mod p.

Ce théorème a été démontré par Dedekind (p. 571 et 572) pour le cas simple des entiers algébriques relatifs à un idéal premier. Dans ses *Leçons*, le professeur Frobenius a complété les résultats de Dedekind, et, en suivant ses méthodes, je suis arrivé aux résultats précédents pour les fonctions algébriques en $[\varphi, x]$ relativement au système modulaire $[\mathfrak{p}, \varphi(x)]$.

Comme aucune des fonctions premières n'est répétée dans le produit ci-dessus, nous pouvons écrire l'équivalence suivante

$$[\mathfrak{p}, \varphi(x), r^{p^h} - r] \backsim \Pi[\mathfrak{p}, \varphi(x), P(r, x)],$$

où le produit doit être étendu à tous les systèmes modulaires possibles de la forme $[\mathfrak{p}, \varphi(x), P(r, x)]$ dans lesquels nous écrirons pour la fonction première $P(r, x)$ toutes les fonctions premières possibles dont le degré en r est h ou un diviseur de h et dont le degré en x est inférieur ou égal à $\lambda - 1$. Car, si nous nous bornons aux coefficients rationnels et entiers dans ces fonctions premières, il est évident, puisque deux quelconques de ces fonctions $P_m(r, x)$ et $P_n(r, x)$ n'ont pas de diviseur commun en r, que nous pouvons trouver deux fonctions

$\overline{\mathrm{P}}_m(r, x)$ et $\overline{\mathrm{P}}_n(r, x)$ entières en r et x à coefficients entiers, de telle sorte qu

$$\mathrm{P}_m(r, x)\,\overline{\mathrm{P}}_m(r, x) + \mathrm{P}_n(r, x)\,\overline{\mathrm{P}}_n(r, x) = \mathrm{K}(x),$$

où $k(x)$ n'a pas de diviseur commun avec $\varphi(x) \pmod{\mathfrak{p}}$.

On voit aussi que le plus grand commun diviseur de $\mathrm{K}(x)$ et $\varphi(x) \pmod{\mathfrak{p}}$ est un entier α de $[\wp]$, et que, finalement, le plus grand commun diviseur de α et $\mathfrak{p}$ est $\wp$.

Dès lors le produit

$$\begin{aligned}(\mathrm{II}) \qquad & [\mathfrak{p}, \varphi(x), \mathrm{P}_m(r, x)]\,[\mathfrak{p}, \varphi(x), \mathrm{P}_n(r, x)] \\ & \backsim [\mathfrak{p}^2, \mathfrak{p}\varphi(x), \mathfrak{p}\mathrm{P}_n(r, x), \varphi(x)^2, \varphi(x)\,\mathrm{P}_n(r, x), \\ & \qquad \mathfrak{p}\mathrm{P}_m(r, x), \varphi(x)\,\mathrm{P}_m(r, x), \mathrm{P}_m(r, x).\ \mathrm{P}_n(r, x)].\end{aligned}$$

Avec les éléments $\mathfrak{p}^2$, $\mathfrak{p}\varphi(x)$, $\mathfrak{p}\,\mathrm{P}_n(r, x)$, $\mathfrak{p}\,\mathrm{P}_m(r, x)$, nous formons le système

$$\begin{aligned}& [\mathfrak{p}^2, \mathfrak{p}\varphi(x), \mathfrak{p}\mathrm{P}_n(r, x), \mathfrak{p}\mathrm{P}_m(r, x)] \\ & \quad \backsim \mathfrak{p}[\mathfrak{p}, \varphi(x), \mathrm{P}_n(r, x), \mathrm{P}_m(r, x)] \backsim \mathfrak{p}[\wp] \backsim \mathfrak{p},\end{aligned}$$

et, comme nous pouvons maintenant adjoindre $\mathfrak{p}$ au système (I), nous formons, avec les éléments $\mathfrak{p}\varphi(x)$ [qui peut aussi être adjoint au système (I)], $[\varphi(x)]^2$, $\varphi(x)\,\mathrm{P}_n(r, x)$ et $\varphi(x)\,\mathrm{P}_m(r, x)$, le système

$$\varphi(x)[\mathfrak{p}, \varphi(x), \mathrm{P}_n(r, x), \mathrm{P}_m(r, x)] \backsim \varphi(x)[\wp] \backsim \varphi(x).$$

Dès lors, le second membre de l'équivalence (I) est équivalent à

$$[\mathfrak{p}, \varphi(x), \mathrm{P}_m(r, x)\,\mathrm{P}_n(r, x)],$$

ce qui démontre le théorème.

Réduction des systèmes modulaires de seconde espèce lorsque la seconde puissance ou des puissances plus hautes de l'idéal premier $\mathfrak{p}$ entrent comme éléments.

Dans le système modulaire de la p. 62,

$$[\nu\mu, f_1(x), f_2(x), \ldots, f_n(x)],$$

nous supposions que m était le plus petit entier rationnel qui fût divisible par $\nu\mu$, et nous supposions qu'aucun des facteurs de m n'était contenu comme facteur dans le discriminant de Ω.

Nous allons maintenant nous débarrasser de cette restriction et nous allons avoir, par conséquent, à discuter les systèmes dans lesquels les secondes ou plus hautes puissances de l'idéal premier $\mathfrak{p}$ entrent comme éléments.

Si cet idéal entre à la seconde puissance, la forme du système modulaire que nous avons à considérer est (*voir* p. 61)

$$(\mathrm{I}) \qquad [\mathfrak{p}^2, \mathfrak{p}g_1(x), \mathfrak{p}g_2(x), \ldots, \mathfrak{p}g_m(x), f_1(x), f_2(x), \ldots, f_n(x)],$$

où tous les éléments qui entrent appartiennent au domaine $[\varphi, x]$.

Pour abréger, nous désignerons le système des éléments $f_1(x)$, $f_2(x)$, $\ldots$, $f_n(x)$ par $\prod_{\nu=1}^{\nu=n}[f_\nu(x)]$ et nous pourrons, par conséquent, écrire le système sous la forme

$$(\mathrm{I}) \qquad \left\{\mathfrak{p}^2, \mathfrak{p}\prod_{\mu=1}^{\mu=m}[g_\mu(x)], \prod_{\nu=1}^{\nu=n}[f_\nu(x)]\right\}.$$

Grâce à la présence des éléments $\prod_{\nu=1}^{\nu=n}[f_\nu(x)]$ dans ce système, nous pouvons adjoindre les éléments $\mathfrak{p}\prod_{\nu=1}^{\nu=n}[f_\nu(x)$, sans que le système cesse d'être équivalent à lui-même; il devient alors

$$\left\{\mathfrak{p}^2, \mathfrak{p}\prod_{\mu=1}^{\mu=m}[g_\mu(x)], \mathfrak{p}\prod_{\nu=1}^{\nu=n}[f_\nu(x)], \prod_{\nu=1}^{\nu=n}[f_\nu(x)]\right\}.$$

Avec les éléments $\mathfrak{p}^2$, $\mathfrak{p}\prod_{\nu=1}^{\nu=n}[f_\nu(x)]$, nous construisons le système

$$\left\{\mathfrak{p}^2, \mathfrak{p}\prod_{\nu=1}^{\nu=n}[f_\nu(x)]\right\} \backsim \left\{\mathfrak{p}, \prod_{\nu=1}^{\nu=n}[f_\nu(x)]\right\}.$$

Il résulte de ce qui a été dit p. 65 que

$$(a) \qquad \left\{\mathfrak{p}, \prod_{\nu=1}^{\nu=n}[f_\nu(x)]\right\} \backsim [\mathfrak{p}, \overline{\mathrm{F}}(x)].$$

De ce système (a), que nous appelons *système modulaire auxiliaire*, nous tirons, d'une part,

$$\overline{\mathrm{F}}(x) = \mathfrak{p}\overline{\pi}(x) + \sum_{\nu=1}^{\nu=n} f_\nu(x)\,\overline{f}_\nu(x), \tag{1}$$

où $\overline{\pi}(x)$, $\overline{f}_1(x)$, $\overline{f}_2(x)$, . . , , $\overline{f}_n(x)$ sont des quantités déterminées de $[\varphi, x]$ et, d'autre part,

$$f_\nu(x) = \mathfrak{p}\pi_\nu(x) + \overline{\mathrm{F}}(x)\,\mathrm{F}_\nu(x) \qquad (\nu = 1, 2, \ldots, n), \tag{2}$$

où $\pi_\nu(x)$, $\mathrm{F}_\nu(x)$ $(\nu = 1, 2, \ldots, n)$ sont aussi des quantités de $[\varphi, x]$. Si nous posons

$$\mathrm{F}(x) = \overline{\mathrm{F}}(x) - \mathfrak{p}\overline{\pi}(x),$$

il résulte de (1) que

$$\mathrm{F}(x) = \sum_{\nu=1}^{\nu=n} f_\nu(x)\,\overline{f}_\nu(x).$$

Dès lors, puisque $\mathrm{F}(x)$ peut s'exprimer par une forme linéaire en fonction des éléments $f_1(x)$, $f_2(x)$, . . . , $f_n(x)$ dont les coefficients sont des quantités de $[\varphi, x]$, on voit que nous pouvons ajouter $\mathrm{F}(x)$ au système (I) sans qu'il cesse d'être équivalent à lui-même.

De la seconde des relations ci-dessus il résulte que

$$f_\nu(x) = \mathfrak{p}\pi_\nu(x) + \mathrm{F}(x)\,\mathrm{F}_\nu(x) + \mathfrak{p}\overline{\pi}(x)\,\mathrm{F}_\nu(x) \qquad (\nu = 1, 2, \ldots, n),$$

et si, pour abréger, nous posons

$$\pi_\nu(x) + \overline{\pi}(x)\,\mathrm{F}_\nu(x) = \mathrm{II}_\nu(x),$$

nous avons

$$f_\nu(x) = \mathfrak{p}\mathrm{II}_\nu(x) + \mathrm{F}(x)\,\mathrm{F}_\nu(x) \qquad (\nu = 1, 2, \ldots, n).$$

Nous pouvons donc écrire le système (I) sous la forme

$$\left\{\mathfrak{p}^2,\ \mathfrak{p}\prod_{\mu=1}^{\mu=m}[g_\mu(x)],\ \prod_{\nu=1}^{\nu=n}[\mathfrak{p}\mathrm{II}_\nu(x) + \mathrm{F}(x)\,\mathrm{F}_\nu(x)],\ \mathrm{F}(x)\right\},$$

système qui, à cause de la présence de $\mathrm{F}(x)$, devient

$$\left\{\mathfrak{p}^2,\ \mathfrak{p}\prod^{\mu=m}[g_\mu(x)],\ \mathfrak{p}\prod^{\nu=n}[\mathrm{II}_\nu(x)],\ \mathrm{F}(x)\right\}. \tag{I'}$$

Le système

$$\left\{\mathfrak{p}^2,\ \mathfrak{p}\prod_{\mu=1}^{\mu=m}[g_\mu(x)],\ \mathfrak{p}\prod_{\nu=1}^{\nu=n}[\Pi_\nu(x)]\right\}$$

est équivalent à

$$\mathfrak{p}\left\{\mathfrak{p},\ \prod_{\mu=1}^{\mu=m}[g_\mu(x)],\ \prod_{\nu=1}^{\nu=n}[\Pi_\nu(x)]\right\},$$

qui (*voir* p. 65) est équivalent à

$$\mathfrak{p}[\mathfrak{p},\ G(x)].$$

Dès lors le système (I′) peut s'écrire

$$[\mathfrak{p}^2,\ \mathfrak{p}G(x),\ F(x)]. \tag{II}$$

Nous pouvons adjoindre à ce système l'élément $\mathfrak{p}F(x)$ et considérer alors le système

$$[\mathfrak{p}^2,\ \mathfrak{p}G(x),\ \mathfrak{p}F(x),\ F(x)];$$

avec les éléments $\mathfrak{p}^2$, $\mathfrak{p}G(x)$, $\mathfrak{p}F(x)$ nous formons le système

$$[\mathfrak{p}^2,\ \mathfrak{p}G(x),\ \mathfrak{p}F(x)] \backsim \mathfrak{p}[\mathfrak{p},\ G(x),\ F(x)].$$

Le système $[\mathfrak{p},\ G(x),\ F(x)]$ est, ou bien équivalent à

$$[\mathfrak{p},\ \theta(x)],$$

où $\theta(x)$ est le plus grand commun diviseur $(\mathrm{mod}\,\mathfrak{p})$ de $G(x)$ et de $F(x)$ ou bien à

$$[\nu],$$

lorsque les deux éléments $G(x)$ et $F(x)$ n'ont pas de diviseur commun $(\mathrm{mod}\,\mathfrak{p})$. Dans le dernier cas puisque

$$[\mathfrak{p}^2,\ \mathfrak{p}G(x),\ \mathfrak{p}F(x)] \backsim [\mathfrak{p}],$$

le système (II) prend la forme

$$[\mathfrak{p},\ F(x)],$$

et peut être étudié d'après les méthodes déjà employées dans les recherches précédentes.

