NOUVELLES ANNALES DE MATHÉMATIQUES

LÉON AUTONNE

Sur un certain domaine holoïde, complet et bien défini

Nouvelles annales de mathématiques 4^e série, tome 7 (1907), p. 49-77

<http://www.numdam.org/item?id=NAM_1907_4_7__49_0>

[A1a]

SUR UN CERTAIN DOMAINE HOLOÏDE, COMPLET ET BIEN DÉFINI;

PAR M. LÉON AUTONNE.

INTRODUCTION.

On sait que les polynomes $f(z) = f(z_1, \ldots, z_n)$, à n variables *indépendantes,* se comportent, *au point de vue formel,* comme des nombres entiers, en ce qui concerne les quatre opérations élémentaires (addition, soustraction, multiplication, division) et la divisibilité.

On peut de même donner du p. g. c. d. (plus grand commun diviseur) une définition identique pour les nombres entiers et les polynomes f.

La voici : *Le p. g. c. d.* D *de deux quantités* (*entiers ou polynomes*) A *et* B *est :* 1° *Un diviseur commun à* A *et* B; 2° *Divisible par tous les diviseurs communs à* A *et* B.

D existe toujours, pour tout choix de A et B, et s'obtient par un nombre fini d'opérations, d'une nature déterminée.

Pour exprimer toutes ces diverses propriétés, nous dirons avec M. König (Julius), dans son livre, *Einleitung in die allgemeine Theorie der algebraischen Grössen* (Teubner, 1903), que les polynomes f constituent, comme les nombres entiers, *un domaine holoïde, complet et bien défini* (ein echter holoider, vollständiger und wohldefinierter Bereich).

L'algèbre formelle de pareils domaines coïncide avec l'arithmétique ordinaire, à cause de l'existence du p. g. c. d. Ainsi :

Tout facteur irréductible (divisible par lui-même et par l'unité seulement) est aussi premier (ne divise pas un produit de deux facteurs sans diviser au moins un des facteurs);

La décomposition en facteurs premiers est toujours possible et d'une seule façon, etc.

Si les variables, qui figurent dans les polynomes f, au lieu d'être indépendantes, sont liées par une ou plusieurs relations algébriques, le p. g. c. d. n'existe plus en général, et le domaine est incomplet. L'algèbre des domaines incomplets est incomparablement plus compliquée et difficile.

Il y a donc intérêt à signaler un domaine de polynomes, qui reste complet, malgré l'existence d'une relation algébrique entre les variables.

Voici le domaine dont il s'agit :

C'est celui des polynomes homogènes

$$F(z) = F(z_1, \ldots, z_n),$$

les z étant liées par la relation quadratique homogène $\omega(z) = 0$, où

$$\omega(z) = z_1^2 + \ldots + z_n^2,$$

c'est-à-dire une forme quadratique quelconque, à déterminant non évanouissant.

Dans le présent travail, j'établis qu'un pareil domaine est holoïde, complet et bien défini.

Notons cependant que l'on a supposé n supérieur à 4. Le cas de 4 et de 3 variables homogènes appelle des recherches spéciales.

Dans les notations et les raisonnements, on trouvera

une certaine analogie avec la deuxième Partie de mon Mémoire *Sur les Formes mixtes* (Paris, Gauthier-Villars; Lyon, A. Rey, 1905), inséré aux *Annales de l'Université de Lyon*.

Comme application de la présente théorie, je signalerai le champ de la géométrie réglée.

Les six coordonnées homogènes p d'une droite sont six variables, liées uniquement par la relation quadratique

$$\omega(p) = p_1p_2 + p_3p_4 + p_5p_6 = 0.$$

Il n'est donc pas douteux que le théorème du présent Mémoire ne trouve son emploi dans les recherches sur les complexes algébriques de droites

$$F(p_1, \ldots, p_6) = 0.$$

GÉNÉRALITÉS.

1° On renverra au livre de M. König (Julius), *Einleitung in die allgemeine Theorie der algebraischen Grössen* (Teubner, 1903) pour explications détaillées et précises sur les *domaines* et notamment sur les domaines *holoïdes*. On ne rappellera ci-après que les principes essentiels de la matière et encore très rapidement.

2° Soit Ω un système de quantités x_1, x_2, ... Définissons deux opérations à effectuer sur les x, l'addition et la multiplication.

L'addition est :

Univoque :	$x_1 + x_2$ bien déterminé et unique;
Commutative :	$x_1 + x_2 = x_2 + x_1$;
Associative :	$x_1 + (x_2 + x_3) = (x_1 + x_2) + x_3$.

Elle admet un module, le zéro, tel que $x_1 + 0 = x_1$ pour tout x_1.

La multiplication est :

Univoque :	$x_1 x_2$ bien déterminé et unique;
Commutative :	$x_1 x_2 = x_2 x_1$;
Associative :	$x_1 (x_2 x_3) = (x_1 x_2) x_3$);
Distributive :	$x_1 (x_2 + x_3) = x_1 x_2 + x_1 x_3$.

Elle admet un module (1 ou unité absolue) tel que $1 x_1 = x_1$ pour tout x_1.

Si la somme et le produit de deux *termes* x_1 et x_2 du système Ω font encore partie de Ω, Ω devient un *domaine* (Bereich).

L'addition et la multiplication peuvent, d'ailleurs, à condition de suivre les règles ci-dessus, *être définies à volonté*.

3° Le domaine Ω devient *holoïde* (echter holoider Bereich) si, en sus des propriétés précédentes :

I. En additionnant, autant de fois qu'on veut, l'unité absolue avec elle-même on n'obtient jamais zéro (l'unité absolue fait partie de Ω);

II. Pour un choix convenable de termes x_1 et x_2 de Ω, l'équation

$$x_1 \xi = x_2$$

n'a pas, dans Ω, de solution ξ.

Le mot *holoïde* rappelle que le domaine Ω se comporte comme celui des nombres *entiers* ordinaires.

4° Dans Ω, le terme a *divise* le terme c, s'il existe, dans Ω, un terme b tel que $c = ab$.

Deux termes a et b de Ω ont un p. g. c. d. (plus grand commun diviseur) d, si le terme d de Ω :

I. Divise a et b;

II. Est divisible par tout diviseur commun à a et b.

En général, dans un domaine holoïde, pour deux termes pris à volonté, le p. g. c. d. n'existe pas. Le domaine est *incomplet*.

Le domaine est *complet* (vollständig), si, *pour tout choix* des termes a et b, leur p. g. c. d. existe.

