Scriptum 2

Mathematisch Centrum 2e Boerhaavestraat 49,
Amsterdam.

LE THEOREME FONDAMENTAL DE L'ALGEBRE SANS AXIOME DE CONTINUITE.

J.G. van der Corput.

Introduction.

Soit Φ un corps commutatif ordonné, c'est-à-dire que l'ordre est transitif et que les inégalités $a>0$ et $b>0$ entraînent $a+b>0$ et $ab>0$. Nous construirons un corps ordonné Ω, contenant tous les éléments de Φ tel que chaque polynome, dont les coefficients appartiennent à $\Omega(i)$ puisse être décomposé en facteurs linéaires dont les coefficients sont des éléments de $\Omega(i)$. Autrement dit: $\Omega(i)$ contient toutes les racines de toutes les équations algébriques dont les coefficients appartiennent à $\Omega(i)$. Nous construirons le corps Ω de telle facon qu'inversement chaque élément de $\Omega(i)$ soit la racine d'une équation algébrique, dont les coefficients appartiennent au corps donné Φ. Nous dirons que $\Omega(i)$ est formé par les quantités qui sont algébriques par rapport à Φ. Nous appellerons les éléments de Ω réels. C'est seulement une conventionsanalogue à la convention usuelle dans le cas particulier où Φ est le corps des nombres rationnels. Ainsi Ω est le corps formé par les quantités réelles qui sont algébriques par rapport à Φ.

Il faut remarquer qu'aucune condition relative

à la continuité n'est nécessaire. Il y a trois ans [1]) j'ai donné une démonstration sous la condition supplémentaire que le corps donné Φ satisfait à l'axiome d'Archimède. Dans la version donnée ci-dessous les démonstrations sont beaucoup plus simples que dans mon raisonnement antérieur. J'y admets seulement des notions, qui peuvent être vérifiées par un nombre fini d'opérations, de sorte que par exemple la notion de réductibilité d'un polynome n'est pas admise.

A la fin de cet article je me placerai au point de vue intuitioniste. J'introduis des suites convergentes $a^* = (a_0, a_1, \ldots)$, dont les éléments appartiennent à $\Omega(i)$. Ces suites convergentes a^* forment un anneau Ω^* avec la propriété suivante: Chaque polynome, dont les coefficients appartiennent à Ω^* et dont au moins un coefficient est différent de zéro, peut être décomposé en facteurs linéaires dont les coefficients appartiennent à Ω^*. Si dans le polynome $A^*(X)$ de degré n le coefficient de X^σ et celui de X^τ sont différents de zéro avec $0 \leqq \sigma \leqq \tau \leqq n$ et si μ désigne un entier $\geqq \sigma$ et $\leqq \tau$,

---

[1]) Proc.Kon.Ak.v.Wetensch. 7 (1946) 722-732; 8 (1946) 878-886; 9 (1946) 985-994
Indag.math. 8,4 (1946), 430-440; 8,4 (1946) 549-557; 8,5 (1946), 605-614.

on a

$$A^*(X) = c^*(X - \alpha_1^*)\ldots(X - \alpha_\mu^*)(1 - \beta_{\mu+1}^* X)\ldots(1 - \beta_n^* X),$$

où c^*, $\alpha_1^*, \ldots, \alpha_\mu^*$, $\beta_{\mu+1}^*, \ldots, \beta_n^*$ sont des éléments de Ω^* et où c^* est différent de zéro.

Si Φ est l'ensemble des nombres rationnels, alors Ω est l'ensemble des nombres algébriques réels, $\Omega(i)$ est l'ensemble des nombres algébriques complexes et Ω^* l'ensemble de tous les nombres complexes. Comme cas particulier on obtient donc non seulement dans les mathématiques traditionelles mais aussi dans les mathématiques intuitionistes ') le théorème:

') Cf. H. Weyl, Randbemerkungen zu Hauptproblemen der Mathematik, Math.Zeitschr. 19 (1934) 131-150.

B. de Loor, Die hoofstelling van die algebra van intuïtionistiese standpunt, Diss. Amsterdam (1925), 63 p.

L.E.J. Brouwer et B. de Loor, Intuitionistischer Beweis des Fundamentalsatzes der Algebra, Proc. Kon.Ak.v.Wetensch. 27 (1924) 186-188. Le même article en hollandais: Intuïstionistisch bewijs van de hoofdstelling der algebra, Versl.Kon.Ak. v.Wetensch. 33 (1924) 82-84

L.E.J. Brouwer, Intuitionistische Ergänzung des Fundamentalsatzes der Algebra, Proc.Kon.Ak.v. Wetensch. 27 (1924), 631-634.