En considérant le cas de

$$[\mathfrak{p},\ G(x),\ F(x)] \backsim [\mathfrak{p},\ \theta(x)], \tag{a}$$

on voit que l'on a d'une part

$$\theta(x) = \mathfrak{p}\,K(x) + G(x)\,G_1(x) + F(x)\,F_1(x).$$

où $K(x)$, $G_1(x)$ et $F_1(x)$ sont des quantités déterminées de $[\varphi, x]$, et par conséquent

$$\mathfrak{p}\theta(x) = \mathfrak{p}^2 K(x) + \mathfrak{p}\,G(x)\,G_1(x) + \mathfrak{p}\,F(x)\,F_1(x),$$

de sorte que

$$\mathfrak{p}\theta(x) \equiv 0 \qquad [\mathrm{mod}\,\mathfrak{p}^2, \mathfrak{p}\,G(x), F(x)],$$

et par conséquent cette quantité peut être ajoutée au système (II). Nous déduirons aussi du système (a)

$$G(x) = \mathfrak{p}\,l(x) + \theta(x)\,G(x),$$

où $l(x)$ et $G(x)$ sont des quantités déterminées de $[\varphi, x]$.

Dès lors

$$\mathfrak{p}G(x) = \mathfrak{p}^2 l(x) + \mathfrak{p}\,\theta(x)\,G(x)$$

et par conséquent, lorsque $\mathfrak{p}\theta(x)$ a été adjoint au système (II), on peut y supprimer $\mathfrak{p}G(x)$.

La valeur suivante de $F(x)$ dérive immédiatement de (a) :

$$F(x) = \mathfrak{p}\varphi(x) + \theta(x)\,\theta^{(1)}(x)$$

où $\varphi(x)$ et $\theta'(x)$ sont des quantités déterminées de $[\varphi, x]$.

Nous pouvons, par suite de ce qui a été dit plus haut, mettre le système modulaire (II) sous la forme

$$(\mathrm{II}') \qquad [\mathfrak{p}^2, \mathfrak{p}\theta(x), \mathfrak{p}\varphi(x) + \theta(x)\,\theta^{(1)}(x)].$$

A cause de la présence de $\mathfrak{p}^2$, $\mathfrak{p}\theta(x)$ dans le système (II') nous pouvons supposer que les éléments ont été réduits de telle sorte que le coefficient de la plus haute puissance de x dans $\theta^{(1)}(x)$ soit l'unité, et que le degré de $\varphi(x)$ soit inférieur au degré $\theta(x)$ par rapport à x.

Nous pouvons, de plus supposer dans le système (II'), que

1° En vertu de la congruence (a), $\theta(x)$ est de la forme

$$\theta(x) = x^{\mu} + \gamma_1 x^{\mu-1} + \gamma_2 x_+^{-2} + \ldots + \gamma_{\mu},$$

où $\gamma_1, \gamma_2, \ldots, \gamma_{\mu}$ sont pris parmi les entiers déterminés $\rho_1, \rho_2, \ldots, \rho_k$.

2° $\theta^{(1)}(x)$ est de la forme

$$\theta^{(1)}(x) = x^{\nu} + \delta_1 x^{\nu-1} + \delta_2 x^{\nu-2} + \ldots + \delta_{\nu}$$

où les δ sont aussi pris parmi les ρ.

3° $\varphi(x)$ est de la forme

$$\varphi(x) = \varepsilon_0 x^{\pi} + \varepsilon_1 x^{\pi-1} + \varepsilon_2 x^{\pi-2} + \ldots + \varepsilon_{\pi},$$

où les ε sont aussi pris parmi les ρ, et où $\pi < \mu$.

Supposons que par une autre méthode le système modulaire initial (I) ait été réduit à une forme

$$[\mathfrak{p}^2, \mathfrak{p}\theta_1(x), \mathfrak{p}\varphi_1(x) + \theta_1(x)\theta_1^{(1)}(x)],$$

où les éléments correspondants remplissent les trois conditions que nous venons d'indiquer.

Nous avons alors

$$(b)\quad [\mathfrak{p}^2, \mathfrak{p}\theta(x), \mathfrak{p}\varphi(x) + \theta(x)\theta^{(1)}(x)] \backsim [\mathfrak{p}^2, \mathfrak{p}\theta_1(x), \mathfrak{p}\varphi_1(x) + \theta_1(x)\theta_1^{(1)}(x)]$$

et nous pouvons montrer que

$$\theta(x) = \theta_1(x), \qquad \varphi(x) = \varphi_1(x)$$

et

$$\theta^{(1)}(x) = \theta_1^{(1)}(x).$$

En effet, il résulte de (b) que

$$\begin{aligned}&\mathfrak{p}\varphi_1(x) + \theta_1(x)\theta_1^{(1)}(x)\\ &\quad \equiv \mathfrak{p}\theta(x) f(x) + [\mathfrak{p}\varphi(x) + \theta(x)\theta^{(1)}(x)] g(x) \pmod{\mathfrak{p}^2},\end{aligned}$$

où $f(x)$ et $g(x)$ sont des quantités du domaine $[\rho, x]$.

Pour éviter des répétitions, toutes les quantités qui sont introduites peuvent, une fois pour toutes, être considérées comme appartenant au domaine $[\rho, x]$, et pour abréger nous nous servirons du signe fonctionnel pour la fonction de x.

D'après la congruence précédente nous avons

$$\theta_1\theta_1^{(1)} = \theta\theta^{(1)} g \pmod{\mathfrak{p}}. \tag{1}$$

De même il résulte aussi de (b) que

$$\mathfrak{p}\varphi + \theta\theta^{(1)} \equiv \mathfrak{p}\theta_1 f_1 + (\mathfrak{p}\varphi_1 + \theta_1\theta_1^{(1)}) g_1 \pmod{\mathfrak{p}^2},$$

ou

$$\theta\theta^{(1)} \equiv \theta_1\theta_1^{(1)} g_1 \pmod{\mathfrak{p}}. \tag{2}$$

En multipliant (1) et (2) membre à membre nous avons

$$\theta\theta^{(1)}\theta_1\theta_1^{(1)} \equiv \theta\theta^{(1)}\theta_1\theta_1^{(1)} g g_1 \pmod{\mathfrak{p}},$$

et par conséquent, puisque le produit $\theta\theta^{(1)}\theta_1\theta_1^{(1)}$ n'est pas divisible par $\mathfrak{p}$, il s'ensuit que

$$1 \equiv g g_1 \pmod{\mathfrak{p}}$$

et par conséquent g et g_1 sont des unités algébriques du domaine $[\rho]$.

Dès lors en vertu de (1) ou (2) nous avons

$$\theta\theta^{(1)} \equiv \theta_1\theta_1^{(1)} \pmod{\mathfrak{p}} \ldots (i).$$

De plus, nous tirons de (b)

$$\mathfrak{p}\theta_1 \equiv \mathfrak{p}\theta . A + (\theta\theta^{(1)} + \mathfrak{p}\varphi) B \pmod{\mathfrak{p}^2},$$

et de cette expression il résulte que $\theta\theta' B$ doit être divisible par $\mathfrak{p}$. Comme θ et $\theta^{(1)}$ ont été réduits tous deux relativement au module $\mathfrak{p}$, le facteur B doit être divisible par $\mathfrak{p}$. Nous pouvons donc poser $B = B_1\mathfrak{p}$.

Par conséquent de la congruence précédente nous tirons

$$\theta_1 \equiv \theta A + (\theta\theta^{(1)} + \mathfrak{p}\varphi) B_1 \pmod{\mathfrak{p}},$$

ou

$$\theta_1 \equiv \theta (A + B_1\theta^{(1)}) \pmod{\mathfrak{p}}. \tag{3}$$

De la même façon on peut montrer que

$$\theta \equiv \theta_1 (A^{(1)} + B_1^{(1)}\theta_1^{(1)}) \pmod{\mathfrak{p}}, \tag{4}$$

et par conséquent

$$\theta\theta_1 \equiv \theta\theta_1 (A + B_1\theta^{(1)}) (A^{(1)} + B_1^{(1)}\theta_1^{(1)}) \pmod{\mathfrak{p}}.$$

Dès lors, en raisonnant comme plus haut, $A + B_1\theta^{(1)}$ et $A^{(1)} + B_1^{(1)}\theta_1^{(1)}$ doivent être des unités algébriques, et alors de (3) ou (4) nous déduisons

$$\theta \equiv \theta_1 \pmod{\mathfrak{p}}.$$

Mais comme les coefficients de 0 et 0_1 ont été réduits (mod $\mathfrak{p}$), il s'ensuit que

$$0 = \theta_1 \ldots (ii)$$

et par conséquent de (i)

$$\theta^{(1)} = \theta_1^{(1)} \ldots (iii)$$

En revenant à l'équivalence (b) on voit que

$$(\mathfrak{p}^2, \mathfrak{p}\theta, \mathfrak{p}\varphi + \theta\theta^{(1)}) \backsim (\mathfrak{p}^2, \mathfrak{p}\theta_1, \mathfrak{p}\varphi_1 + \theta_1\theta_1^{(1)}, \mathfrak{p}\varphi + \theta\theta^{(1)}),$$

ou, puisque $0 = 0_1$ et $0^{(1)} = 0_1^{(1)}$,

$$(\mathfrak{p}^2, \mathfrak{p}\theta, \mathfrak{p}\varphi + \theta\theta^{(1)}) \backsim [\mathfrak{p}^2, \mathfrak{p}\theta, \mathfrak{p}\varphi_1 + \theta\theta_1^{(1)}, \mathfrak{p}(\varphi - \varphi_1)].$$

De cette équation nous tirons

$$\mathfrak{p}(\varphi - \varphi_1) \equiv \mathfrak{p}\theta C + (\mathfrak{p}\varphi + \theta\theta^{(1)}) D \qquad (\mathrm{mod}\,\mathfrak{p}^2)$$

et par conséquent $D\theta\theta^{(1)}$ doit être divisible par $\mathfrak{p}$, de sorte que $D = D_1\mathfrak{p}$. Nous pouvons donc écrire la congruence

$$\varphi - \varphi_1 \equiv \theta(C + D_1\theta^{(1)}) \qquad (\mathrm{mod}\,\mathfrak{p}).$$

Puisque le degré de 0 en x est plus grand que le degré de φ ou de φ_1, nous devons avoir

$$C + D_1\theta^{(1)} \equiv 0 \qquad (\mathrm{mod}\,\mathfrak{p}),$$

et, par conséquent,

$$\varphi - \varphi_1 \equiv 0 \qquad (\mathrm{mod}\,\mathfrak{p})$$

ou

$$\varphi = \varphi_1 \ldots (i\nu)$$

Nous pouvons donc regarder $(\mathfrak{p}^2, \mathfrak{p}\theta, \mathfrak{p}\varphi + \theta\theta^{(1)})$ *comme une forme canonique de la représentation unique du système modulaire* (I).