Le domaine holoïde et complet Ω est, en outre, *bien défini* (wohldefiniert), si l'on possède une méthode pour obtenir le p. g. c. d. d de a et b, en effectuant sur a et b *un nombre fini d'opérations d'une nature déterminée.*

5° Dans le domaine holoïde Ω, tout diviseur de l'unité absolue est une unité. Est dit *irréductible* tout terme qui n'est divisible que par lui-même et les unités. Est *premier* tout terme qui ne peut diviser un produit de deux facteurs sans en diviser au moins un. Tout facteur premier est irréductible, mais la réciproque n'est vraie que pour les domaines complets.

6° Ces derniers suivent les *règles formelles* de l'arithmétique ordinaire en ce qui concerne :

Les quatre opérations élémentaires;

La divisibilité;

Le p. g. c. d.;

La décomposition en facteurs premiers, etc.

Les choses sont incomparablement plus compliquées pour les domaines incomplets. Il est, par suite, très intéressant de reconnaître si un domaine holoïde donné est ou non complet et bien défini.

7° Est complet, par exemple, le domaine des polynomes à n variables *indépendantes* $x_1, \ldots, x_n$. Pour

préciser cette notion de variables indépendantes, je dirai : soit un polynome

$$f = f(x_1, \ldots, x_n; a_1, a_2, \ldots),$$

pris à volonté, mais avec un au moins des coefficients a différent de zéro; on doit pouvoir trouver au moins un système de valeurs

$$x_1 = \xi_1, \quad \ldots, \quad x_n = \xi_n,$$

tel que

$$f(\xi_1, \ldots, \xi_n; a_1, a_2, \ldots) \neq 0.$$

Un polynome nul, à variables indépendantes, est donc nul identiquement, c'est-à-dire a tous ses coefficients nuls.

8° Le domaine, au contraire, est incomplet, en général, quand les variables sont liées par une ou plusieurs relations algébriques.

9° L'objet du présent travail est précisément de montrer que le domaine holoïde Ω des polynomes homogènes $F(z) = F(z_1, \ldots, z_n)$ *reste complet et bien défini*, lorsqu'on introduit, entre les n variables, une relation quadratique

$$\omega(z) = z_1^2 + \ldots + z_n^2 = 0.$$

10° Je suppose connue du lecteur la théorie :
Des *Tableaux*

$$[a_{\lambda\mu}], \qquad \{\lambda = 1, 2, 3, \ldots, L;\ \mu = 1, 2, \ldots, M\},$$

à L lignes et M colonnes

$$\left\| \begin{matrix} a_{11} & \ldots & a_{1M} \\ \ldots & \ldots & \ldots \\ \ldots & a_{\lambda\mu} & \ldots \\ \ldots & \ldots & \ldots \\ a_{L1} & \ldots & a_{LM} \end{matrix} \right\|;$$

Des *matrices* L-*aires* ou Tableaux carrés, $L = M$;

Des collinéations, des formes bilinéaires, etc.

On consultera par exemple le livre de M. Pascal, *Die Determinanten* (Leipzig, Teubner, 1900).

CHAPITRE I.

Domaine holoïde Ω *des formes* $F(z)$.

1° Soient $z_1, \ldots, z_n$ des variables indépendantes et $F\binom{m}{z}$ un polynome *homogène*, de degré m par rapport aux z. Si l'on a soin d'additionner ensemble seulement des polynomes F de même degré, les F sont les termes d'un domaine E_n.

Si $m = 0$, on a une constante C. Si $C = 1$, on a l'unité absolue, module de la multiplication ; si $C = 0$, on a le zéro, module de l'addition.

E_n est holoïde, car, par exemple, l'équation

$$z_1 \zeta = z_2^2$$

ne possède pas, dans E_n, de solution ξ.

Le domaine E_n est-il complet et bien ordonné ?

Oui, et voici pourquoi :

Le p. g. c. d. $D(z)$ de deux termes $A(z)$ et $B(z)$ s'obtient toujours par les procédés de l'algèbre élémentaire.

Reste à montrer que $D(z)$ appartient à F_n, c'est-à-dire est homogène. Si D n'est pas homogène, on écrira pour D

$$D = D_0 + D_1 + \ldots + D_k$$

$\{ D_0$ étant homogène avec le degré μ_0, D_1 avec le degré $\mu_1, \ldots, \mu_0 < \mu_1 < \ldots < \mu_k \}$, et, pour le quo-

tient $K = A : D$,

$$K = K_0 + K_1 + \ldots + K_g$$

| K_0 étant homogène avec le degré λ_0, K_1 avec le degré $\lambda_1, \ldots$; $\lambda_0 < \lambda_1 < \ldots < \lambda_g$ |.

Le produit $A = KD$ contiendra sûrement les deux expressions $K_0 D_0$ et $K_g D_k$ de degrés inégaux $\lambda_0 + \mu_0$ et $\lambda_g + \mu_k$, $\lambda_0 < \lambda_g$, $\mu_0 < \mu_k$; cela est absurde; K et D sont homogènes.

2° Nommons $\omega(z)$ une forme quadratique n-aire, à déterminant non nul. On peut toujours écrire

$$\omega = z_1^2 + \ldots + z_n^2, \tag{1}$$

ou encore, ou bien

$$\omega = z_1 z_2 + z_3 z_4 + \ldots + z_{2n'-1} z_{2n'}, \tag{2}$$

si $n = \text{pair} = 2n'$;

Ou bien, si $n = \text{impair} = 2n' + 1$,

$$\omega = z_1 z_2 + \ldots + z_{2n'-1} z_{2n'} + z_{2n'+1}^2. \tag{3}$$

En effet ($i^2 + 1 = 0$),

$$z_1^2 + z_2^2 = (z_1 + iz_2)(z_1 - iz_2) \ldots.$$

Posons $\omega = z_1 z_2 - \zeta$; la forme quadratique

$$-\zeta = z_3 z_4 + \ldots,$$

à $n - 2$ variables, a encore son déterminant non nul.

Si $n = 4$ ou 3, il vient $-\zeta = z_3 z_4$ ou z_3^2. ζ n'est plus irréductible.

Jusqu'à nouvel avis, on prendra $n \geq 5$ et ζ irréductible.

3° Altérant la synonymie habituelle des mots *forme*

et *polynome homogène,* je dirai que le polynome homogène $F\binom{m}{z}$, terme du domaine E_n, devient une *forme,* si, au lieu d'être indépendantes, les n variables z sont liées par la relation $\omega(z) = 0$.