Le même article en hollandais: Intuitionistische aanvulling van de hoofdstelling der algebra, Versl.Kon.Ak.v.Wetensch. 33 (1924) 459-462.

Chaque polynome à coefficients complexes peut être décomposé en facteurs linéaires à coefficients complexes.

J'appelle polynome simple un polynome qui est premier avec sa dérivée, c'est-à-dire un polynome dont le plus grand diviseur commun avec sa dérivée est égal à une constante $\neq 0$.

Je dis qu'un corps ordonné Ψ possède la propriété E_n, n désignant un nombre naturel, si à tout polynome A(X), non identiquement nul, de degré inférieur ou égal à n et dont les coefficients appartiennent à Ψ, on peut faire correspondre des éléments $y_1, \ldots, y_q$ de Ψ, tels que

1) $A(y_1) = \ldots = A(y_q) = 0$;

2) Dans chacun des q+1 intervalles déterminés dans Ψ par $y_1, \ldots, y_q$ le polynome A(X) est toujours positif, ou toujours négatif.

3) Si A(X) est un polynome simple les signes de A(X) dans deux intervalles consécutifs sont opposés.

Chaque corps ordonné possède la propriété E_1. Je dis que Ψ est une extension d'un corps commutatif ordonné Φ, si Ψ est un corps commutatif ordonné, qui contient tous les éléments de Φ. Tout

bord je vais donner une méthode qui permet de
truire pour tout nombre naturel n et pour cha-
corps commutatif ordonné Φ une extension Ψ,
possède la propriété E_n. Ce procédé satisfait
conditions suivantes:
Si Φ^* est un souscorps de Φ la méthode donne
ne extension de Φ^* un souscorps Ψ^* de Ψ, tel
dans Ψ^* l'ordre, l'addition et la multiplication
t les mêmes que dans Ψ,
Chaque élément de Ψ satisfait à une équation
ébrique dont les coefficients sont des éléments
Φ.
s la construction d'une extension Ψ de Φ ayant
propriété E_n je peux supposer $n \geq 2$, car pour
1 je choisis $\Psi = \Phi$. Pour la construction j'au-
besoin de l'identité suivante:
Si m désigne un nombre naturel quelconque, il
possible de trouver $2^m + 1$ nombres positifs ra-
nnels $c_{m,h}$ $(h = 0, 1, \ldots, 2^m)$ avec $c_{m,h} = c_{m,2^m-h}$ et
$\leq c_{m,h} \leq c_{m,1}$ tels que l'identité

$$f(a+\ell) - f(a) = \ell \sum_{h=0}^{2^m}{}' c_{m,h} f'(a + \frac{h\ell}{2^m})$$

t valable pour chaque polynome f(x) de degré <
m + 2, dont les coefficients appartiennent à un
ps commutatif, qui contient aussi les éléments
t ℓ. Le prime du $\sum$ signifie que dans les termes
c h = 0 et avec $h = 2^m$ on doit remplacer $c_{m,0}$
$c_{m,2^m}$ par $\frac{c_{m,0}}{2}$ et $\frac{c_{m,2^m}}{2}$.

L'identité (1) est évidente pour m = 1, puisqu'on a pour chaque polynome de degré < 4, la formule des 3 niveaux:

$$f(a+\ell)-f(a)=\ell\left\{\frac{1}{6}f'(a)+\frac{2}{3}f'(a+\frac{\ell}{2})+\frac{1}{6}f'(a+\ell)\right\},$$

d'où il suit que dans le cas m = 1 on peut prendre $c_{1,0}=\frac{1}{3}$; $c_{1,1}=\frac{2}{3}$; $c_{1,2}=\frac{1}{3}$

Supposons que l'identité (1) soit démontrée pour m; nous allons la démontrer pour m + 1.