Dans le système

$$(\mathrm{I}) \qquad \left\{ \mathfrak{p}^2, \mathfrak{p} \sum_{\mu=1}^{\mu=m} [g_\mu(x)], \sum_{\nu=1}^{\nu=n} [f_\nu(x)] \right\}$$

nous avons supposé la présence des éléments

$$\mathfrak{p} \sum_{\mu=1}^{\mu=m} [g_\mu(x)].$$

On voit toutefois que, sans employer ces éléments, nous avons introduit, à l'aide des éléments $f_1(x), f_2(x), \ldots, f_n(x)$, les éléments

$$\mathfrak{p} \prod_{\nu=1}^{\nu=n} \Pi_\nu(x)$$

dans le système (I') de la page 86, où

$$\Pi_\nu(x) = \pi_\nu(x) + \overline{\pi}(x) F_\nu(x) \qquad (\nu = 1, 2, \ldots, n).$$

Dès lors, à moins que les n quantités ne soient congrues à o $[\mathrm{mod}\mathfrak{p}, F(x)]$, et même lorsque les éléments $\mathfrak{p} \prod_{\mu=1}^{\mu=m} [g_\mu(x)]$ manquent dans le système initial, le système modulaire réduit est

$$(A) \qquad [\mathfrak{p}^2, \mathfrak{p} G(x), F(x)].$$

D'autre part, lorsque les éléments $\mathfrak{p} \prod_{\mu=1}^{\mu=m} [G_\mu(x)]$ manquent dans le système initial et si l'on a aussi

$$\Pi_\nu(x) \equiv o \quad [\mathrm{mod}\mathfrak{p}, F(x)] \qquad (\nu = 1, 2, \ldots, n),$$

le système réduit est de la forme

$$(B) \qquad [\mathfrak{p}^2, F(x)].$$

Considérons le système

$$(A) \qquad [\mathfrak{p}^2, \mathfrak{p} G(x), F(x)],$$

et supposons que $F(x)$ admette les deux facteurs $F_1(x)$, $F_2(x)$ relativement aux modules $\mathfrak{p}^2$, $\mathfrak{p}G(x)$, c'est-à-dire que l'on a

$$(1) \qquad F(x) = F_1(x) F_2(x) + \mathfrak{p} G(x) \psi(x) + \mathfrak{p}^2 \chi(x),$$

où $\psi(x)$ et $\chi(x)$ sont des fonctions de $[\nu, x]$.

De plus, supposons que $F_1(x)$ et $F_2(x)$ n'aient pas de facteur commun relativement aux modules $\mathfrak{p}^2$, $\mathfrak{p}G(x)$, et formons le produit

$$(M) \quad [\mathfrak{p}^2, \mathfrak{p}G(x), F_1(x)]\,[\mathfrak{p}^2, \mathfrak{p}G(x), F_2(x)]$$
$$\equiv \left[\begin{array}{ccc} \mathfrak{p}^4, & \mathfrak{p}^3 G(x), & \mathfrak{p}^2 F_2(x), \\ & \mathfrak{p}^2 F_1(x), & \end{array} \begin{array}{cc} \mathfrak{p}^2 G(x)^2, & \mathfrak{p} G(x) F_2(x), \\ \mathfrak{p} G(x) F_1(x), & F_1(x) F_2(x) \end{array}\right].$$

Les quatre éléments $\mathfrak{p}^4$, $\mathfrak{p}^3 G(x)$, $\mathfrak{p}^2 F_2(x)$, $\mathfrak{p}^2 F_1(x)$ peuvent être pris dans le système

$$\mathfrak{p}^2[\mathfrak{p}^2, \mathfrak{p}G(x), F_1(x), F_2(x)] \backsim \mathfrak{p}^2(v) \backsim \mathfrak{p}^2,$$

de sorte que le produit (M) est équivalent à

$$(N) \qquad [\mathfrak{p}^2, \mathfrak{p}G(x)F_1(x), \mathfrak{p}G(x)F_2(x), F_1(x)F_2(x)].$$

Maintenant si $F_1(x)$ et $F_2(x)$ n'ont pas de facteur commun (mod $\mathfrak{p}$), le système (N) se réduit à

$$[\mathfrak{p}^2, \mathfrak{p}G(x), F(x)].$$

Dès lors, afin de mettre le système (A) sous la forme d'un produit des deux systèmes donnés plus haut, la fonction $F(x)$ doit avoir la forme (1) et les fonctions $F_1(x)$ et $F_2(x)$ doivent n'avoir aucun facteur commun (mod $\mathfrak{p}$).

Dans le système

$$[\mathfrak{p}^2, \mathfrak{p}g(x), f(x)]$$

supposons *d'abord* que $f(x)$ est irréductible (mod $\mathfrak{p}$). Nous avons alors la congruence

$$\begin{aligned}[\mathfrak{p}^2, \mathfrak{p}g(x), f(x)] &\backsim [\mathfrak{p}^2, \mathfrak{p}g(x), \mathfrak{p}f(x), f(x)] \\ &\backsim \{\mathfrak{p}[\mathfrak{p}, g(x), f(x)], f(x)\} \backsim [\mathfrak{p}, f(x)],\end{aligned}$$

à moins que $g(x)$ ne soit un multiple de $f(x)$ (mod $\mathfrak{p}$); si $G(x)$ (mod $\mathfrak{p}$) est un multiple de $f(x)$, on a

$$[\mathfrak{p}^2, \mathfrak{p}g(x), f(x) \backsim [\mathfrak{p}^2, f(x)]$$

et le système est de la forme (B).

Dans le système $[\mathfrak{p}^2, \mathfrak{p}g(x), f(x)^2]$ supposons que $f(x)$ soit une fonction irréductible (mod $\mathfrak{p}$). Nous avons alors

$$\{\mathfrak{p}[\mathfrak{p}, g(x), f(x)^2], f(x)^2\} \backsim [\mathfrak{p}, f(x)^2],$$

à moins que $g(x)$ ne soit un multiple de $f(x)$.

Si ce multiple est plus grand que 1, on a

$$[\mathfrak{p}^2, \mathfrak{p}g(x), f(x)^2] \backsim [\mathfrak{p}^2, f(x)^2];$$

et si ce multiple est égal à 1, on a

$$[\mathfrak{p}^2, \mathfrak{p}g(x), f(x)^2] \backsim [\mathfrak{p}^2, \mathfrak{p}f(x), f(x)^2].$$

Supposons maintenant que $f(x) \equiv f_1(x) f_2(x) \pmod{\mathfrak{p}}$ et, de plus, supposons $f_1(x)$ et $f_2(x)$ irréductibles $(\mathrm{mod}\ \mathfrak{p})$, on a

$$[\mathfrak{p}^2, \mathfrak{p}g(x), f(x)] \backsim [\mathfrak{p}, f(x)],$$

lorsque $f(x)$ et $g(x)$ n'ont pas de facteur commun $(\mathrm{mod}\ \mathfrak{p})$, et

$$[\mathfrak{p}^2, \mathfrak{p}g(x), f(x)] \backsim [\mathfrak{p}^2, \mathfrak{p}f_1(x), f(x)]$$

lorsque g est divisible par $f_1(\mathrm{mod}\ \mathfrak{p})$, mais non par $f_2(\mathrm{mod}\ \mathfrak{p})$.

En mettant le système $[\mathfrak{p}^2, \mathfrak{p}G(x), F(x)]$ sous la forme canonique

$$(A) \qquad [\mathfrak{p}^2, \mathfrak{p}\theta(x), \mathfrak{p}\varphi(x) + \theta(x)\theta^{(1)}(x)],$$

on voit que ce système *contient* le système

$$[\mathfrak{p}, d(x)],$$

où $d(x)$ est un diviseur quelconque $(\mathrm{mod}\ \mathfrak{p})$ du produit $\theta(x)\theta^{(1)}(x)$.

De plus, le système (B) peut s'écrire

$$(B) \qquad [\mathfrak{p}^2, \mathfrak{p}H(x) + k(x)],$$

et, par conséquent, il contient le système

$$[\mathfrak{p}, \delta(x)],$$

où $\delta(x)$ est un diviseur $(\mathrm{mod}\ \mathfrak{p})$ de $k(x)$.

Les systèmes (A) et (B) ne sont donc pas des systèmes *premiers* (*cf.* KRONECKER, *Grundzüge*, p. 83, ou *Werke*, t. II, p. 341).

Réduction des systèmes modulaires dans lesquels la troisième puissance de l'idéal premier $\mathfrak{p}$ entre comme élément.

Ces systèmes sont de la forme

$$(I) \qquad \left\{\mathfrak{p}^3, \mathfrak{p}^2 \prod_{\nu=1}^{\nu=n} [g_\nu(x)], \mathfrak{p} \prod_{\mu=1}^{\mu=m} [f_\mu(x)], \prod_{\lambda=1}^{\lambda=l} [h_\lambda(x)]\right\},$$

où tous les éléments qui y entrent sont des quantités du domaine $[o, x]$.

Nous pouvons adjoindre à ce système les éléments

$$\mathfrak{p}^2 \prod^{\mu=m} [f_\mu(x)] \quad \text{et} \quad \mathfrak{p} \prod^{\lambda=l} [h_\lambda(x)],$$

et, à l'aide de ces éléments et de l'élément p^3, nous construisons le système

$$\left\{\mathfrak{p}^3,\ p^2\prod_{\mu=1}^{\mu=m}[f_\mu(x)],\ p\prod_{\lambda=1}^{\lambda=l}[h_\lambda(x)]\right\}\backsim\mathfrak{p}\left\{\mathfrak{p}^2,\ \mathfrak{p}\prod_{\mu=1}^{\mu=m}[f_\mu(x)],\ \prod_{\lambda=1}^{\lambda=l}[h_\lambda(x)]\right\}.$$

Nous déduisons du système modulaire auxiliaire

$$(\mathrm{A})\qquad\left\{\mathfrak{p}^2,\ \mathfrak{p}\prod_{\mu=1}^{\mu=m}[f_\mu(x)],\quad\prod_{\lambda=1}^{\lambda=l}[h_\lambda(x)]\right\}\backsim[\mathfrak{p}^2,\ \mathfrak{p}\overline{\mathrm{F}}(x),\ \overline{\mathrm{H}}(x)],$$

d'une part

$$(1)\qquad\overline{\mathrm{H}}(x)=\mathfrak{p}^2\overline{\pi}(x)+\mathfrak{p}\sum_{\mu=1}^{\mu=m}f_\mu\overline{f}_\mu+\sum_{\lambda=1}^{\lambda=l}h_\lambda\overline{h}_\lambda,$$

où nous employons le signe fonctionnel pour la fonction de x; et d'autre part

$$(2)\qquad h_\lambda(x)=\mathfrak{p}^2\pi_\lambda+\mathfrak{p}\overline{\mathrm{F}}\mathrm{F}_\lambda+\overline{\mathrm{H}}\mathrm{H}_\lambda\qquad(\lambda=1,2,\ldots,l).$$

En posant $\mathrm{H}(x)=\overline{\mathrm{H}}(x)-\mathfrak{p}^2\overline{\pi}$, on voit que de (1) on tire

$$\mathrm{H}(x)=\mathfrak{p}\sum_{\mu=1}^{\mu=m}f_\mu\overline{f}_\mu+\sum_{\lambda=1}^{\lambda=l}h_\lambda\overline{h}_\lambda,$$

et, par conséquent, $\mathrm{H}(x)$ peut être ajouté au système (I) sans qu'il cesse d'être équivalent à lui-même.

Nous avons, de plus, en vertu de (2),

$$h_\lambda(x)=\mathfrak{p}^2\pi_\lambda+\mathfrak{p}\overline{\mathrm{F}}\mathrm{F}_\lambda+\mathrm{H}\mathrm{H}_\lambda+\mathfrak{p}^2\overline{\pi}\mathrm{H}_\lambda\qquad(\lambda=1,2,\ldots,l),$$

ou

$$h_\lambda(x)=\mathfrak{p}^2\mathrm{II}_\lambda+\mathfrak{p}\mathrm{F}\mathrm{F}_\lambda+\mathrm{H}\mathrm{H}_\lambda\qquad(\lambda=1,2,\ldots,l),$$

où, pour abréger, II_λ est mis pour $\pi_\lambda+\overline{\pi}\mathrm{H}_\lambda$ $(\lambda=1,2,\ldots,l)$.