Les z sont alors les coordonnées homogènes d'un point z pris sur une quadrique Z, dans un espace à $n-1$ dimensions. Sur Z, il y a $n-1$ variables indépendantes $z_2, \ldots, z_n$, la $n^{\text{ième}}$ z_1 s'obtenant par la formule

$$z_1 = \frac{\zeta}{z_2} = -\frac{z_3 z_4 + \ldots}{z_2}.$$

Des notations telles que $F^{(1)}$, $F^{(12)}$, ... indiquent que dans la forme F manque la variable z_1, ou manquent les deux variables z_1 et z_2, etc.

Comme les $n-1$ variables de $F^{(1)}$ sont indépendantes, les $F^{(1)}$ constituent un domaine tel que E_n (1°), c'est-à-dire un domaine E_{n-1}.

De là une conséquence évidente : *Une forme* $F^{(1)}$, *nulle pour tout point z de la quadrique* Z, *est nulle identiquement, c'est-à-dire a tous ses*

$$\varphi(m) = \frac{(m+n-2)!}{(n-2)!\,m!}$$

coefficients nuls.

4° Théorème. — *Si une forme* $F\binom{m}{z}$ *est nulle pour tout point z de* Z, *le polynome homogène* F *est divisible par* ω.

Divisons le polynome, en z_1, $z_2^m F\binom{m}{z}$ par le binome en z_1, $\omega = z_2 z_1 - \zeta$. Il viendra l'identité

$$(1) \qquad z_2^m F\binom{m}{z} = \omega\binom{2}{z} Q\binom{2m-2}{z} + R^{(1)}\binom{2m}{z}.$$

Le reste $R^{(1)}$ de la division ne contient plus z_1 et est une expression $F^{(1)}$ du domaine E_{n-1} (3°).

En un point z de Z, $\omega = 0$ et, par hypothèse, $F = 0$. Donc, en vertu de l'identité (1), $R^{(1)} = 0$, et (3°, *in fine*) $R^{(1)}$ est identiquement nulle. Il reste l'identité

$$z_2^m F = \omega Q,$$

z_2 ne divise pas ω; z_2^m doit diviser Q. Si

$$P\binom{m-2}{z} = Q : z_2^m,$$

il vient

$$F\binom{m}{z} = \omega\binom{2}{z} P\binom{m-2}{z}. \qquad \text{C. Q. F. D.}$$

5° Pour exprimer que ω divise F, on écrira

$$F \equiv 0 \pmod{\omega},$$

et l'on dira que F est congrue à zéro suivant le module ω.

Deux formes de même degré $A\binom{m}{z}$ et $B\binom{m}{z}$ sont *équivalentes* ou *indistinctes à l'équivalence près,* si elles sont égales pour tout point z de **Z**. Il faut et il suffit pour cela que $A - B \equiv 0 \pmod{\omega}$, ou $A \equiv B \pmod{\omega}$, c'est-à-dire

$$B = A + \omega P\binom{m-2}{z}.$$

Ne sont à étudier pour des formes A, B, ... que les propriétés *permanentes,* qui subsistent quand on remplace, par exemple, A par une quelconque de ses formes équivalentes.

6° Je suis maintenant à même d'introduire le domaine Ω, objet principal des présentes recherches.

7° Les termes de Ω sont les formes $F(z)$, dont chacune n'est définie qu'à l'équivalence près (5°). Ainsi l'égalité ordinaire de l'Algèbre est remplacée par la congruence suivant le module ω.

L'addition (entre formes du même degré) et la multiplication, dans le domaine Ω, sont les opérations de même nom en algèbre ordinaire, mais à l'équivalence près.

Le domaine E_{n-1} des expressions $F^{(1)}$ (3°) est contenu dans Ω.

Quelle est l'unité absolue dans Ω?

Raisonnant sur un terme $F^{(1)}$ de Ω, on voit que cette unité absolue ne peut être que $1 = F\binom{0}{z}$, forme de degré zéro. Le zéro, module de l'addition, est toute forme divisible par ω.

8° Lemme. — *Soient* $A\binom{\alpha}{z}$ *et* $B\binom{\beta}{z}$ *deux formes, avec* $AB \equiv 0 \pmod{\omega}$, *mais* $A \not\equiv 0 \pmod{\omega}$. Alors $B \equiv 0 \pmod{\omega}$.

On a, comme au 4°,

$$Az_2^{\alpha} = \omega \mathfrak{A}_0 \binom{2\alpha - 2}{z} + \mathfrak{A}_1 \binom{2\alpha}{z},$$

$$Bz_2^{\beta} = \omega \mathfrak{B}_0 \binom{2\beta - 2}{z} + \mathfrak{B}_1 \binom{2\beta}{z};$$

$$z_2^{\alpha+\beta} AB \equiv \mathfrak{A}_1 \mathfrak{B}_1 \pmod{\omega}.$$

$\mathfrak{A}_1$ et $\mathfrak{B}_1$ sont des expressions $F^{(1)}$ (3°) pour lesquelles la congruence (mod ω) et l'égalité ordinaire se confondent.

Donc $AB \equiv 0 \pmod{\omega}$ entraîne $\mathfrak{A}_1 \mathfrak{B}_1 = 0$. $\mathfrak{A}_1 \not\equiv 0$, sans quoi ω diviserait A; on aurait, contrairement à l'hypothèse, $A \equiv 0 \pmod{\omega}$. Il vient

$$\mathfrak{B}_1 = 0, \quad B \equiv 0 \pmod{\omega}. \qquad \text{C. Q. F. D.}$$

9° D'autre part, l'équation $AX \equiv B \pmod{\omega}$, où A et B sont deux formes données et X une forme inconnue, n'a pas toujours de solutions dans Ω. Il en est ainsi, par exemple, pour $A = z_1$, $B = z_2^2$.

De tout cela résulte que *le domaine* ω *est holoïde.*

10° La forme $A\left(\begin{matrix} m \\ z \end{matrix}\right)$ *divise* $\pmod{\omega}$ la forme $C\left(\begin{matrix} m+m' \\ z \end{matrix}\right)$, s'il existe une forme $B\left(\begin{matrix} m' \\ z \end{matrix}\right)$ telle que

$$C \equiv AB \pmod{\omega}.$$

Une forme est *irréductible* $(\mathrm{mod}\,\omega)$, si elle n'est divisible $(\mathrm{mod}\,\omega)$ que par elle-même ou une constante.

Une forme-facteur est *première* $(\mathrm{mod}\,\omega)$, si, divisant $(\mathrm{mod}\,\omega)$ un produit de deux facteurs, elle divise $(\mathrm{mod}\,\omega)$ au moins l'un d'eux.