Un polynome g(X) de degré < 2m + 4 peut être écrit sous la forme

$$g(X)=p(X-a-\frac{\ell}{2})^{2m+3}+q(X-a-\frac{\ell}{2})^{2m+2}+f(X),$$

où f(X) est de degré < 2m + 2. Si nous remplaçons dans l'identité (1) le polynome f(X) par g(X), les deux membres sont augmentés respectivement de $u_m p\ell^{2m+3}$ et de $v_m q\ell^{2m+3}$ où u_m et v_m dépendent seulement de m de sorte que (1) devient

$$(2)\quad g(a+\ell)-g(a)=\ell\sum_{h=0}^{2^m}{}'\, c_{m,h}\, g'(a+\frac{h\ell}{2^m})+(u_m p-v_m q)\ell^{2m+3}$$

En remplaçant ℓ par $\frac{1}{2}\ell$, nous obtenons

$$g(a+\frac{\ell}{2})-g(a)=\frac{\ell}{2}\sum_{h=0}^{2^m}{}'\, c_{m,h}\, g'(a+\frac{h\ell}{2^{m+1}})+(u_m p-v_m q)(\frac{\ell}{2})^{2m+3}$$

et en remplaçant ensuite a par $a+\frac{\ell}{2}$ nous trouvons

$$g(a+\ell)-g(a+\tfrac{\ell}{2}) = \frac{\ell}{2} \sum_{h=0}^{2^m}{}' c_{m,h}\, g'(a+\tfrac{\ell}{2}+\frac{h\ell}{2^{m+1}}) +$$

$$+ (u_m p - v_m q)\left(\frac{\ell}{2}\right)^{2m+3},$$

donc

$$(3)\quad g(a+\ell)-g(a) = \frac{\ell}{2} \sum_{h=0}^{2^{m+1}}{}' \gamma_{m,h}\, g'(a+\frac{h\ell}{2^{m+1}}) + 2(u_m p - v_m q)\left(\frac{\ell}{2}\right)^{2m+3}$$

où $\gamma_{m,h} = c_{m,h}$ si $h < 2^m$;

$\gamma_{m,h} = c_{m,h-2^m}$ si $h > 2^m$

et

$\gamma_{m,h} = \frac{1}{2}(c_{m,0} + c_{m,2^m})$ si $h = 2^m$

Par conséquent $\gamma_{m,k} = \gamma_{m,2^{m+1}-k}$ et

$$0 < \gamma_{m,2} \leq \gamma_{m,h} = \gamma_{m,1} \quad (h=0,1,\ldots,2^{m+1})$$

Si nous multiplions les deux membres de (3) par 2^{2m+2} et si nous retranchons ensuite membre à membre de (2) nous obtenons, après division par $M = 2^{2m+2} - 1$,

$$g(a+\ell)-g(a) = \ell \sum_{h=0}^{2^{m+1}}{}' c_{m+1,h}\, g'(a+\frac{h\ell}{2^{m+1}})$$

où $Mc_{m+1,h} = 2^{2m+1}\gamma_{m,h}$, si h est impair

$= 2^{2m+1}\gamma_{m,h} - c_{m,\frac{1}{2}h}$, si h est pair.

Ainsi nous trouvons pour h impair

$$Mc_{m+1,h} = 2^{2m+1}\gamma_{m,h} \begin{cases} \leq 2^{2m+1}\gamma_{m,1} = Mc_{m+1,1} \\ \geq 2^{2m+1}\gamma_{m,2} > Mc_{m+1,2} > 0 \end{cases}$$

et pour h pair

$$Mc_{m+1,h} = 2^{2m+1}\gamma_{m,h} - c_{m,\frac{h}{2}} \begin{cases} \leqq 2^{2m+1}\gamma_{m,1} = Mc_{m+1,1} \\ \geqq 2^{2m+1}\gamma_{m,2} - c_{m,1} = \end{cases}$$

$$= Mc_{m+1,2} > 0$$

Ainsi l'identité (1) est démontrée, ce qui nous permet d'énoncer le théorème suivant:
Soit $\sum$ un corps commutatif ordonné, contenant 2 éléments y et z avec $y < z$ et soit $F(X)$ un polynome non constant, dont les coefficients appartiennent à $\sum$ tel que $F'(s)$ soit $\geqq 0$ pour chaque élément s de $\sum$ dans l'intervalle $y \leqq s \leqq z$. Alors dans cet intervalle $F(X)$ est une fonction toujours croissante. En effet nous pouvons appliquer l'identité avec $\ell > 0$ de telle manière que le nombre des termes figurant dans le membre de droite surpasse le degré de $F'(X)$; alors au moins un des ces termes est positif, donc $F(a+\ell) - F(a) > 0$.

De la même manière on obtient le résultat suivant:
Soit $\sum$ un corps commutatif ordonné contenant 2 éléments y et z avec $y < z$ et soit $F(X)$ un polynome non constant, dont les coefficients appartiennent à $\sum$ tel que $F'(s)$ soit $\leqq 0$ pour chaque élément s de $\sum$ dans l'intervalle $y \leqq s \leqq z$. Alors dans cet intervalle $F(X)$ est une fonction toujours décroissante.