Nous pouvons donc écrire le système (I) sous la forme

$$\left\{\mathfrak{p}^3,\ \mathfrak{p}^2 \sum_{\nu=1}^{\nu=n} [g_\mu(x)],\ \mathfrak{p} \sum_{\mu=1}^{\mu=m} [f_\mu(x),\ \sum_{\lambda=1}^{\lambda=l} [\mathfrak{p}^2 \Pi_\lambda(x) + \mathfrak{p} F F_\lambda],\ H(x)\right\}$$

$$\backsim \left\{\mathfrak{p}\left\{\mathfrak{p}^2,\ \mathfrak{p} \sum_{\nu=1}^{\nu=n} [g_\nu(x)],\ \sum_{\mu=1}^{\mu=m} [f_\mu(x)],\ \sum_{\lambda=1}^{\lambda=l} [\mathfrak{p}\Pi_\lambda(x) + F F_\lambda]\right\},\ H(x)\right\}$$

$$\backsim \{\mathfrak{p}[\mathfrak{p}^2,\ \mathfrak{p}G(x),\ F(x)],\ H(x)\}.$$

Nous voyons donc que le système (I) est équivalent au système

$$(II) \qquad [\mathfrak{p}^3,\ \mathfrak{p}^2 G(x),\ \mathfrak{p}F(x),\ H(x)].$$

Nous formerons le système modulaire auxiliaire

$$(b) \qquad [\mathfrak{p}^2\ \mathfrak{p}G(x),\ F(x),\ H(x)] \backsim [\mathfrak{p}^2,\ \mathfrak{p}\theta(x),\ \mathfrak{p}\varphi(x) + \theta(x)\theta^{(1)}(x)],$$

où les éléments $\theta(x)$, $\varphi(x)$ et $\theta'(x)$ satisfont aux conditions des pages 88 et 89.

De (b) nous dirons

$$\mathfrak{p}\theta(x) = \mathfrak{p}^2 \Pi + \mathfrak{p} G G^{(1)} + \mathfrak{p} F F^{(1)} + H H^{(1)}$$

ou

$$\mathfrak{p}^2\theta(x) = \mathfrak{p}^3 \Pi + \mathfrak{p}^2 G G^{(1)} + \mathfrak{p}^2 F F^{(1)} + \mathfrak{p} H H^{(1)};$$

et, par suite,

$$\mathfrak{p}^2\theta(x) \equiv o[\mathfrak{p}^3,\ \mathfrak{p}^2 G,\ \mathfrak{p}F,\ H].$$

Nous pouvons donc adjoindre $\mathfrak{p}^2\theta$ au système (II), et, par une méthode analogue, on voit que l'élément $\mathfrak{p}^2\varphi + \mathfrak{p}\theta\theta^{(1)}$ peut aussi être adjoint à ce système.

Ceci fait, on voit que les éléments $\mathfrak{p}^2 G$ et $\mathfrak{p}F$, à cause de l'équivalence (b), peuvent être supprimés du système (II).

Finalement, si nous donnons à $H(x)$ la valeur tirée de (b)

$$H(x) = \mathfrak{p}^2\psi + \mathfrak{p}\theta\theta^{(2)} + (\mathfrak{p}\varphi + \theta\theta^{(1)})\varphi^{(1)},$$

on voit que nous pouvons écrire (II) sous la forme

$$(II') \qquad [\mathfrak{p}^3,\ \mathfrak{p}^2\theta,\ \mathfrak{p}^2\varphi + \mathfrak{p}\theta\theta^{(1)},\ \mathfrak{p}^2\psi + \mathfrak{p}\theta\theta^{(2)} + \mathfrak{p}\varphi\varphi^{(1)} + \theta\theta^{(1)}\varphi^{(1)}].$$

Grâce à la présence de $\mathfrak{p}^3$, $\mathfrak{p}^2\theta$, $\mathfrak{p}^2\varphi + \mathfrak{p}\theta\theta^{(1)}$, nous pouvons supposer

que le coefficient initial de $\varphi^{(1)}$ est l'unité, et nous pouvons supposer :

1° Que les coefficients initiaux de θ, $\theta^{(1)}$ et $\varphi^{(1)}$ sont l'unité;

2° Que les degrés en x de φ et ψ sont inférieurs au degré de θ;

3° Que $\theta^{(2)}$ est de degré inférieur au degré de $\theta^{(1)}$;

4° Que les coefficients de toutes les fonctions qui entrent comme éléments dans le système sont pris parmi les entiers déterminés ρ_1, ρ_2, ..., ρ_k.

On peut prouver par une méthode tout à fait analogue à celle donnée dans le *Journal de Crelle*, t. 119, p. 161, que le système (II′) est *une forme canonique de la représentation unique du système* (I).

En général, les formes canoniques des systèmes modulaires de Kronecker de seconde espèce, où la première, ou une plus haute puissance de l'idéal premier $\mathfrak{p}$ entre comme élément, peuvent s'écrire (voir le *Journal de Crelle*, t. 119, p. 164) :

$$(\mathfrak{p}, \theta),$$
$$(\mathfrak{p}^2, \mathfrak{p}\theta, \mathfrak{p}\varphi + \theta\theta^{(1)}),$$
$$(\mathfrak{p}^3, \mathfrak{p}^2\theta, \mathfrak{p}^2\varphi + \mathfrak{p}\theta\theta^{(1)}, \mathfrak{p}^2\psi + \mathfrak{p}\theta\theta^{(2)} + \mathfrak{p}\varphi\varphi^{(1)} + \theta\theta^{(1)}\varphi^{(1)}),$$
$$\left(\begin{array}{l}\mathfrak{p}^4, \mathfrak{p}^3\theta, \mathfrak{p}^3\varphi + \mathfrak{p}^2\theta\theta^{(1)}, \mathfrak{p}^3\psi + \mathfrak{p}^2\theta\theta^{(2)} + \mathfrak{p}^2\varphi\varphi^{(1)} + \mathfrak{p}\theta\theta^{(1)}\varphi^{(1)}, \\ \mathfrak{p}^3\chi + \mathfrak{p}^2\theta\theta^{(3)} + \mathfrak{p}^2\varphi\varphi^{(2)} + \mathfrak{p}^2\psi\psi^{(1)} + \mathfrak{p}\theta\theta^{(1)}\varphi^{(2)} + \mathfrak{p}\theta\theta^{(2)}\psi^{(1)} + \mathfrak{p}\varphi\varphi^{(1)}\psi^{(1)} + \theta\theta^{(1)}\varphi^{(1)}\psi^{(1)}\end{array}\right),$$
.....

Posons

$$\mathbf{M}_1 = \theta,$$
$$\mathbf{M}_2 = \mathfrak{p}\varphi + \theta\theta^{(1)},$$
$$\mathbf{M}_3 = \mathfrak{p}^2\psi + \mathfrak{p}\theta\theta^{(2)} + \mathfrak{p}\varphi\varphi^{(1)} + \theta\theta^{(1)}\varphi^{(1)},$$
$$\mathbf{M}_4 = \mathfrak{p}^3\chi + \mathfrak{p}^2\theta\theta^{(3)} + \mathfrak{p}^2\varphi\varphi^{(2)} + \mathfrak{p}^2\psi\psi^{(1)} + \mathfrak{p}\theta\theta^{(1)}\varphi^{(2)} + \mathfrak{p}\theta\theta^{(2)}\psi^{(1)} + \mathfrak{p}\varphi\varphi^{(1)}\psi^{(1)} + \theta\theta^{(1)}\varphi^{(1)}\psi^{(1)},$$
.....,

de sorte que

$$\mathbf{M}_1 = \theta,$$
$$\mathbf{M}_2 = \mathfrak{p}\varphi + \mathbf{M}_1\theta^{(1)},$$
$$\mathbf{M}_3 = \mathfrak{p}^2\psi + \mathfrak{p}\mathbf{M}_1\theta^{(2)} + \mathbf{M}_2\varphi^{(1)},$$
$$\mathbf{M}_4 = \mathfrak{p}^3\chi + \mathfrak{p}^2\mathbf{M}_1\theta^{(3)} + \mathfrak{p}\mathbf{M}_2\varphi^{(2)} + \mathbf{M}^3\psi^{(1)},$$
$$\mathbf{M}_5 = \mathfrak{p}^4\sigma + \mathfrak{p}^3\mathbf{M}_1\theta^{(4)} + \mathfrak{p}^2\mathbf{M}_2\varphi^{(3)} + \mathfrak{p}\mathbf{M}_3\psi^{(2)} + \mathbf{M}_4\chi^{(1)},$$
$$\mathbf{M}_6 = \mathfrak{p}^5\tau + \mathfrak{p}^4\mathbf{M}_1\theta^{(5)} + \mathfrak{p}^3\mathbf{M}_2\varphi^{(4)} + \mathfrak{p}^2\mathbf{M}_3\psi^{(3)} + \mathfrak{p}\mathbf{M}_4\chi^{(2)} + \mathbf{M}_5\sigma^{(1)},$$
.....

Nous pouvons donc écrire les formules canoniques

$$
\begin{aligned}
&(\mathfrak{p}_1, \mathrm{M}_1),\\
&(\mathfrak{p}_2, \mathfrak{p}\mathrm{M}_1, \mathrm{M}_2),\\
&(\mathfrak{p}^3, \mathfrak{p}^2\mathrm{M}_1, \mathfrak{p}\mathrm{M}_2, \mathrm{M}_3),\\
&(\mathfrak{p}^4, \mathfrak{p}^3\mathrm{M}_1, \mathfrak{p}^2\mathrm{M}_2, \mathfrak{p}^2\mathrm{M}_3, \mathrm{M}_4),\\
&(\mathfrak{p}^5, \mathfrak{p}^4\mathrm{M}_1, \mathfrak{p}^3\mathrm{M}_2, \mathfrak{p}^2\mathrm{M}_3, \mathfrak{p}\mathrm{M}_4, \mathrm{M}_5),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,
\end{aligned}
$$

où M_5 est exprimé linéairement en fonction de M_4, M_3, M_2, M_1 par la formule donnée ci-dessus, etc.

Réduction des systèmes modulaires de troisième espèce.

Considérons d'abord le système de la forme

$$
\text{(I)} \qquad [\mu_1, \mu_2, \ldots, \mu_k, g_1(x), g_2(x), \ldots, g_m(x), f_1(x,y), f_2(x,y), \ldots, f_n(x,y)],
$$

où $\mu_1, \mu_2, \ldots, \mu_k$ sont des entiers algébriques de Ω; $g_1(x)$, $g_2(x)$ .... $g_m(x)$ sont des fonctions entières en x dont les coefficients sont des entiers algébriques de Ω, et $f_1(x,y)$, $f_2(x,y)$, ..., $f_n(x,y)$ sont des fonctions entières en x et y dont les coefficients sont des entiers algébriques de Ω. Nous pouvons donc dire, pour abréger, que tous les éléments du système modulaire sont des quantités appartenant au domaine d'intégrité $[\rho, x, y]$, et, en employant la notation que nous avons adoptée précédemment, nous pouvons écrire le système ci-dessus

$$
\text{(I)} \qquad \left\{ \sum_{\lambda=1}^{\lambda=k} (\mu_\lambda), \sum_{\pi=1}^{\pi=m} [g_\pi(x)], \sum_{\nu=1}^{\nu=n} [f_\nu(x,y)] \right\}.
$$

Des résultats obtenus dans la réduction des systèmes de première espèce, il résulte que ce système peut être remplacé sans qu'il cesse de rester équivalent à lui-même par le système

$$
\text{(A)} \qquad \left\{ \mu, \sum_{\pi=1}^{\pi=m} [g_\pi(x)], \sum_{\nu=1}^{\nu=n} [f_\nu(x,y)] \right\},
$$

où l'idéal μ est le plus grand commun diviseur des éléments μ_1, μ_2, ..., μ_k.