11° Soient quatre formes A, B, C, D de degrés α, β, γ, δ. Les deux *fractions*

$$\frac{B}{A} \quad \text{et} \quad \frac{D}{C}$$

sont *équivalentes* ou congrues $(\mathrm{mod}\,\omega)$

$$\frac{B}{A} \equiv \frac{D}{C} \pmod{\omega},$$

si $AD - BC \equiv 0 \pmod{\omega}$, avec, bien entendu,

$$\alpha + \delta = \beta + \gamma \quad \text{et} \quad A \not\equiv 0, \quad C \not\equiv 0 \pmod{\omega}.$$

L'addition et la multiplication des fractions s'obtiennent par les formules

$$\left.\begin{aligned} \frac{B}{A} + \frac{D}{C} &\equiv \frac{AD + BC}{AC} \\ \frac{B}{A} \times \frac{D}{C} &\equiv \frac{BD}{AC} \end{aligned}\right\} \pmod{\omega}.$$

12° L'objet principal du présent travail est d'établir que le domaine ω est *complet* et *bien défini* (Généralités, 4°).

Il est nécessaire pour cela d'introduire certaines formations, qui seront étudiées au Chapitre suivant.

CHAPITRE II.

Invariants et résiduelles d'une forme $F(z)$.

13° Si un polynome homogène $F\binom{m}{z}$ est divisible par ω, le quotient $Q\binom{m-2}{z} = F : \omega$ est unique et bien déterminé, puisque, en algèbre élémentaire, la division des polynomes, quand elle est possible, est une opération univoque.

Nommons a les $\varphi(m) = \frac{(m+n-1)!}{(n-1)!\,m!}$ coefficients de $F(z; a)$ et b les $\varphi(m-2)$ coefficients de $Q(z; b)$. L'identité $F = \omega Q$ fournit $\varphi(m)$ relations

$$a_\lambda = \sum_\mu l_{\lambda\mu} b_\mu, \tag{1}$$

$$\{\lambda = 1, 2, \ldots, \varphi(m);\ \mu = 1, 2, \ldots, \varphi(m-2)\},$$

où les $l_{\lambda\mu}$ sont des entiers nuls ou positifs, lesquels ne dépendent que de m et de n.

Je dis que *le Tableau* $[l_{\lambda\mu}]$ *à* $\varphi(m)$ *lignes et* $\varphi(m-2)$ *colonnes possède son rang maximum* $\varphi(m-2)$.

Si, en effet, ce rang était moindre que $\varphi(m-2)$, on pourrait satisfaire au système (1) *en annulant tous les a, un au moins des b n'étant pas zéro.*

Q n'étant pas identiquement nul, on aurait, ce qui

est absurde,

$$o = F = \omega Q.$$

14° L'élimination des $\varphi(m-2)$ lettres b entre les $\varphi(m)$ équations (1), introduira entre les a *exactement*

$$\begin{aligned}\mathfrak{M}(m) &= \varphi(m) - \varphi(m-2)\\ &= \frac{(m+n-1)!}{(n-1)!\,m!} - \frac{(m+n-3)!}{(n-1)!\,(m-2)!}\\ &= \frac{(m+n-3)!\,(2m+n-2)}{m!\,(n-2)!}\end{aligned}$$

relations linéaires distinctes, savoir

$$o = \Delta_\alpha(a) = \sum_\lambda a_\lambda d_\alpha, \qquad \{\alpha = 1, 2, \ldots, \mathfrak{M}(m)\},$$

où les $d_{\alpha\lambda}$ sont des nombres entiers réels qui ne dépendent que de m et de n.

Le Tableau $[d_{\alpha\lambda}]$ à $\mathfrak{M}(m)$ lignes et $\varphi(m)$ colonnes a son rang maximum $\mathfrak{M}(m)$, sans quoi les $\mathfrak{M}(m)$ expressions $\Delta_\alpha(a)$ ne seraient plus linéairement distinctes. On peut donc exprimer linéairement tous les $\varphi(m)$ coefficients a à l'aide :

I. Des $\mathfrak{M}(m)$ quantités Δ_α;

II. De $\varphi(m-2)$ paramètres arbitraires

$$a'_\mu, \quad \mu = 1, 2, \ldots, \varphi(m-2).$$

Cela permet d'écrire l'identité

$$(o) \qquad F\begin{pmatrix} m \\ z\,;a \end{pmatrix} = \sum_\alpha \Delta_\alpha \Phi_\alpha \begin{pmatrix} m \\ z \end{pmatrix} + \sum_\mu a'_\mu Q'_\mu \begin{pmatrix} m \\ z \end{pmatrix},$$

où les polynomes homogènes Φ_α et Q'_μ sont connus, en vertu du calcul précédent, dès qu'on possède m et n.

15° Les $\mathfrak{M}(m)$ conditions $\Delta_\alpha = 0$ sont nécessaires et suffisantes, quels que soient les paramètres a'_μ, pour que ω divise F.

L'égalité (o) donne, pour $\Delta_\alpha = 0$,

$$\omega Q = \sum_\mu a'_\mu Q'_\mu(z),$$

pour *tout choix* des a'_μ, en particulier, quand on annule tous les a'_μ sauf un. Donc Q'_μ est divisible par ω et (o) devient

$$F = \omega Q + \sum_\alpha \Phi_\alpha \Delta_\alpha. \tag{1}$$

16° Changeant légèrement les notations, je dirai que :

Tout polynome homogène F *de degré m, à n variables, peut identiquement s'écrire*

$$F = \sum_\alpha a_\alpha \Phi_\alpha + \omega Q,$$

où les constantes a_α, *au nombre* $\mathfrak{M}(m)$, *et les coefficients, au nombre de* $\varphi(m-2)$, *du polynome homogène* Q, *de degré* $m-2$, *changent avec les* $\varphi(m)$ *coefficients de* F, *tandis que les* $\mathfrak{M}(m)$ *polynomes* Φ_α *homogènes de degré m peuvent être choisis une fois pour toutes, dès qu'on s'est donné m et n.*

Les a_α sont les *invariants* du polynome F. Leur évanouissement simultané est la condition nécessaire et suffisante pour que F admette le diviseur ω.

Les $\Phi_\alpha(z)$ sont les formes *résiduelles élémentaires* pour le degré *m* et le nombre *n* de variables.