Soit $\sum$ un corps possédant la propriété E_{n-1} tel que chaque élément de $\sum$ satisfait à une équation algébrique dont les coefficients appartiennent à Φ
Au moyen des résultats trouvés je vais construire

un corps $\sum(\alpha)$ dont je dis qu'il s'obtient à partir de $\sum$ par adjonction du symbole α. Ce symbole est défini au moyen d'un polynome simple

$$A(X) = X^n + a_1 X^{n-1} + \ldots + a_n$$

de degré n, dont les coefficients appartiennent à $\sum$. D'après la définition de la condition E_{n-1} le corps $\sum$ contient des racines $y_1 < y_2 \ldots < y_q$ de $A'(X)$ où $0 \leqq q \leqq n-1$; ces racines divisent $\sum$ en q+1 intervalles tels que $A'(X)$ possède dans chacun de ces intervalles un signe constant et que les signes sont toujours opposés dans deux intervalles consécutifs. Le polynome $A(X)$ ne s'annule pas aux points $y_1, \ldots y_q$, puisqu'il est simple. D'après le résultat obtenu $A(X)$ est monotone dans chacun des q+1 intervalles. Je distinguerai deux espèces d'intervalles. Dans les intervalles de première espèce $A(X)$ prend des signes opposés aux points extrêmes et dans les intervalles de seconde espèce $A(X)$ prend le même signe aux points extrêmes; je donne à $A(X)$ au point $+\infty$ le signe + et au point $-\infty$ le signe $(-1)^n$. Je choisis le polynome $A(X)$ de telle façon qu'au moins un intervalle de première espèce se présente. (Ceci est toujours le cas si le degré de $A(X)$ est impair)

J'introduis un couple $\alpha = [A(X), J]$, où J est un intervalle de première espèce et je dis que α est une racine réelle de $A(X)$, situé à l'intérieur de J.

Je dis qu'α est supérieur à tout élément s de $\sum$, situé à gauche de J et que α est inférieur à tout

élément s de Σ situé à droite de J. Pour définir la situation de α par rapport à un élément s de J je distingue deux cas différents:

1° Soit A(X) une fonction croissante dans J. Alors je dirai que X est égal ou supérieur ou inférieur à α selon que A(X) est égal, superieur ou inférieur à 0.

2° Soit A(X) une fonction décroissante dans J. Alors j'appelle X égal, supérieur ou inférieur à α selon que A(X) est égal, inférieur ou supérieur à 0.

La définition de l'égalité de α avec un élément de Σ se justifie par le fait qu'il est impossible qu'on ait à la fois $\alpha = s$ et $\alpha = s'$, où s et s' désignent des éléments differents appartenant à Σ. En effet s et s' seraient des racines de A(X) appartenant à un même intervalle J, ce qui est impossible puisque A(X) est ou bien croissant, ou bien décroissant dans J.

Pour démontrer que l'ensemble, formé par Σ et α possède un ordre transitif, je démontre d'abord que les inégalités $\alpha < x$ et $x < y$, où x et y désignent des éléments de Σ, entraînent $\alpha < y$. La propriété est évidente, si x est situé à droite de J et aussi si y est situé à droite de J. Si x et y appartiennent tous les deux à J et si A(x) est une fonction croissante dans J, on a: $A(x) > 0$ et $A(y) > A(x)$, donc $A(y) > 0$, d'où $y > \alpha$. Le même raisonnement peut être appliqué si A(x) est une fonction décroissante dans J. De la même manière on voit que les inéga-

lités $x < \alpha$ et $\alpha < y$ entraînent $x < y$ et finalement que les inégalités $x < y$ et $y < \alpha$ impliquent $x < \alpha$