En procédant comme nous l'avons fait pour la réduction des systèmes de la seconde espèce, on peut montrer que, si un entier algébrique entre comme facteur dans l'un des éléments $g_1(x)$, $g_2(x)$, ..., $g_m(x)$; $f_1(x,y)$, $f_2(x,y)$, ..., $f_n(x,y)$, cet élément peut, sans que le système modulaire cesse d'être équivalent à lui-même, être remplacé par un élément dans lequel le facteur est un diviseur de μ.

Nous avons vu, de plus, dans la réduction des systèmes modulaires de seconde espèce, que nous pouvions remplacer le système (A) par un produit de systèmes de la forme

$$\left\{\mathfrak{p}^a, \sum_{\pi=1}^{\pi=m}[g_\pi(x)], \sum_{\nu=1}^{\nu=n}[f_\nu(x,y)]\right\}, \tag{II}$$

où a est un entier rationnel positif.

En prenant les différentes puissances de $\mathfrak{p}$, nous en avons déduit la forme canonique de la représentation unique du système modulaire correspondant.

En particulier, lorsque $a = 1$, on a vu que le système (II) était équivalent au système

$$\left\{\mathfrak{p}, \overline{g}(x), \sum_{\nu=1}^{\nu=n}[f_\nu(x,y)]\right\}, \tag{B}$$

où $\overline{g}(x)$ est le plus grand commun diviseur (mod $\mathfrak{p}$) des éléments $g_1(x)$, $g_2(x)$, ..., $g_m(x)$.

Supposons que l'un des éléments $f_1(x,y)$, $f_2(x,y)$, ..., $f_n(x,y)$ par exemple $f_1(x,y)$, admette comme facteur $h_1(x)$ (mod $\mathfrak{p}$), de sorte que

$$f_1(x,y) = h_1(x)\overline{f}_1(x,y) + \mathfrak{p}\varphi(x,y),$$

où $\varphi(x,y)$ est une quantité appartenant au domaine $[\rho, x, y]$, et considérons le système

$$[\mathfrak{p}, \overline{g}(x), h_1(x)\overline{f}_1(x,y)]. \tag{a}$$

De plus, soit $d(x)$ le plus grand commun diviseur (mod $\mathfrak{p}$) de $\overline{g}(x)$ et de $\overline{h}_1(x)$.

Nous pouvons écrire (a) sous la forme

$$[\mathfrak{p}, \overline{g}(x), \overline{g}(x)\overline{f_1}(x,y), h_1(x)\overline{f_1}(x,y)]$$
$$\backsim [\mathfrak{p}, \overline{g}(x), \overline{g}(x)\overline{f_1}(x,y), h_1(x)\overline{f_1}(x,y), d(x)\overline{f_1}(x,y)]$$
$$= [\mathfrak{p}, \overline{g}(x), d(x)\overline{f_1}(x,y)].$$

Dès lors il est évident que tous ceux des éléments $f_1(x,y)$, $f_2(x,y)$, ..., $f_n(x,y)$ qui admettent comme facteur commun $(\mathrm{mod}\mathfrak{p})$ une fonction de x seul peuvent être remplacés dans le système (B) par des éléments dans lesquels de telles fonctions de x sont des diviseurs $(\mathrm{mod}\mathfrak{p})$ de l'élément $\overline{g}(x)$.

De plus, si

$$\overline{g}(x) \equiv \overline{g_1}(x)\overline{g_2}(x) \qquad (\mathrm{mod}\mathfrak{p}),$$

et si $\overline{g_1}(x)$, $\overline{g_2}(x)$ n'ont pas de facteur commun $(\mathrm{mod}\mathfrak{p})$, le système que nous venons d'écrire peut être remplacé par le produit des systèmes

$$\left\{\mathfrak{p}, \overline{g_1}(x), \prod_{\nu=1}^{\nu=n} [f_\nu(x,y)]\right\}, \qquad \left\{\mathfrak{p}, \overline{g_2}(x), \prod_{\nu=1}^{\nu=n} [f_\nu(x,y)]\right\}.$$

Nous avons donc à considérer des systèmes de la forme

$$\text{(III)} \qquad \left\{\mathfrak{p}, g(x), \prod_{\nu=1}^{\nu=n} [f_\nu(x,y)]\right\},$$

où $g(x)$ est une fonction irréductible $(\mathrm{mod}\mathfrak{p})$ ou une puissance d'une telle fonction.

Si d'abord $g(x)$ entre à la première puissance dans (III), il résulte de ce que nous avons dit plus haut qu'aucun des éléments $f_1(x,y)$, $f_2(x,y)$, ..., $f_n(x,y)$ n'a un facteur $(\mathrm{mod}\mathfrak{p})$ en x seulement.

L'élément $g(x)$ développé est de la forme

$$g(x) = x^\tau + \gamma_1 x^{\tau-1} + \gamma_2 x^{\tau-2} + \ldots + \gamma_\tau$$

où les entiers $\gamma_1, \gamma_2, \ldots, \gamma_\tau$ sont pris parmi les quantités déterminées $\rho_1, \rho_2, \ldots, \rho_k$; et les fonctions $f(x,y)$ peuvent s'écrire

$$f(x,y) = a_0(x)y^k + a_1(x)y^{k-1} + a_2(x)y^{k-2} + \ldots + a_k(x).$$

où

$$a_0(x) = a_{00}x^{k_0} + a_{01}x^{k_0-1} + a_{02}x^{k_0-2} + \ldots + a_{0k_0},$$
$$a_1(x) = a_{10}x^{k_1} + a_{11}x^{k_1-1} + a_{12}x^{k_1-2} + \ldots + a_{1k_1},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$a_k(x) = a_{k0}x^{k_k} + a_{k1}x^{k_k-1} + a_{k2}x^{k_k-2} + \ldots + a_{kk_k},$$

expressions dans lesquelles toutes les quantités a_{ij} sont des entiers algébriques de Ω et qui, prises relativement au module $\mathfrak{p}$, sont congrues respectivement chacune à chacune aux quantités déterminées ρ_1, ρ_2, ..., ρ_k et peuvent par conséquent être remplacées par ces quantités.

La fonction $a_0(x)$ est, ou divisible (mod$\mathfrak{p}$) par la fonction irréductibles (mod$\mathfrak{p}$) $g(x)$, ou n'a aucun facteur commun avec cette fonction.

Dans le premier cas on peut la supprimer comme n'apportant rien de nouveau au système et nous pouvons opérer de même avec les fonctions $a_1(x)$, $a_2(x)$, ..., jusqu'à ce que nous en trouvions une qui ne soit pas divisible par $g(x)$ (mod$\mathfrak{p}$).

Supposons maintenant que $a_0(x)$ n'a pas de facteur (mod$\mathfrak{p}$) en commun avec $g(x)$. Par une méthode analogue à la méthode ordinaire qui permet de trouver le plus grand commun diviseur de deux fonctions, nous pouvons déterminer deux fonctions $\overline{a_0}(x)$ et $\overline{g}(x)$ appartenant à $[\rho, x]$ et telles que

$$a_0(x)\,\overline{a_0}(x) + g(x)\,\overline{g}(x) = c,$$

où c est un entier algébrique dans Ω qui n'est pas divisible par l'idéal premier $\mathfrak{p}$.

Par conséquent, le plus grand commun diviseur de $\mathfrak{p}$ et $c\rho$ est ρ, de sorte que

$$\mathfrak{p} + c\rho = \rho.$$

Puisque l'unité est divisible par ρ, il existe dans Ω (*voir* DEDEKIND, p. 559) un entier algébrique π divisible par $\mathfrak{p}$ et un entier algébrique c_1 divisible par ρ et tel que

$$\pi + cc_1 = 1,$$

ou

$$cc_1 \equiv 1 \pmod{\mathfrak{p}}.$$

Dès lors on a aussi

$$a_0(x)c_1\overline{a_0}(x) + g(x)c_1\overline{g}(x) \equiv 1 \pmod{\mathfrak{p}}.$$

De là il résulte que si nous multiplions $f(x)$ par $c_1\,\overline{a_0}(x)$ et si nous ajoutons au résultat $g(x)c_1\,\overline{g}_1(x)$ nous aurons une fonction $\overline{\mathrm{F}}\,(x,y)$, par exemple, qui développée prend la forme

$$\overline{\mathrm{F}}(x,y)\equiv y^{\pi}+\overline{\mathrm{A}_1}(x)y^{\pi-1}+\overline{\mathrm{A}_2}(x)y^{\pi-2}+\ldots+\overline{\mathrm{A}_\pi}(x)\qquad(\mathrm{mod}\mathfrak{p}),$$

où $\overline{\mathrm{A}_1}(x)$, $\overline{\mathrm{A}_2}(x)$, ..., $\overline{\mathrm{A}_\pi}(x)$ sont des fonctions entières en x dont les coefficients sont pris parmi les entiers déterminés $\rho_1, \rho_2, \ldots, \rho_k$, et au moyen de la fonction $g(x)$ nous pouvons réduire chacune de ces fonctions de façon que les degrés des fonctions obtenus $\mathrm{A}_1(x)$, $\mathrm{A}_2(x)$, ..., $\mathrm{A}_\pi(x)$ soient tous moindres que τ, τ étant le degré de $g(x)$, fonction dont les coefficients sont pris parmi les entiers déterminés $\rho_1, \rho_2, \ldots, \rho_k$.

Nous pourrons donc écrire

$$\mathrm{F}(x,y)\equiv y^{\pi}+\mathrm{A}_1(x)y^{\pi-1}+\mathrm{A}_1(x)y^{\pi-2}+\ldots+\mathrm{A}_k(x)\qquad[\mathrm{mod}\mathfrak{p},g(x)].$$

Soient $\mathrm{F}_1(x,y)$, $\mathrm{F}_2(x,y)$, ..., $\mathrm{F}_n(x,y)$ les éléments réduits de $f_1(x,y)$, $f_2(x,y)$, ..., $f_n(x,y)$ relativement aux modules $[\mathfrak{p}.\,g(x)]$.

Nous pouvons considérer maintenant au lieu du système (III), le système

$$(\mathrm{III}')\qquad\left\{\mathfrak{p},\,g(x),\,\prod_{\nu=1}^{\nu=n}[\mathrm{F}_\nu(x,y)]\right\}.$$

Supposons ensuite que l'on ait

$$\mathrm{F}_1(x,y)=y^k+\mathrm{A}_1(x)y^{k-1}+\mathrm{A}_2(x)\,y^{k-2}+\ldots+\mathrm{A}_k(x),$$
$$\mathrm{F}_2(x,y)=y^l+\mathrm{B}_1(x)y^{l-1}+\mathrm{B}_2(x)\,y^{l-2}+\ldots+\mathrm{B}_l(x),$$

et $k\geqq l$.

Par une division nous aurons

$$\mathrm{F}_1(x,y)=\mathrm{Q}_1(x,y)\mathrm{F}_2(x,y)+\mathrm{R}_1(x,y)$$

où $\mathrm{Q}_1(x,y)$ et $\mathrm{R}_1(x,y)$ sont des quantités appartenant à $[\varphi,x,y]$.

On voit que le degré de $\mathrm{R}_1(x,y)$ en y est moindre que le degré en y de $\mathrm{F}_1(x,y)$ et de $\mathrm{F}_2(x,y)$; il est clair aussi que $\mathrm{R}_1(x,y)$ peut être adjoint au système (III') et, ceci étant fait, $\mathrm{F}_1(x,y)$ peut en être supprimé sans qu'il cesse d'être équivalent à lui-même.

Soit $\Phi_3(x,y)$ l'élément réduit de $\mathrm{R}_1(x,y)$, et formons l'expression

$$\mathrm{F}_2(x,y)=\mathrm{Q}_2(x,y)\Phi_3(x,y)+\mathrm{R}_2(x,y).$$

Soit $\Phi_4(x,y)$ l'élément réduit de $R_2(x,y)$ que nous supposons avoir été ajouté au système (III') et supposons qu'ensuite on y ait supprimé $F_2(x,y)$.