17° La formule (1) du 15° montre que F se confond, à l'équivalence près, avec l'expression $\overline{F} = \sum_{\alpha} a_\alpha \Phi_\alpha$, puisque

$$F \equiv \overline{F} \qquad (\mathrm{mod}\,\omega).$$

Je dirai que la forme $\overline{F}$ est la *résiduelle* de F, les Φ_α étant les *résiduelles élémentaires*.

Dans le domaine Ω, chaque forme F ne figure que par sa résiduelle $\overline{F}$, c'est-à-dire par ses invariants, puisque les résiduelles élémentaires sont fixes pour m et n donnés.

Toute expression

$$\mathfrak{R}_{mn} = \sum_{\alpha} K_\alpha \Phi_\alpha, \qquad K_\alpha = \text{const.}$$

est la résiduelle d'un polynome F, de degré m à n variables, dont les K_α sont les invariants.

18° Si $F = ef + e'f' + \ldots$, les e étant des constantes et les f des formes de degré m, comme F, l'invariant $\alpha^{\text{ième}}$ de F est évidemment

$$e a_\alpha + e' a'_\alpha + \ldots,$$

a_α étant l'invariant $\alpha^{\text{ième}}$ de f, etc.

Théorème. — *Les $\partial\mathfrak{l}(m)$ résiduelles élémentaires Φ_α sont linéairement indépendantes.*

En effet, admettons qu'on ait

$$\Phi_\alpha = \sum_{\gamma} g_{\alpha\gamma} \Psi_\gamma \binom{m}{z}, \qquad g_{\gamma\alpha} = \text{const.},$$

$\alpha = 1, 2, \ldots, \partial\mathfrak{l}(m); \qquad \gamma = 1, 2, \ldots, M; \qquad M < \partial\mathfrak{l}(m);$

les Ψ_γ étant linéairement indépendantes.

Prenons le polynome $F(z; a)$, aux $\varphi(m)$ coefficients indéterminés a, savoir (16°)

$$F = \omega Q + \sum_{\alpha} a_\alpha \Phi_\alpha = \omega Q + \sum_{\alpha\gamma} \Psi_\gamma a_\alpha g_{\alpha\gamma}$$

$$= \omega Q + \sum_{\gamma} \Psi_\gamma \sum_{\alpha} a_\alpha g_{\alpha\gamma}.$$

Pour rendre F divisible par ω, il n'est pas nécessaire d'écrire, comme l'exige le 14°, entre les a, $\mathfrak{M}(m)$ relations linéaires *distinctes*. Il suffit d'en écrire seulement $M < \mathfrak{M}(m)$, savoir

$$0 = \sum_{\alpha} a_\alpha g_{\alpha\gamma}, \qquad \{\gamma = 1, 2, \ldots, M\},$$

ce qui est absurde.

19° Théorème. — *Pour l'équivalence de deux formes* F *et* G, *de même degré, il faut et il suffit que les invariants correspondants soient égaux, ou les résiduelles* $\overline{F}$ *et* $\overline{G}$ *identiques.*

Soient, en effet, $\{a_\alpha, b_\alpha = \text{invariants}\}$,

$$\overline{F} = \sum_{\alpha} a_\alpha \Phi_\alpha, \qquad \overline{G} = \sum_{\alpha} b_\alpha \Phi_\alpha,$$

$$F \equiv \overline{F}, \qquad G \equiv \overline{G} \qquad (\text{mod}\,\omega).$$

Par hypothèse et en vertu de 18°

$$G - F \equiv \overline{G} - \overline{F} \equiv \overline{(G - F)} \equiv \sum_{\alpha} (a_\alpha - b_\alpha)\Phi_\alpha \equiv 0 \qquad (\text{mod}\,\omega).$$

Donc $F - G$, pour être $\equiv 0 \,(\text{mod}\,\omega)$, doit avoir tous ses invariants $a_\alpha - b_\alpha$ nuls.

$$b_\alpha \equiv a_\alpha, \qquad \overline{F} = \overline{G}. \qquad \text{C. Q. F. D.}$$

20° Soit R une matrice $\mathfrak{M}(m)$-aire, à coefficients constants, $|R| \neq 0$.

La résiduelle $\overline{F} = \sum_{\alpha} a_\alpha \Phi_\alpha$ ne change pas quand on effectue :

Sur les invariants a_α la collinéation R;

Sur les résiduelles élémentaires Φ_α la collinéation R'^{-1}, inverse de la transposée de R.

Les invariants et les résiduelles élémentaires ne sont définis qu'à une collinéation $\mathfrak{M}(m)$-aire près.

21° Soit

$$S = [s_{ij}], \qquad \{i, j = 1, 2, \ldots, n\}, \qquad |S| \neq 0,$$

une matrice n-aire.

Par hypothèse, la collinéation S admet pour invariant absolu la forme quadratique ω. Comme ω, au choix des variables près, est une somme de n carrés, S est, au choix aussi des variables près, une matrice orthogonale.

Posons $z = S[y]$, c'est-à-dire

$$z_i = \sum_{j} s_{ij} y_j,$$

$$F\begin{pmatrix} m \\ z; a \end{pmatrix} = F(S[y]; a) = \mathfrak{F}\begin{pmatrix} m \\ y; b \end{pmatrix}.$$

On a évidemment

$$[\lambda, \lambda' = 1, 2, \ldots, \varphi(m)],$$

$$b_\lambda = \sum_{\lambda'} p_{\lambda\lambda'} a_{\lambda'}, \qquad b = P[a],$$

$P = [p_{\lambda\lambda'}]$ étant une matrice $\varphi(m)$-aire, dont le coefficient $p_{\lambda\lambda'}$ est, par rapport aux s_{ij}, une forme de degré m.

Les invariants b_α de $\mathfrak{F}$ se construisent avec les b,

comme les invariants a_α de F se construisent avec les a, c'est-à-dire linéairement. D'autre part (14°), les a s'expriment linéairement avec les a_α et $\varphi(m-2)$ autres paramètres a'_μ, $\{\mu = 1, 2, \ldots, \varphi(m-2)\}$. Comme $b = P[a]$, on a finalement

$$(o) \qquad b_\alpha = \sum_{\alpha'} h_{\alpha\alpha'} a_{\alpha'} + \sum_{\mu} g_{\alpha\mu} a'_\mu,$$

$$\{h_{\alpha\alpha'}, g_{\alpha\mu} = \text{const.}; \qquad \alpha', \alpha = 1, 2, \ldots, \mathfrak{M}(m)\}.$$

Pour que $\omega(y)$ divise $\mathfrak{F}(y)$, il faut et il suffit que $\omega(z)$ divise $F(z)$. Ainsi dans (o), dès que tous les a sont nuls, les b_α doivent tous s'évanouir, pour tout choix des indéterminées a'_μ. De là déjà $g_{\alpha\mu} = o$.