Introduisons maintenant les symboles

$$P(\alpha) = p_0\alpha^{n-1} + \ldots + p_{n-1}$$

$$Q(\alpha) = q_0\alpha^{n-1} + \ldots + q_{n-1} \qquad \text{où}$$

les coefficients appartiennent à Σ. Si le polynome $V(X) = (p_0 - q_0)X^{n-1} + \ldots$ est identiquement nul, je pose naturellement $P(\alpha) = Q(\alpha)$. Si le polynome $V(X)$ n'est pas identiquement nul, il possède dans Σ r racines réelles $u_1, u_2, \ldots, u_r$ $(0 \leq r \leq n-1)$, qui divisent Σ en r+1 intervalles tels que dans chacun d'eux $V(X)$ possède un signe constant, puisque Σ a la propriété E_{n-1}. Si α coincide avec une de ces racines, il appartient à Σ et on a $P(\alpha) = Q(\alpha)$ en vertu de $V(\alpha) = 0$. Si par contre α est situé à l'intérieur d'un des r+1 intervalles je dis que $P(\alpha)$ est supérieur où inférieur à $Q(\alpha)$ selon que $P(X)-Q(X)$ est positif ou négatif dans cet intervalle. Je dois montrer que cette dernière définition n'est pas en contradiction avec la définition antérieure dans le cas particulier où un des deux polynomes $P(X)$ et $Q(X)$ est égal à X et l'autre égal à une constante. Considérons le cas $P(X) = X$ et $Q(X) = s$, où s est un élément de Σ et supposons $\alpha > s$ d'après la dernière définition. Alors α est situé dans l'intervalle (s,∞). Si s est situé à gauche de l'intervalle J, qui contient α, on a également $\alpha > s$ d'après la première définition. Si

par contre s et α sont situés tous les deux dans J, et si A(X) est une fonction croissante dans J, on a A(s) < A(α), donc α > s d'après la première définition. Le même raisonnement peut être appliqué si A(X) est une fonction décroissante dans J et on obtient de la même manière: Si l'inégalité α < s est valable d'après la dernière définition, elle l'est aussi d'après la première.

Les expressions P(α) forment un ensemble ordonné, c'est à dire que pour chaque couple d'expressions P(α) et Q(α) une et une seule des trois possibilités P(α) = Q(α), P(α) > Q(α) et P(α) < Q(α) se présente.
Il faut remarquer que l'inégalité P(α) $\geqq$ Q(α) reste valable, si les deux membres sont augmentés d'une même expression R(α), naturellement de degré < n.

Pour la suite de mon raisonnement les deux lemmes suivants sont importants:
LEMME: Si P(α) > Q(α), on peut trouver un intervalle qui contient α à son intérieur et dont les points extrêmes sont des éléments de $\sum$ ou $\pm\infty$, tel qu'on ait P(s) > Q(s) pour tous les éléments s de $\sum$ à l'intérieur de cet intervalle.

En effet, α est situé à l'intérieur d'un intervalle borné par $\pm\infty$ où par des racines réelles du polynome V(X); à l'intérieur de cet intervalle on a toujours V(s) > 0, donc P(s) > Q(s).

LEMME: Si l'on a $P(s) > Q(s)$ pour tous les éléments s de $\sum$ appartenants à un intervalle borné par $\pm\infty$ ou par des éléments de $\sum$ et si α est situé dans cet intervalle on a $P(\alpha) > Q(\alpha)$.

La proposition est évidente si α appartient à $\sum$ Si α n'y appartient pas, le cas $P(\alpha) = Q(\alpha)$ est exclu et l'inégalité $P(\alpha) < Q(\alpha)$ également, puisque cette inégalité entraînerait $P(s) < Q(s)$ pour les éléments s de $\sum$ au voisinage de α.

L'ordre de l'ensemble, formé par les expressions $P(\alpha)$ est transitif, c'est à dire que $P(\alpha) > Q(\alpha)$ et $Q(\alpha) > R(\alpha)$ entraînent $P(\alpha) > R(\alpha)$. En effet pour tous les éléments s de $\sum$ au voisinage de α on a $P(s) > Q(s)$ et $Q(s) > R(s)$, donc $P(s) > R(s)$ d'où il suit $P(\alpha) > R(\alpha)$.

Dans l'ensemble ordonné formé par les expressions de la forme $P(\alpha)$ je définis l'addition et la soustraction en posant

$$P(\alpha) + Q(\alpha) = (p_0 + q_0)\alpha^{n-1} + \ldots + (p_{n-1} + q_{n-1})$$

et

$$P(\alpha) - Q(\alpha) = (p_0 - q_0)\alpha^{n-1} + \ldots + (p_{n-1} - q_{n-1})$$

Pour justifier cette définition je dois montrer que les relations

$$P(\alpha) = U(\alpha) \text{ et } Q(\alpha) = V(\alpha) \tag{4}$$

impliquent

$$P(\alpha)+Q(\alpha) = U(\alpha)+V(\alpha) \text{ et } P(\alpha)-Q(\alpha) = U(\alpha)-V(\alpha)$$

Si les polynomes $P(X)$ et $U(X)$ sont identiques et également $Q(X)$ et $V(X)$, la propriété est évidente,

Si non, α est un élément de $\sum$ et la propriété est également vraie.