En continuant ainsi nous avons

$$\Phi_3(x,y) = Q_3(x,y)\Phi_4 \quad (x,y) + R_3(x,y),$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\Phi_i(x,y) = Q_i(x,y)\Phi_{i+1}(x,y) + R_i(x,y).$$

Puisque les degrés des fonctions $R_3, R_4, \ldots$, en y sont continuellement décroissants sans devenir négatifs, nous devons finalement avoir

$$\Phi_{\nu-2}(x,y) = Q_{\nu-2}(x,y)\Phi_{\nu-1}(x,y) + R_{\nu-2}(x,y),$$
$$\Phi_{\nu-1}(x,y) = Q_{\nu-1}(x,y)\Phi_{\nu}(x,y),$$

où $\Phi_\nu(x,y)$ est l'élément réduit $[\mathrm{mod}\mathfrak{p}, g(x)]$ de $R_{\nu-2}(x,y)$.

Nous pouvons ainsi remplacer les deux éléments $F(x,y)$ et $F_2(x,y)$ dans le système modulaire (III') par leur plus grand commun diviseur $[\mathrm{mod}\mathfrak{p}, \varphi(x)]$, l'élément $\Phi_\nu(x,y)$.

Si cette fonction $\Phi_\nu(x,y)$ se trouvait être congrue à o $[\mathrm{mod}\mathfrak{p}, \varphi(x)]$, on voit que les éléments initiaux $F_1(x,y)$ et $F_2(x,y)$ n'ajoutent rien au système; tandis que, si

$$\Phi_\nu(x,y) = k(x),$$

où $k(x)$ est une fonction entière en x seul, nous pouvons, comme plus haut, déterminer une fonction $\overline{k}(x)$ appartenant à $[\nu, x]$, telle que

$$k(x).\overline{k}(x) \equiv 1 \qquad [\mathrm{mod}\mathfrak{p}, g(x)].$$

Le système est donc un *système unité* et est sans intérêt dans la discussion actuelle.

Si nous continuons comme plus haut, on voit que, si le système modulaire considéré au début (III) n'est pas un système unité, nous pouvons remplacer

$$\text{(III)} \qquad \left\{\mathfrak{p}, g(x), \sum_{\nu=1}^{\nu=n} [f_\nu(x,y)]\right\}$$

par le système modulaire équivalent

$$[\mathfrak{p}, g(x), \overline{f}(x,y)],$$

où $\overline{f}(x,y)$ est le plus grand commun diviseur $[\mathrm{mod}\,\mathfrak{p}, g(x)]$ des éléments

$$f_1(x,y), \quad f_i(x,y), \quad \ldots, \quad f_n(x,y).$$

L'élément $\overline{f}(x,y)$, développé suivant les puissances décroissantes de y, est de la forme

$$\overline{f}(x,y) = y^\sigma + b_1(x)y^{\sigma-1} + b_2(x)y^{\sigma-2} + \ldots + b_\sigma(x),$$

où $b_1(x), b_2(x), \ldots, b_\sigma(x)$ ont tous été réduits $[\mathrm{mod}\,\mathfrak{p}, g(x)]$.

Puisque les degrés de $b_1(x), b_2(x), \ldots, b_n(x)$ ne peuvent pas être plus grands que $\tau - 1$, où τ est le degré de $g(x)$, et puisque le coefficient de chaque puissance de x dans ces fonctions peut prendre l'une des k valeurs $\rho_1, \rho_2, \ldots, \rho_k$, on voit que le nombre de fonctions de la forme $\overline{f}(x,y)$ est $(k^\tau)^\sigma = k^{\tau\sigma}$.

Nous pouvons dire que le nombre de fonctions $\nu = k^{\tau\sigma} - 1$, différentes de $\overline{f}(x,y)$, forme un *système complet de résidus incongrus* $[\mathrm{mod}\,\mathfrak{p}, g(x), \overline{f}(x,y)]$.

Ce système de résidus a les trois propriétés caractéristiques suivantes :

1° Ces résidus sont des quantités de $[\rho, x, y]$;

2° Chacun d'eux est incongru des autres $[\mathrm{mod}\,\mathfrak{p}, g(x), \overline{f}(x,y)]$;

3° Toute fonction appartenant au domaine d'intégrité $[\rho, x, y]$ est congru à un et à un seul des représentatifs du système

$$[\mathrm{mod}\,\mathfrak{p}, g(x), \overline{f}(x,y)].$$

Si maintenant $\varpi(x,y)$ est une fonction quelconque appartenant au domaine $[\rho, x, y]$, nous avons le *théorème de Fermat :*

$$(\mathrm{A}) \qquad [\varpi(x,y)]^{k^{\tau\sigma}} \equiv \varpi(x,y) \qquad [\mathrm{mod}\,\mathfrak{p}, g(x), \overline{f}(x,y)].$$

Considérons maintenant le système modulaire

$$[\mathfrak{p}, g(x), \overline{f}(x,y)]$$

et supposons que l'on ait

$$\overline{f}(x,y) \equiv \overline{f}_1(x,y).\overline{f}_2(x,y) \qquad [\mathrm{mod}\,\mathfrak{p}, g(x)],$$

et que $\overline{f_1}(x,y)$ et $\overline{f_2}(x,y)$ n'aient pas de facteur commun

$$[\mathrm{mod}\mathfrak{p}, g(x)].$$

Nous pouvons facilement démontrer que

$$[\mathfrak{p}, g(x), \overline{f}(x,y)] \backsim [\mathfrak{p}, g(x), \overline{f_1}(x,y)]\,[\mathfrak{p}, g(x), \overline{f_2}(x,y)].$$

Nous pouvons donc considérer le système

$$[\mathfrak{p}, g(x), f(x,y)], \tag{IV}$$

où $f(x,y)$ est une fonction irréductible $[\mathrm{mod}\mathfrak{p}, g(x)]$.

Le système (IV) est un système modulaire premier (*voir* p. 55).

Supposons que, développé, $f(x,y)$ soit de la forme

$$f(x,y) = y^\lambda + c_1(x)\,y^{\lambda-1} + c_2(x)^{\lambda-2} + \ldots + c_\lambda(x),$$

de sorte qu'il y a

$$(k)^{\lambda\tau} - 1 = m$$

résidus incongrus relativement au système (IV). Désignons alors ces m résidus par $r_1, r_2, \ldots, r_m$.

Alors, comme à la page 71, on peut démontrer que *si r est l'un des résidus ci-dessus et si*

$$\mathrm{G}(r) = \mathrm{A}_0 r^m + \mathrm{A}_1 r^{m-1} + \ldots + \mathrm{A}_m \equiv 0\,[\mathrm{mod}\mathfrak{p}, g(x), f(x,y)]$$

où $\mathrm{A}_0, \mathrm{A}_1, \ldots, \mathrm{A}_m$ sont des fonctions du domaine $[\rho, x, y]$, et

$$\mathrm{A}_0 \equiv 0\,[\mathrm{mod}\mathfrak{p}, g(x), f(x,y)];$$

cette congruence ne peut avoir plus de m racines incongrues

$$[\mathrm{mod}\mathfrak{p}, g(x), f(x,y)];$$

et si

$$\mathrm{G}(r) \equiv 0\,[\mathrm{mod}\mathfrak{p}, g(x), f(x,y)]$$

a exactement m racines incongrues $r_1, r_2, \ldots, r_m$, *par exemple, nous avons la congruence identique*

$$\mathrm{G}(r) \equiv \mathrm{A}_0 \prod_{i=1}^{i=m} (r - r_i)\,[\mathrm{mod}\mathfrak{p}, g(x), f(x,y)].$$

Dès lors, puisque

$$r^m - 1 \equiv 0 \qquad [\mathrm{mod}\,\mathfrak{p}, g(x), f(x,y)]$$

a les m racines incongrues $[\mathrm{mod}\,\mathfrak{p}, g(x), f(x,y)]$, $r_1, r_2, \ldots, r_m$, on voit que

$$r^m - 1 \equiv \Pi\{r - [\gamma_1(x)\,y^{\lambda-1} + \gamma_2(x)\,y^{\lambda-2} + \ldots + \gamma_\lambda(x)]\} \quad [\mathrm{mod}\,\mathfrak{p}, g(x), f(x,y)],$$

le produit devant s'étendre à $m = k^{\lambda\tau} - 1$ résidus du système

$$[\mathfrak{p}, g(x), f(x,y)],$$

chacun d'eux étant de la forme

$$\gamma_1(x)\,y^{\lambda-1} + \gamma_2\,y^{\lambda-2} + \ldots + \gamma_\lambda(x),$$

où $\gamma_1(x), \gamma_2(x), \ldots, \gamma_\lambda(x)$ sont des fonctions entières en x de degré au plus égal à $\tau - 1$, dont les coefficients sont pris parmi les entiers $\rho_1, \rho_2, \ldots, \rho_k$.

En particulier, si nous égalons les coefficients des puissances égales de x de chacun des membres de la congruence identique, nous avons le *théorème de Wilson* pour le système modulaire $[\mathfrak{p}, g(x), f(x,y)]$, savoir

$$-1 \equiv \Pi[\gamma_1(x)\,y^{\lambda-1} + \gamma_2(x)\,y^{\lambda-2} + \ldots + \gamma_\lambda(x)] \qquad [\mathrm{mod}\,\mathfrak{p}, g(x), f(x,y)],$$

où le produit est étendu comme plus haut.

Fonctions premières primaires qui sont liées à la considération du système modulaire premier $[\mathfrak{p}, g(x), f(x,y)]$.

Puisque $k = p^f$, il s'ensuit que le nombre des résidus incongrus relativement au système modulaire $[\mathfrak{p}, g(x), f(x,y)]$ est $m = p^{\lambda\tau f} - 1$ et que [*voir* la formule (A), p. 104] toute fonction $\psi(x,y)$ appartenant au domaine d'intégrité $[o, x, y]$ satisfait à la congruence

$$[\psi(x,y)]^{p^{\lambda\tau f}} \equiv \psi(x,y) \qquad [\mathrm{mod}\,\mathfrak{p}, g(x), f(x,y)].$$

Si h est la *hauteur* de la fonction $\psi(x,y)$ relativement au système modulaire $[\mathfrak{p}, g(x), f(x,y)]$, on a

$$[\psi(x,y)]^{p^h} \equiv \psi(x,y) \qquad [\mathrm{mod}\,\mathfrak{p}, g(x), f(x,y)],$$

et chacune des h fonctions constituant la période de la fonction $\psi(x,y)$ relativement au système modulaire $[\mathfrak{p}, g(x), f(x,y)]$

$$[\psi(x,y)]^{p^0},\quad [\psi(x,y)]^{p^1},\quad [\psi(x,y)]^{p^2},\quad \ldots,\quad [\psi(x,y)]^{p^{h-1}}$$

est de hauteur h.

De plus, si s est un entier positif tel que l'on ait

$$\psi(x,y)^{p^s} \equiv \psi(x,y) \qquad [\mathrm{mod}\,\mathfrak{p}, g(x), f(x,y)],$$

s est un multiple de h; et aussi h est un diviseur de $\lambda\tau f$, où f est le degré de l'idéal premier $\mathfrak{p}$, τ est le degré de $g(x)$ en x et λ est le degré de $f(x,y)$ en y.

Si une fonction $\varpi(x,y)$ *appartenant au domaine* $[v,y,z]$ *a une hauteur* $h = \lambda\tau$ *prise relativement au système modulaire* $[\mathfrak{p}, g(x), f(x,y)]$, $\varpi(x,y)$ *est congru* $[\mathrm{mod}\,\mathfrak{p}, g(x), f(x,y)]$ *à une fonction entière en* x, y *dont le degré est inférieur ou égal à* $\tau - 1$ *en* x *et à* $\lambda - 1$ *en* y *et dont les coefficients sont des entiers rationnels qui peuvent être considérés comme réduits* $(\mathrm{mod}\,p)$, p *étant l'entier premier qui est divisible par l'idéal premier* $\mathfrak{p}$, *et* vice versa *toute fonction qui est congrue*

$$[\mathrm{mod}\,\mathfrak{p}, g(x), f(x,y)]$$

à une fonction dont le degré est inférieur ou égal à $\tau - 1$ *en* x *et à* $\lambda - 1$ *en* y *à coefficients rationnels réduits* $(\mathrm{mod}\,p)$, *est de hauteur* $h = \lambda\tau$.