Mais les invariants b ne peuvent s'évanouir tous que si les a s'évanouissent tous, donc le déterminant des $h_{\alpha\alpha'}$ est différent de zéro.

En résumé, $b = H[a]$, où $H = [h_{\alpha\alpha'}]$ est une matrice $\mathfrak{M}(m)$-aire avec $|H| \not\equiv o$.

Ainsi, *le changement de variables* $z = S[y]$ *se traduit sur les invariants par une collinéation* $\mathfrak{M}(m)$-aire H. Cela (20°) peut être considéré comme indifférent.

La propriété des formations $a_\alpha(a)$ est donc projective; de là leur nom d'*invariants*.

22° On a nommé, au 17°, *résiduelle* $\mathfrak{R}_{mn}$ toute combinaison linéaire, homogène, à coefficients constants des résiduelles élémentaires Φ. Il est évident que la résiduelle $\mathfrak{R}_{mn} \equiv \Sigma K \Phi$ ne peut devenir $\equiv o \pmod{\omega}$ qu'en s'évanouissant identiquement avec toutes les constantes K.

23° On a (16°)

$$F = \overline{F} + \omega Q = \mathfrak{R}_{mn} + \omega Q \binom{m-2}{z};$$

à son tour

$$Q\binom{m-2}{z} = \mathfrak{R}_{m-2,n} + \omega\, Q_1\binom{m-4}{z},$$

et ainsi de suite. Bref

$$F = \sum_{s=0}^{s=\sigma} \omega^s \mathfrak{R}_{m-2s,n},$$

σ étant $\frac{1}{2}m$ ou $\frac{1}{2}(m-1)$ suivant que m est pair ou impair.

Écrire F sous cette expression c'est *ordonner* F *par rapport aux puissances croissantes de* ω.

L'opération est univoque.

Admettons, en effet, qu'on ait à la fois

$$F = A_0 + A_1\omega + A_2\omega^2 + \ldots = B_0 + B_1\omega + \ldots.$$

Il vient

$$A_0 - B_0 \equiv 0 \pmod{\omega};$$

mais $A_0 - B_0$ est une résiduelle $\mathfrak{R}_{mn}$, donc (22°) $A_0 = B_0$. Après départ de ω, on aurait de même

$$A_1 - B_1 = \mathfrak{R}_{m-2,n} \equiv 0 \pmod{\omega} \quad \text{et} \quad A_1 = B_1, \ldots.$$

C. Q. F. D.

CHAPITRE III.

Domaine holoïde Ω, *complet et bien défini.*

24° Posons, comme au 2°,

$$\omega = z_1 z_2 - \zeta, \qquad -\zeta = z_3 z_4 + \ldots,$$

de façon que

$$z_1 z_2 \equiv \zeta \pmod{\omega}.$$

Les formes $F^{(1)}$, où z_1 manque, ou $F^{(12)}$, où z_1 et z_2 manquent simultanément, constituent (Chap. I) des domaines E_{n-1} ou E_{n-2} complets et bien définis, qui suivent les règles de l'algèbre ordinaire.

Vis-à-vis des $n-2$ variables z_3 z_4, ..., z_n, la formation $\zeta(z)$ *joue le même rôle* que la formation ω par rapport aux n variables z_1, ..., z_n.

On peut donc, toujours et d'une seule façon (23°), ordonner $F^{(12)}$ par rapport aux puissances de ζ et écrire

$$F^{(12)} = A_0 + \zeta A_1 + \zeta^2 A_2 + \ldots,$$

les A étant des *résiduelles* aux $n-2$ variables z_2, ..., z_n.

Entre expressions $F^{(1)}$ ou $F^{(12)}$ toute congruence (mod ω) est une égalité ordinaire.

25° Pour diminuer les accumulations d'indices, je poserai

$$z_1 = x, \qquad z_2 = t,$$

et j'étudierai la divisibilité (mod ω) d'une forme F par le facteur t, lequel est (10°) irréductible (mod ω). Je montrerai que t est aussi (10°) premier (mod ω).

26° Mettons, dans F, t en facteur dans les termes qui le contiennent; on aura

$$F = t(\ldots\ldots) + F_1.$$

F_1 ne contient pas t; c'est donc un polynome en x, à coefficients du type $F^{(12)}$. Chacun de ces coefficients peut être ordonné par rapport aux puissances de ζ (24°) et l'on écrira

$$(1) \qquad \begin{cases} F = t(\ldots) + \zeta(\ldots) + F', \\ F' = x^\rho A_\rho + x^{\rho-1} A_{\rho-1} + \ldots, \end{cases}$$

où les A sont des *résiduelles,* par rapport à ζ, à $n-2$ variables $z_3, \ldots, z_n$.

L'expression F′ est permanente (5°), car elle ne change pas si l'on ajoute à F l'expression

$$\omega P = (xt - \zeta) P.$$

27° Lemme. — *Pour que* F *soit divisible* (mod ω) *par t, il faut et il suffit que* F′ *s'évanouisse identiquement.*

La condition est suffisante, en se reportant à la formule (1) du 26°, puisque $\zeta \equiv xt \pmod{\omega}$.

Montrons que la condition $F' = 0$ est nécessaire. Si t divise (mod ω) F, on a

$$F = t(\ldots) + \omega(\ldots) = t(\ldots) + \zeta(\ldots).$$

$F = 0$ pour $t = \zeta = 0$, quel que soit x.

La formule (1) du 26° montre que F′ doit s'évanouir, pour toute valeur de x, dès que $\zeta = 0$.

ζ étant irréductible (2°), divise donc A_ρ, $A_{\rho-1}$, ...; ces expressions sont des résiduelles vis-à-vis de ζ. Alors

$$A_\rho = A_{\rho-1} = \ldots = 0, \qquad F' = 0. \qquad \text{C. Q. F. D.}$$

28° Théorème. — *Si t ne divise* (mod ω) *ni* A, *ni* B, *t ne saurait diviser* (mod ω) *le produit* AB, autrement dit : *le facteur t est premier* (mod ω).

Appliquons à A et B la formule (1) du 26° et écrivons :

$$\begin{aligned} A &= t(\ldots) + \zeta(\ldots) + A', \\ B &= t(\ldots) + \zeta(\ldots) + B', \\ A' &= x^\rho A_\rho + x^{\rho-1} A_{\rho-1} + \ldots, \\ B' &= x^\sigma B_\sigma + x^{\sigma-1} B_{\sigma-1} + \ldots, \end{aligned}$$

où les $A_\rho, \ldots, B_\sigma, \ldots$ sont des résiduelles par rapport aux $n-2$ variables $z_3, \ldots, z_n$.