L'addition et la soustraction satisfont aux règles usuels de calcul, de sorte que les expressions $P(\alpha)$ forment un groupe additif abélien. Ce groupe abélien est ordonné, c'est à dire que les inégalités $P(\alpha) > 0$ et $Q(\alpha) > 0$ entraînent $P(\alpha) + Q(\alpha) > 0$. En effet, on a pour tous les éléments s de $\sum$ au voisinage de α $P(s) > 0$ et $Q(s) > 0$, donc $P(s) + Q(s) > 0$, d'où il suit $P(\alpha) + Q(\alpha) > 0$.

Afin de définir le produit $P(\alpha)Q(\alpha)$, je considère le reste $R(X)$ de la division du produit ordinaire $P(X).Q(X)$ par $A(X)$ suivant les puissances décroissantes et je pose par définition $P(\alpha)Q(\alpha) = R(\alpha)$.

Pour la justification de cette définition il est nécessaire de déduire $P(\alpha)Q(\alpha) = U(\alpha)V(\alpha)$ de (4). La relation à démontrer est évidente, si les deux polynomes $P(X)$ et $U(X)$ et également les deux polynomes $Q(X)$ et $V(X)$ sont identiques. Si non, α est un élément de $\sum$ et le résultat demandé découle de la relation $A(\alpha) = 0$. La multiplication satisfait aux règles usuels de calcul, de sorte que les expressions $P(\alpha)$ forment un anneau commutatif. Cet anneau est ordonné, c'est à dire les inégalités $P(\alpha) > 0$ et $Q(\alpha) > 0$ entraînent $P(\alpha)Q(\alpha) > 0$. En effet posons

(5) $\quad P(X).Q(X) = T(X).A(X) + R(X);$

les produits pointés désignant des produits ordinaires. Considérons d'abord le cas où α est une racine d'au moins un des deux polynomes $T(X)$ et $R(X)$. Alors ce polynome est identiquement nul ou α est un élément de $\sum$. Si α est un élément de $\sum$ et aussi si $T(X)$ est identiquement nul, on obtient pour la racine α de $A(X)$ l'inégalité $R(\alpha) = P(\alpha).Q(\alpha) > 0$. Si $R(X)$ est identiquement nul et si $T(\alpha) \neq 0$, on peut trouver un voisinage de α où $P(X)$, $Q(X)$ et $T(X)$ ont des signes constants d'où il suivrait que $A(X)$ ait également un signe constant dans cet intervalle ce qui est exclu à cause de $A(\alpha) = 0$. Nous pouvons donc supposer $T(\alpha) \neq 0$ et $R(\alpha) \neq 0$ de sorte que nous pouvons trouver un voisinage de α où $P(s)$ et $Q(s)$ sont positifs et où $T(s)$ et $R(s)$ ont des signes constants pour chaque élément s de $\sum$ appartenant à ce voisinage. Puisque $A(X)$ est un polynome simple ce polynome possède des signes opposés des deux cotés de α. Nous pouvons donc trouver un élément s de $\sum$ appartenant au dit voisinage où $T(s).A(s) < 0$, donc $R(s) > 0$. Parce que cette inégalité est valable pour tous les éléments s de $\sum$ appartenant au voisinage de α, on obtient $R(\alpha) > 0$. Ainsi nous trouvons dans tous les cas $P(\alpha)Q(\alpha) > 0$.

Si $A(X)$ est égal au produit ordinaire $B(X).D(X)$ de deux polynomes $B(X)$ et $D(X)$ de degré $< n$, la racine α de $A(X)$ est une racine d'au moins un de ces deux facteurs; en effet si non, ces deux facteurs $B(s)$ et $D(s)$, donc aussi $A(s)$ auraient des signes

constants au voisinage de α.

Les expressions $P(\alpha)$ ne forment pas seulement un anneau, mais même un corps. En effet supposons $P(\alpha) \neq 0$. Si les polynomes $P(X)$ et $A(X)$ sont premiers entre eux, nous pouvons trouver deux polynomes $Q(X)$ et $T(X)$ tous les deux de degré $< n$ tels que $P(X).Q(X) = T(X).A(X) + 1$, de sorte que $Q(\alpha)$ est l'élément inverse de $P(\alpha)$. Si par contre le plus grand commun diviseur $D(X)$ de $P(X)$ et $A(X)$ n'est pas constant, on a $A(X) = B(X).D(X)$, où $B(X)$ et $D(X)$ désignent des polynomes de degré $< n$; α est une racine du produit $B(X).D(X)$, donc une racine d'au moins un de ces deux facteurs, d'où il suit que α et par conséquent aussi $P(\alpha)$ appartient à $\sum$; dans ce cas $P(\alpha)$ possède même un élément inverse appartenant à $\sum$.