De là il résulte que si $\varpi(x, y)$ est de hauteur h, toute fonction symétrique entière des h fonctions

$$[\varpi(x,y)]^{p^0}, [\varpi(x,y)]^{p^1}, [\varpi(x,y)]^{p^2}, \ldots, [\varpi(x,y)]^{p^{h-1}}$$

est congrue $[\mathrm{mod}\,\mathfrak{p}, g(x), f(x,y)]$ à une fonction entière en x, y dont le degré est inférieur à $\tau - 1$ en x et à $\lambda - 1$ en y et dont les coefficients sont réduits, mod p.

Dès lors il s'ensuit que

$$\{r - \varpi[x,y]\}\{r - [\varpi(x,y)]^{p}\}\{r - [\varpi(x,y)]^{p^2}\}\ldots\{r - [\varpi(x,y)]^{p^{h-1}}\}$$
$$\equiv \mathrm{P}(r,x,y) \qquad [\mathrm{mod}\,\mathfrak{p} g(x), f(x,y)],$$

où $\mathrm{P}(r, x, y)$ est une fonction irréductible en r, x, y de degré h en r, d'un degré inférieur ou égal à $\tau - 1$ en x et à $\lambda - 1$ en y et dont les coefficients sont des entiers rationnels réduits (mod p).

Finalement nous avons

$$r^{p^h} - r \equiv \Pi_i (r - r_i) \equiv \Pi P(r, x, y) \qquad [\text{mod } \mathfrak{p}, g(x), f(x, y)],$$

où r est une fonction quelconque de r, x, y qui est de hauteur h. Le premier produit doit être étendu à un système de $\mathfrak{p}^h$ fonctions incongrues r_i [mod $\mathfrak{p}$, $g(x)$, $f(x, y)$] qui sont de hauteur h ou de hauteur d, où d est un diviseur de h. Le second produit doit être étendu à toutes les *fonctions premières primaires* $P(r, x, y)$ dans lesquelles le coefficient de la plus haute puissance de r est l'unité, le degré en r étant h ou d, où d est un diviseur de h, en x le degré étant inférieur ou égal à $\tau - 1$ et à $\lambda - 1$ en y et tous les coefficients constants étant des entiers rationnels qui ont été réduits (mod p).

Puisque ces fonctions premières primaires ne sont pas répétées dans le produit précédent, on voit que nous avons l'équivalence

$$[\mathfrak{p}, g(x), f(x, y), r^{p^h} - r] \backsim \Pi [\mathfrak{p}, g(x), f(x, y), P(r, x, y)],$$

où le produit doit être étendu à tous les systèmes modulaires où il apparaît comme élément une fonction première *primaire* différente, dont le degré en r est h ou d, d étant un diviseur de h, le degré en x étant inférieur ou égal à $\tau - 1$ et en y à $\lambda - 1$ et dont les coefficients sont des entiers rationnels réduits (mod p).

Réduction des systèmes modulaires de troisième espèce dans lesquels la seconde puissance ou une puissance plus élevée de la fonction irréductible $g(x)$ (mod $\mathfrak{p}$) entre comme élément.

Les systèmes sont de la forme

$$\left\{ \mathfrak{p}, g(x)^2, g(x) \sum_{\nu=1}^{\nu=n} [f_\nu(x, y)], \sum_{\mu=1}^{\mu=m} [h_\mu(x, y)] \right\},$$

qui, par l'introduction des systèmes auxiliaires, est immédiatement réduite à la *forme canonique*

$$[\mathfrak{p}, g(x)^2, g(x)\theta(x, y), g(x)\varphi(x, y) + \theta(x, y)\theta^{(1)}(x, y)],$$

dans laquelle, lorsqu'elle est développée suivant les puissances décroissantes de y :

1°

$$\theta(x, y) = y^k + A_0(x) y^{k-1} + \ldots + A_k(x),$$

les degrés de $A_0(x), \ldots, A_k(x)$ étant au plus égaux à $\tau - 1$, où τ est le degré de $g(x)$;

2° Le coefficient de la plus haute puissance de y dans $\theta^{(1)}$ est l'unité et les autres ont été réduits [mod $g(x)$];

3° Le degré de $\varphi(x, y)$ en y est inférieur au degré de $\theta(x, y)$ en y;

4° Tous les coefficients constants sont pris parmi les entiers déterminés $\rho_1, \rho_2, \ldots, \rho_k$.

Lorsque $g(x)$ entre à la troisième puissance, la forme du système modulaire est

$$\left\{ \mathfrak{p},\ g(x)^3,\ g(x)^2 \prod_{\nu=1}^{\nu=n} [f_\nu(x, y)],\ g(x) \prod_{\mu=1}^{\mu=m} [h_\mu(x, y)],\ \prod_{\lambda=1}^{\lambda=l} [k_\lambda(x, y)] \right\},$$

qui est équivalente à la *forme canonique*

$$\left[\begin{array}{c} \mathfrak{p},\ g(x)^3,\ g(x)^2\theta(x, y),\ g(x)^2\varphi(x, y) + g(x)\theta(x, y)\theta^{(1)}(x, y), \\ g(x)^2\psi(x, y) + g(x)\theta(x, y)\theta^{(2)}(x, y) + g(x)\varphi(x, y)\varphi^{(1)}(x, y) \\ + \theta(x, y)\theta^{(1)}(x, y)\varphi^{(1)}(x, y) \end{array} \right].$$

Dans cette forme canonique nous observons que, lorsqu'elle est développée suivant les puissances décroissantes de y:

1° Le premier coefficient de $\theta(x, y)$, de $\theta^{(1)}(x, y)$ et de $\varphi^{(1)}(x, y)$ est l'unité et les autres coefficients ont été réduits [mod $g(x)$];

2° $\varphi(x, y)$ et $\psi(x, y)$ sont, en y, de degré inférieur au degré de $\theta(x, y)$ et leurs coefficients ont tous été réduits [mod $g(x)$];

3° $\theta^{(2)}(x, y)$ est en y de degré inférieur au degré de $\theta^{(1)}(x, y)$ et ses coefficients ont été réduits [mod $g(x)$];

4° Les coefficients constants qui entrent dans tous les éléments sont pris parmi les entiers déterminés $\rho_1, \rho_2, \ldots, \rho_k$.

Des formes analogues peuvent être déterminées pour les systèmes dans lesquels la quatrième puissance ou des puissances plus élevées de $g(x)$ entrent comme élément.

Considérons maintenant le système

$$\text{(I)} \qquad \left\{ \mathfrak{p}^2,\ g(x),\ \mathfrak{p} \prod_{\nu=1}^{\nu=n} [f_\nu(x, y)],\ \prod_{\mu=1}^{\mu=m} [h_\mu(x, y)] \right\},$$

et supposons que $g(x) \equiv g_1(x) g_2(x) \pmod{\mathfrak{p}}$ et que $g_1(x)$ et $g_2(x)$ soient irréductibles (mod $\mathfrak{p}$).

Du système auxiliaire

$$(a) \quad \left\{ \mathfrak{p}, g(x), \prod_{\mu=1}^{\mu=m} [h_\mu(x, y)] \right\}$$
$$\backsim \left\{ \mathfrak{p}, g_1(x), \prod_{\mu=1}^{\mu=m} [h_\mu(x, y)] \right\} \left\{ \mathfrak{p}, g_2(x), \prod_{\mu=1}^{\mu=m} [h_\mu(x, y)] \right\}$$
$$\backsim [\mathfrak{p}, g_1(x), \mathrm{H}_1(x, y)][\mathfrak{p}, g_2(x), \mathrm{H}_2(x, y)]$$
$$\backsim [\mathfrak{p}, g(x), g_1(x)\mathrm{H}_2(x, y), g_2(x)\mathrm{H}_1(x, y), \mathrm{H}_1(x, y)\mathrm{H}_2(x, y)]$$

nous tirons, d'une part,

$$(1) \quad h_\mu(x, y) = \mathfrak{p}\pi_\mu + g\gamma_\mu + g_1\mathrm{H}_2\delta_\mu + g_2\mathrm{H}_1\beta_\mu + \mathrm{H}_1\mathrm{H}_2\alpha_\mu \qquad (\mu = 1, 2, \ldots, m),$$

où nous employons le signe fonctionnel pour les fonctions de x, y et où toutes les quantités introduites appartiennent au domaine $[\rho, x, y]$; d'autre part, nous tirons

$$(2) \quad \begin{cases} g_1(x)\mathrm{H}_2(x, y) = \mathfrak{p}\mathrm{A}_1 + g\mathrm{B}_1 + \sum_{\mu=1}^{\mu=m} h_\mu b_\mu^{(1)}, \\ g_2(x)\mathrm{H}_1(x, y) = \mathfrak{p}\mathrm{A}_2 + g\mathrm{B}_2 + \sum_{\mu=1}^{\mu=m} h_\mu b_\mu^{(2)}, \\ \mathrm{H}_1(x, y)\mathrm{H}_2(x, y) = \mathfrak{p}\mathrm{A}_3 + g\mathrm{B}_3 + \sum_{\mu=1}^{\mu=m} h_\mu b_\mu^{(3)}. \end{cases}$$

On voit, d'après (2), que nous pouvons ajouter les éléments

$$\begin{aligned} \mathrm{S}_1 &= g_1(x)\mathrm{H}_2(x, y) - \mathfrak{p}\mathrm{A}_1, \\ \mathrm{S}_2 &= g_2(x)\mathrm{H}_1(x, y) - \mathfrak{p}\mathrm{A}_2, \\ \mathrm{S}_3 &= \mathrm{H}_1(x, y)\mathrm{H}_2(x, y) - \mathfrak{p}\mathrm{A}_3, \end{aligned}$$

au système (I) sans qu'il cesse d'être équivalent à lui-même.