Comme t ne divise (mod ω) ni A ni B, on a (27°) $A' \not\equiv 0$, $B' \not\equiv 0$ et, en particulier, $A_\rho \not\equiv 0$, $B_\sigma \not\equiv 0$.

Or

$$AB = t(\ldots) + \zeta(\ldots) + A'B',$$
$$A'B' = x^{\rho+\sigma} A_\rho B_\sigma + x^{\rho+\sigma-1}(\ldots) + \ldots.$$

Si t divise (mod ω) le produit AB, on a (27°) $AB \equiv 0$ pour $t = \zeta = 0$ *quel que soit* x.

$A'B' = 0$ pour $\zeta = 0$ quel que soit x; notamment $A_\rho B_\sigma = 0$ pour $\zeta = 0$. Nous sommes en algèbre ordinaire; ζ, qui est un facteur irréductible et premier, doit diviser le produit $A_\rho B_\sigma$ sans diviser par hypothèse ni A_ρ, ni B_σ. Si, en effet, ζ divisait les résiduelles A_ρ ou B_σ, on aurait $A_\rho = 0$ ou $B_\sigma = 0$, ce qui est contre l'hypothèse.

Bref, t ne peut diviser (mod ω) le produit AB.

C. Q. F. D.

t étant (mod ω) à la fois irréductible et premier, le diviseur t se comporte, dans le domaine Ω, suivant les règles de l'arithmétique ordinaire.

29° Désignons :

Par des majuscules latines A, B, C, ... des formes de Ω, *non divisibles* (mod ω) *par* t;

Par des minuscules grecques $\alpha, \beta, \gamma, \ldots$ des entiers non négatifs;

Par des minuscules latines $a, b, c, \ldots$ des formes du type $F^{(1)}$ (c'est-à-dire où $x = z_1$ ne figure pas), *non divisibles par* t.

Je dis que dans une relation

$$(o) \quad t^\alpha A \binom{m}{z} \equiv a \binom{m+\alpha}{z}, \quad \text{ou} \quad A \equiv \frac{a}{t^\alpha} \pmod{\omega}$$

supposée existante, *chacune des expressions* A *ou* a, *supposée donnée, définit sans ambiguïté l'autre expression, ainsi que l'exposant* α.

I. Donnons-nous A et supposons un instant qu'on ait à la fois, $\alpha' \geqq \alpha$,

$$t^{\alpha}\mathrm{A} \equiv a \qquad \text{et} \qquad t^{\alpha'}\mathrm{A} \equiv a' \pmod{\omega};$$

il viendrait, puisque a et a' sont du type $\mathrm{F}^{(1)}$,

$$t^{\alpha'}a \equiv t^{\alpha}a' \pmod{\omega}, \qquad a' = t^{\alpha'-\alpha}a.$$

Or t ne divise pas a'; alors $\alpha' = \alpha$, $a' = a$.

C. Q. F. D.

II. Donnons-nous a et admettons qu'on ait à la fois

$$a \equiv t^{\alpha}\mathrm{A} \equiv t^{\alpha'}\mathrm{A}' \pmod{\omega}; \qquad \alpha' \geqq \alpha.$$

Il viendrait

$$\mathrm{A} \equiv t^{\alpha'-\alpha}\mathrm{A}' \pmod{\omega};$$

cela est absurde pour $\alpha' - \alpha \neq 0$, puisque t ne divise pas (mod ω) la forme A.

Donc $\alpha' = \alpha$ et

$$\mathrm{A}' \equiv \mathrm{A} \pmod{\omega}.$$

A est définie, dans le domaine Ω, à l'équivalence près, c'est-à-dire sans ambiguïté.

La relation

$$a \equiv t^{\alpha}\mathrm{A} \pmod{\omega}$$

établit donc entre les expressions A, d'une part, et a, d'autre part, *une correspondance biunivoque.*

30° Construisons A, connaissant a. Grâce aux explications des 26° et 27°, on connaîtra l'exposant,

entier et non négatif α, tel que a admette pour diviseur (mod ω) t^α, mais non plus $t^{\alpha+1}$. Alors A est le quotient (mod ω) de a par t^α.

Construisons a, connaissant A. Ordonnons A par rapport aux puissances décroissantes de $z_1 = x$,

$$A = x^p K + x^{p-1} K_1 + \dots \qquad \{ \text{les K du type } F^{(1)} \}.$$

On peut admettre que $t = z_2$ ne divise pas K. En effet, si $K = tL$, on a, puisque $\omega = tx - \zeta$,

$$\begin{aligned} A &= x^{p-1} L tx + x^{p-1} K_1 + \dots \\ &= x^{p-1} L(\omega + \zeta) + x^{p-1} K_1 + \dots \\ &\equiv x^{p-1} \{ L\zeta + K_1 \} + \dots \qquad (\text{mod}\,\omega). \end{aligned}$$

Eu égard à l'équivalence, l'exposant maximum de x serait $p-1$ et non pas p, et ainsi de suite.

Bref, on admettra que t ne divise pas K et l'on écrira

$$\begin{aligned} A &= x^\alpha K + x^{\alpha-1} K_1 + \dots, \\ t^\alpha A &= (tx)^\alpha K + t(tx)^{\alpha-1} K_1 + \dots \\ &\equiv \zeta^\alpha K + \zeta^{\alpha-1} t K_1 + \dots \equiv a \qquad (\text{mod}\,\omega), \end{aligned}$$

a est bien du type $F^{(1)}$; a n'est pas divisible par t, puisque K ne l'est pas.

Les procédés ci-dessus fournissent un certain a partant d'un A donné, ou un certain A partant d'un a donné. Mais on sait (29°) que A et a se définissent mutuellement sans ambiguïté; donc *la correspondance biunivoque est effectivement réalisée,* entre les expressions (29°) A, B, C, ... et a, b, c, ... qui seront dites *correspondantes* A avec a, B avec b, ... par la relation

$$t^\alpha A \equiv a, \qquad \text{ou} \qquad A \equiv \frac{a}{t^\alpha} \qquad (\text{mod}\,\omega).$$

31° Théorème. — *Pour que* A *divise* (mod ω) *la forme* C, *il faut et il suffit que a divise c.*

I. *La condition est nécessaire.* — En effet, s'il existe une forme B telle que $C \equiv AB \pmod{\omega}$, on aurait

$$\pmod{\omega} \begin{cases} a \equiv t^{\alpha} A, \quad b \equiv t^{\beta} B, \quad c \equiv t^{\gamma} C; \\ t^{\alpha+\beta+\gamma} C \equiv t^{\alpha+\beta} c \equiv t^{\alpha+\beta+\gamma} AB \equiv t^{\gamma} ab; \\ t^{\alpha+\beta} c \equiv t^{\gamma} ab \quad (\mathrm{mod}\,\omega), \end{cases}$$

et, comme nous sommes dans le type F(1),

$$t^{\alpha+\beta} c = t^{\gamma} ab;$$

t ne divise ni a, ni b, ni c; donc $\gamma = \alpha + \beta$ et a divise c, puisque $c = ab$.