Nous désignerons par $\sum(\alpha)$ le corps formé par les expressions $P(\alpha)$ et nous dirons que $\sum(\alpha)$ est formé à partir de $\sum$ par adjonction de α.

Si nous partons non pas du corps $\sum$ mais d'un souscorps $\sum^*$ de $\sum$ possédant également la propriété E_{n-1} et si nous adjoignons une racine réelle α d'une équation de degré exact n dont les coefficients appartiennent à $\sum^*$, nous obtenons le corps commutatif ordonné $\sum^*(\alpha)$

Il est immédiatement clair que $\sum^*(\alpha)$ est un souscorps de $\sum(\alpha)$ et que dans ce souscorps l'ordre d'addition et de la multiplication sont les mêmes que dans $\sum(\alpha)$.

Il suit du raisonnement précédent que α est une

racine de l'équation

$$X^n + a_1 X^{n-1} + \ldots + a_n = 0,$$

dont les coefficients appartiennent à $\sum$. D'après la condition, imposée à $\sum$, chacun de ces coefficients satisfait à une équation algébrique dont les coefficients appartiennent à Φ. On sait [1]) que α et même le polynome $P(\alpha)$ satisfont également à une équation algébrique, dont les coefficients appartiennent à Φ. Cette remarque n'est pas nécessaire pour la démonstration du théorème fondamental de l'algèbre, mais nous en aurons besoin pour démontrer que tout élément du corps construit $\Omega(i)$ satisfait à une équation algébrique dont les coefficients appartiennent au corps donné Φ.

D'après notre hypothèse nous avons à notre disposition une méthode qui nous permet de construire des extensions Γ de $\sum(\alpha)$ et Γ^* de $\sum^*(\alpha)$ possédentes toutes les deux les propriétés E_{n-1} de telle facon que chaqu'élément de Γ satisfait à une équation algébrique dont les coefficients appartiennent à Φ. Nous savons que Γ^* est un souscorps de Γ avec le même ordre, la même addition et la même multiplication..

Nous pouvons répéter le procédé précédent avec Γ au lieu de $\sum$ et avec β au lieu de α, où β désigne une racine réelle d'une équation de degré

---

[1]) Cf par exemple E. Landau, Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale, Teubner '27, théorèmes 22 et 25

$(0 \leq q \leq n)$ de l'équation $A(X) = 0$ de telle manière que $y_1, \ldots, y_q$ divisent Ω en $q+1$ intervalles tels que dans chacun d'eux $A(X)$ garde un signe constant. Si le degré de $A(X)$ est impair on a $q \geq 1$. Par conséquent Ω contient au moins une racine réelle de chaque équation simple de degré impair dont les coefficients appartiennent à Ω. Cette propriété est aussi vraie pour un polynome qui n'est pas simple, puisqu'on peut décomposer un tel polynome en facteurs simples. Si le degré de $A(X)$ est impair au moins un de ces facteurs possède également un degré impair.

Gauss a montré de quelle manière on peut déduire très facilement le théorème fondamental de l'algèbre de ce resultat.

Considérons d'abord les équations du deuxième degré. Si a désigne un élément positif de Ω, ce corps Ω contient deux racines réelles $\sqrt{a}$ et $-\sqrt{a}$ de l'équation $X^2 - a = 0$, puisque Ω est divisé par la racine $X = 0$ de l'équation dérivée $2X = 0$ en deux intervalles tous les deux de première espèce.

Par conséquent Ω contient aussi les deux racines réelles de l'équation $X^2 + pX + q = 0$ à discriminant $p^2 - 4q > 0$. Si le discriminant est égal à zéro, l'équation possède une seule racine $-\frac{p}{2}$, appartenant à Ω. Si p et q appartiennent à $\Omega(i)$, le corps $\Omega(i)$ contient deux racines (coincidant ou non) de l'équation $X^2 + pX + q = 0$. En effet dans la démonstration on peut supposer $p = 0$ et si l'on pose

$X = Y + iZ$ et $\alpha = U + iV$ on obtient

$$2Y^2 = -U + \sqrt{U^2 + V^2} \geqq 0 \text{ et } 2Z^2 = U + \sqrt{U^2 + V^2} \geqq 0.$$

Démontrons ensuite que chaque équation $A(X) = X^n + \ldots + a_n$ dont les coefficients appartiennent à Ω, possède au moins une racine appartenant à $\Omega(i)$. Nous pouvons supposer que n est pair et que la propriété est déjà démontrée dans tous les cas où n est remplacé par un nombre naturel m, qui possède moins de facteurs 2 que n. Je choisis $m = \frac{1}{2}n(n-1)$.