De plus, d'après (1), on voit que

$$h_\mu(x, y) = \mathfrak{p}(\pi_\mu + \mathrm{A}_1\delta_\mu + \mathrm{A}_2\beta_\mu + \mathrm{A}_3\alpha_\mu) + g\gamma_\mu + \mathrm{S}_1\delta_\mu + \mathrm{S}_2\beta_\mu + \mathrm{S}_3\alpha_\mu$$
$$(\mu = 1, 2, \ldots, m),$$

ou

$$h_\mu(x, y) \equiv \mathfrak{p} k_\mu \qquad (\mathrm{mod}\ g, S_1, S_2, S_3)$$
$$(\mu = 1, 2, \ldots, m),$$

où pour abréger j'ai posé

$$k_\mu = \pi_\mu + A_1\delta_\mu + A_2\beta_\mu + A_3\alpha_\mu \qquad (\mu = 1, 2, \ldots, m).$$

Le système (I) est équivalent à

$$(II) \qquad \left\{ \mathfrak{p}^2,\ g(x),\ \mathfrak{p}\sum_{\nu=1}^{\nu=n}[f_\nu(x, y)],\ \mathfrak{p}\sum_{\mu=1}^{\mu=m}[k_\mu(x, y)],\ S_1,\ S_2,\ S_3 \right\}.$$

Avec les éléments

$$\mathfrak{p}^2, \quad \mathfrak{p}g(x), \quad \mathfrak{p}\sum_{\nu=1}^{\nu=m}[f_\nu(x, y)], \quad \mathfrak{p}\sum_{\mu=1}^{\mu=m}[k_\mu(x, y)],$$

nous formerons le système

$$\mathfrak{p}\left\{\mathfrak{p},\ g(x),\ \sum_{\nu=1}^{\nu=n}[f_\nu(x, y)],\ \sum_{\mu=1}^{\mu=m}[k_\mu(x, y)]\right\}$$
$$\backsim \mathfrak{p}\left\{\mathfrak{p}, g_1(x), \sum_{\nu=1}^{\nu=n}[f_\nu(x, y)], \sum_{\mu=1}^{\mu=m}[k_\mu(x, y)]\right\}\left\{\mathfrak{p}, g_2(x), \sum_{\nu=1}^{\nu=n}[f_\nu(x, y)], \sum_{\mu=1}^{\mu=m}[k_\mu(x, y)]\right\}$$
$$\backsim \mathfrak{p}[\mathfrak{p}, g_1(x), F_1(x, y)][\mathfrak{p}, g_2(x), F_2(x, y)]$$
$$\backsim \mathfrak{p}[\mathfrak{p}, g(x), g_1(x)F_2(x, y), g_2(x)F_1(x, y), F_1(x, y)F_2(x, y)].$$

On déduit de là que le système (II) est équivalent au système

$$(III) \qquad \left\{ \mathfrak{p}^2,\ g(x),\ \mathfrak{p} \left| \begin{array}{ll} g_1(x)F_2(x, y), & g_1(x)H_2(x, y) - \mathfrak{p}A_1 \\ g_2(x)F_1(x, y), & g_2(x)H_1(x, y) - \mathfrak{p}A_2 \\ F_1(x, y)F_2(x, y), & H_1(x, y)H_2(x, y) - \mathfrak{p}A_3 \end{array} \right. \right\}.$$

Puisque

$$\mathfrak{p}[g_1(x)H_2(x, y) - \mathfrak{p}A_1] \equiv \mathfrak{p}g_1(x)H_2(x, y) \qquad (\mathrm{mod}\ \mathfrak{p}^2),$$

on voit que nous pouvons ajouter au système (III) les éléments

$$\mathfrak{p}g_1(x)H_2(x, y), \quad \mathfrak{p}g_2(x)H_1(x, y), \quad \mathfrak{p}H_1(x, y)H_2(x, y),$$
$$\mathfrak{p}g_1(x)A_2(x, y), \quad \mathfrak{p}g_2(x)A_1(x, y).$$

Des systèmes

$$(1)\qquad \mathfrak{p}(\mathfrak{p}, g, F_1F_2, H_1H_2) \backsim \mathfrak{p}(\mathfrak{p}, g_1, F_1F_2, H_1H_2)(\mathfrak{p}, g_2, F_1F_2, H_1H_2)$$
$$\backsim (\mathfrak{p}, g_1, M_1)(\mathfrak{p}, g_2, M_1) \backsim \mathfrak{p}(\mathfrak{p}, g, g_1M_2, g_2M_1, M_1M_2),$$

$$(2)\qquad (\mathfrak{p}^2 g_1, \mathfrak{p} g_1 g_2, \mathfrak{p} g_1 F_2, \mathfrak{p} g_1 A_2, \mathfrak{p} g_1 H_2, \mathfrak{p} g_1 M_2)$$
$$\backsim \mathfrak{p} g_1(\mathfrak{p}, g_2, F_2, H_2, A_2, M_2) \backsim \mathfrak{p} g_1(\mathfrak{p}, g_1, L_2),$$

$$(3)\qquad \mathfrak{p} g_2(\mathfrak{p}, g_1, F_1, H_1, A_1, M_1) \backsim \mathfrak{p} g_2(\mathfrak{p}, g_1, L_1),$$

on déduit que le système (III) devient

$$(III')\qquad \left\{ \begin{array}{ccc|cc} \mathfrak{p}^2, & g, & \mathfrak{p} & g_1L_2, & g_1H_2 - \mathfrak{p}A_1 \\ & & & g_2L_1, & g_2H_1 - \mathfrak{p}A_2 \\ & & & M_1M_2, & H_1H_2 - \mathfrak{p}A_3 \end{array} \right\},$$

dans lequel g_1H_2, g_2H_1, H_1H_2, A_1 et A_2 peuvent être exprimés par des formes linéaires des éléments L_1, L_2, M_1M_2 et $\mathfrak{p}$ par le moyen des formules (1), (2) et (3).

Corollaire. — Le système modulaire

$$\left\{ \mathfrak{p}^2, \mathfrak{p} g_1(x), g(x), \mathfrak{p} \prod_{\nu=1}^{\nu=n} [f_\nu(x, y)], \prod_{\mu=1}^{\mu=m} [h_\mu(x, y)] \right\}$$

où

$$g(x) \equiv g_1(x) g_2(x) \pmod{\mathfrak{p}},$$

et où $g_1(x)$ et $g_2(x)$ sont irréductibles (mod $\mathfrak{p}$), est équivalent à

$$[\mathfrak{p}^2, \mathfrak{p} g_1(x), \mathfrak{p}\theta(x, y), g_1(x)\varphi(x, y)].$$

Lorsque les fonctions sont développées suivant les puissances décroissantes de y, nous remarquons que :

1° Le coefficient de la plus haute puissance de $\theta(x, y)$ est l'unité et que les autres coefficients ont été réduits [mod $\mathfrak{p}$, $g_1(x)$] ;

2° Le coefficient de la plus haute puissance de $\varphi(x, y)$ est l'unité et que les autres ont été réduits [mod $\mathfrak{p}$, $g_2(x)$].

Si $g(x) \equiv g_1(x) g_2(x) g_3(x)$ (mod $\mathfrak{p}$) et si $g_1(x)$, $g_2(x)$, $g_3(x)$ sont des fonctions irréductibles (mod $\mathfrak{p}$), la méthode de réduction est tout à fait la même que celle que nous venons de donner.

Finalement le système

$$\left\{\mathfrak{p}^2,\ g(x)^2,\ \mathfrak{p}\prod_{\nu=1}^{\nu=n}[f_\nu(x,y)],\ g(x)\prod_{\mu=1}^{\mu=m}[h_\mu(x,y)],\ \mathfrak{p}g(x)\prod_{\lambda=1}^{\lambda=l}[\varphi_\lambda(x,y)],\ \prod_{\tau=1}^{\tau=t}\psi_\tau(x,y)]\right\},$$

où $g(x)$ est irréductible (mod $\mathfrak{p}$) est équivalent à un système de la forme

$$[\mathfrak{p}^2,\ g(x)^2,\ \mathfrak{p}g(x)\theta(x,y),\ \mathfrak{p}\psi(x,y),\ \mathfrak{p}\chi(x,y)+\mathbf{M}(x,y),\ g(x)\mathbf{A}(x,y)+\mathfrak{p}\mathbf{K}(x,y)].$$

Le système

$$\left\{\mathfrak{p}^3,\ g(x),\ \mathfrak{p}^2\prod_{\nu=1}^{\nu=n}[f_\nu(x,y)],\ \mathfrak{p}\prod_{\mu=1}^{\mu=m}[h_\mu(x,y)],\ \prod_{\lambda=1}^{\lambda=l}[\varphi_\lambda(x,y)]\right\},$$

où $g(x)$ est irréductible (mod $\mathfrak{p}$) est équivalent au système

$$[\mathfrak{p}^3,\ g(x),\ \mathfrak{p}^2\mathbf{F}(x,y),\ \mathfrak{p}\mathbf{H}(x,y),\ \mathbf{\Phi}(x,y)].$$

Lorsque $g(x)\equiv g_1(x)g_2(x)$ (mod $\mathfrak{p}$) la méthode de réduction est la même que celle qui a déjà été donnée.

Les réductions précédentes ont toutes été faites pour des systèmes de la forme

$$\left\{\prod_{\lambda=1}^{\lambda=k}(\mu_\lambda),\ \prod_{\pi=1}^{\pi=m}[g_\pi(x)],\ \prod_{\nu=1}^{\nu=n}[f_\nu(x,y)]\right\}.$$

Nous avons donc supposé la présence d'un entier algébrique et d'une fonction entière d'une variable à coefficients entiers et algébriques parmi les éléments.

Si le système donné est de la forme

$$\left\{\prod_{\nu=1}^{\nu=n}[f_\nu(x,y)]\right\},$$

puisque les fonctions $f_1(x,y)$, $f_2(x,y)\ldots, f_n(x,y)$ n'ont pas toutes un diviseur commun (un tel diviseur peut être enlevé comme facteur du système), il est, en général, possible de trouver des fonctions

$\bar{f}_1(x,y)$, $\bar{f}_2(x,y)$, ..., $\bar{f}_n(x,y)$, telles que

$$(1)\quad f_1(x,y)\bar{f}_1(x,y)+f_2(x,y)\bar{f}_2(x,y)+\ldots+f_\nu(x,y)\bar{f}_\nu(x,y)=g(x),\qquad \nu\leq n,$$

où $g(x)$ est une fonction entière en x à coefficients entiers appartenant à Ω.

Cela est toujours vrai lorsque les équations

$$f_1(x,y)=0,\qquad f_2(x,y)=0,\qquad \ldots,\qquad f_n(x,y)=0$$

ont un nombre fini de solutions communes à deux quelconques d'entre elles.

S'il n'y a pas de solution commune à certaines des équations précédentes, par l'algorithme du plus grand commun diviseur nous pouvons déterminer les fonctions $\bar{f}_1(x,y)$, $\bar{f}_2(x,y)$, ..., $\bar{f}_n(x,y)$ de telle façon que

$$(2)\quad f_1(x,y)\bar{f}_1(x,y)+f_2(x,y)\bar{f}_2(x,y)+\ldots+f_\nu(x,y)\bar{f}_\nu(x,y)=\mu,\qquad \nu>1,$$

où μ est un entier algébrique de Ω.

Dès lors, dans nos hypothèses, nous avons supposé tout au plus l'existence de l'élément μ ou de l'élément $g(x)$.

En choisissant différents éléments $f_1(x,y)$, $f_2(x,y)$, ..., $f_n(x,y)$, nous pouvons, en général, former deux formes linéaires telles que (1) dans lesquelles les fonctions d'une variable $g(x)$ et $g_1(x)$, par exemple, n'ont pas de valeur commune qui les fasse s'évanouir simultanément.

Nous pouvons alors trouver deux fonctions $\bar{g}(x)$ et $\bar{g}_1(x)$ telles que

$$g(x)\,\bar{g}(x)+g_1(x)\,\bar{g}_1(x)=\mu,$$

où μ est un entier algébrique de Ω qui peut être adjoint comme élément au système modulaire.

Si le système est de la forme

$$\left\{g(x),\ \prod_{\nu=1}^{\nu=n}[f_\nu(x,y)]\right\},$$

nous pouvons encore effectuer les réductions précédentes, si nous changeons le domaine d'intégrité dans lequel nous admettons que, à côté des entiers algébriques, nous considérions aussi, dans la discussion, des fractions algébriques de Ω (*voir* DEDEKIND, p. 537), tandis que, pour obtenir les réductions précédentes dans les systèmes tels que

$$\left\{\mu, \prod_{\nu=1}^{\nu=n} [f_\nu(x, y)]\right\},$$

nous devons laisser entrer les fonctions rationnelles aussi bien que les fonctions entières de l'une des variables dans le domaine donné.

La réduction des systèmes de la forme

$$\left\{\mathfrak{p}, g(x), f(x, y), \prod_{\mu=1}^{\mu=m} [h_\mu(x, y, z)]\right\},$$

où $g(x)$ est irréductible (mod $\mathfrak{p}$) et $f(x, y)$ irréductible [mod $\mathfrak{p}, g(x)$], et aussi des systèmes dans lesquels il entre comme éléments des puissances de ces fonctions, peut être obtenue de la même manière que les réductions précédentes. Un Mémoire qui touche brièvement ce sujet, mais seulement pour le domaine des entiers rationnels, paraîtra dans le *Journal de Crelle*. Eu égard à ce Travail et aux résultats déjà obtenus dans le présent Mémoire, il ne semble pas nécessaire d'entrer ici dans une discussion détaillée des systèmes modulaires de quatrième espèce et d'espèce supérieure.