II. *La condition est suffisante.* — Nommons b le quotient $c : a$ et B la forme telle que $t^{\beta} B \equiv b \pmod{\omega}$.

Il viendra

$$c = ab \equiv t^{\gamma} C \equiv t^{\alpha+\beta} AB \left\{ \pmod{\omega}. \right.$$
$$t^{\gamma} C \equiv t^{\alpha+\beta} AB \left\{ \right.$$

Si $\gamma < \alpha + \beta$, t divise (mod ω) la forme C, ce qui est absurde.

Si $\gamma > \alpha + \beta$, t divise (mod ω) le produit AB. Or t est un facteur premier (mod ω); t doit diviser (mod ω) soit A, soit B, ce qui n'est pas. Alors $\gamma = \alpha + \beta$,

$$C \equiv AB \pmod{\omega}. \qquad \text{C. Q. F. D.}$$

32° Soient :

deux formes de Ω, A et B, non divisibles (mod ω) par t, telles que

$$a \equiv t^{\alpha} A, \quad b \equiv t^{\beta} B \pmod{\omega};$$

d, le p. g. c. d. des deux formes a et b du type $F^{(1)}$; ce d existera toujours, car le domaine des formes $F^{(1)}$ est complet; t, ne divisant ni a, ni b, ne divise pas d;

D, la forme de Ω telle que

$$t^{\delta} D \equiv d \pmod{\omega}.$$

Je dis que D *est le p. g. c. d.* (mod ω) *de* A *et* B.

En effet, puisque d divise a et b, D divise (mod ω) tant A que B (31°).

Soit d'autre part D', avec

$$t^{\delta'} D' \equiv d' \pmod{\omega},$$

un diviseur (mod ω) quelconque, commun à A et B. En vertu de 31°, d' divise a et b et aussi d, qui est leur p. g. c. d. Donc, toujours d'après 31°, D' divise (mod ω) la forme D.

D est donc bien le p. g. c. d. (mod ω) cherché des deux formes A et B.

La construction de D s'effectue par des opérations déjà décrites, connues et en nombre fini.

On retiendra donc ceci :

Deux formes A et B prises à volonté dans Ω, mais dont aucune n'est divisible (mod ω) par le facteur t, admettent toujours (mod ω) un p. g. c. d. D, lequel non plus n'est pas divisible (mod ω) par le facteur t.

33° Pour avoir deux formes *tout à fait quelconques* dans Ω, prenons

$$\left.\begin{aligned} L &\equiv t^{\lambda} A \\ M &\equiv t^{\mu} B \end{aligned}\right\} \pmod{\omega}, \qquad \text{avec} \qquad \lambda \leqq \mu.$$

Nommons D le p. g. c. d. (mod ω) de A et B obtenu

par la méthode du 32°, et posons

$$A \equiv PD, \qquad B \equiv QD \qquad (\mathrm{mod}\,\omega).$$

Écrivons enfin

$$\Delta \equiv t^{\lambda} D \qquad (\mathrm{mod}\,\omega).$$

Je dis que L *et* M *admettent* Δ *pour p. g. c. d.* $(\mathrm{mod}\,\omega)$.

Cela suffit pour établir que le domaine Ω est complet et bien défini.

I. Δ *est* $(\mathrm{mod}\,\omega)$ *un diviseur commun à* L *et* M.

Cela devient évident si l'on écrit

$$\left.\begin{aligned} L &\equiv t^{\lambda} A \equiv t^{\lambda} PD \equiv \Delta P \\ M &\equiv t^{\mu} B \equiv t^{\mu} QD \equiv \Delta t^{\mu-\lambda} Q \end{aligned}\right\} (\mathrm{mod}\,\omega).$$

II. *Toute forme* $\Delta' \equiv t^{\rho} R$, $\rho \geqq 0$, *qui est* $(\mathrm{mod}\,\omega)$ *un diviseur commun à* L *et* M, *divise* $(\mathrm{mod}\,\omega)$ *aussi la forme* Δ.

Écrivons

$$\left.\begin{aligned} L &\equiv t^{\lambda} A \equiv \Delta' t^{\sigma} S \\ M &\equiv t^{\mu} B \equiv \Delta' t^{\tau} T \end{aligned}\right\} (\mathrm{mod}\,\omega),$$

où $t^{\sigma} S$ et $t^{\tau} T$ sont les quotients $(\mathrm{mod}\,\omega)$ L:Δ' et M:Δ'; ou bien

$$\left.\begin{aligned} t^{\lambda} A &\equiv t^{\rho+\sigma} SR \\ t^{\mu} B &\equiv t^{\rho+\tau} TR \end{aligned}\right\} (\mathrm{mod}\,\omega).$$

Le facteur t, qui est $(\mathrm{mod}\,\omega)$ à la fois irréductible et premier, ne divise $(\mathrm{mod}\,\omega)$ ni A, ni B, ni R, ni S, ni T.

Donc

$$\rho = \lambda - \sigma = \mu - \tau, \qquad A \equiv RS \quad \text{et} \quad B \equiv RT \qquad (\mathrm{mod}\,\omega).$$

Par suite, $\rho \leqq \lambda$, R est $(\mathrm{mod}\,\omega)$ un diviseur de D (en

vertu du 32°), et

$$\Delta' \equiv l^{\rho} R$$

est (mod ω) un diviseur de $\Delta \equiv l^{\lambda} D \pmod{\omega}$.

C. Q. F. D.

34° J'ai ainsi achevé la démonstration du théorème annoncé dans l'Introduction.

On a exclu toutefois les cas (2°) où ζ n'est pas irréductible, c'est-à-dire

$$n = 4, \quad -\zeta = z_3 z_4,$$
$$n = 3, \quad -\zeta = z_3^2.$$

Ces cas appellent une discussion spéciale, que je publierai ultérieurement.