Introduisons n quantités indéfinies $\xi_1, \ldots, \xi_n$. Soit κ un nombre entier fixe $\geqq 0$ et $\leqq m$. Les m nombres $\tau_\kappa = \xi_\rho \xi_\sigma + \kappa(\xi_\rho + \xi_\sigma)$ $(1 \leqq \sigma < \rho \leqq n)$ satisfont à une équation de la forme

$$(6) \qquad \tau^m + \beta_{1,\kappa}\tau^{m-1} + \ldots + \beta_{m,\kappa} = 0,$$

où les coefficients désignent des fonctions entières rationnelles symétriques des n quantités indéfinies $\xi_1, \ldots, \xi_n$. Par conséquent ces coefficients sont des fonctions rationnelles de

$$\alpha_1 = -\sum \xi_1, \ \alpha_2 = \sum \xi_1\xi_2, \ldots, \alpha_n = (-1)^n \xi_1 \ldots \xi_n$$

Si nous remplaçons dans ces fonctions rationnelles $\alpha_1, \alpha_2, \ldots, \alpha_n$ respectivement par $a_1, \ldots, a_n$, nous obtenons des éléments $b_{1,\kappa}, b_{2,\kappa}, \ldots, b_{m,\kappa}$ appartenant à Ω, de sorte que la substitution transforme l'équation (6) en

$$(7) \qquad \tau^m + b_{1,\kappa}\tau^{m-1} + \ldots + b_{m,\kappa} = 0.$$

D'après notre hypothèse cette équation possède au

moins une racine appartenant à $\Omega(i)$, Désignons une telle racine par t_K . La théorie des équations du deuxième degré nous a montré que chacune des équations

$$X^2 - \frac{t_K - t_\lambda}{K - \lambda} X + \frac{K t_\lambda - \lambda t_K}{K - \lambda} = 0 \quad (0 \leqq \lambda < K \leqq m)$$

possède deux racines $U_{K\lambda}$ et $U'_{K\lambda}$ appartenant à $\Omega(i)$. Il suffit de démontrer qu'au moins une de ces équations quadratiques possède au moins une racine qui satisfont également à l'équation $A(X) = 0$. Il suffit donc de démontrer que

$$\prod_{0 \leqq \lambda < K \leqq m} A(u_{K\lambda}) A(u'_{K\lambda}) = 0,$$

c'est à dire que

$$\xi = \prod_{\rho=1}^{m} \prod_{0 \leqq \lambda < K \leqq n} (u_{K\lambda} - \xi_\rho)(u'_{K\lambda} - \xi_\rho)$$

prend la valeur zéro, si l'on écrit ξ comme fonction rationelle de $\alpha_1, \ldots, \alpha_n$ et si l'on remplace ensuite ces quantités respectivement par $a_1, a_2, \ldots, a_n$. Puisque $U_{K\lambda}$ et $U'_{K\lambda}$ sont les racines des équations du deuxième degré mentionnées ci-dessus, on a

$$\xi = \prod_{\rho=1}^{m} \prod_{0 \leqq \lambda < K \leqq n} \left(\xi_\rho^2 - \frac{t_K - t_\lambda}{K - \lambda} \xi_\rho + \frac{K t_\lambda - \lambda t_K}{K - \lambda} \right).$$

Puisque les m nombres t_K satisfont à l'équation (7), on obtient

$$(8) \qquad \prod_{\rho=1}^{m} \prod_{0 \leqq \lambda < K \leqq n} \left(\xi_\rho^2 - \frac{\tau_K - \tau_\lambda}{K - \lambda} \xi_\rho + \frac{K \tau_\lambda - \lambda \tau_K}{K - \lambda} \right) = \sum \gamma_{\mu_0 \ldots \mu_m} \tau_0^{\mu_0} \ldots \tau_m^{\mu_m}$$

où chaque exposant est ≥ 0 et $< m$; les coefficients $\mu_0, \ldots, \mu_m$ sont des fonctions entières rationnelles symétriques de $\xi_1, \ldots, \xi_m$ et peuvent donc être écrits comme fonctions rationnelles de $\alpha_1, \alpha_2, \ldots, \alpha_n$. Je dis que chacun de ces coefficients est égal à zéro. En effet à chaque nombre K $(0 \leq K \leq m)$ il correspond un couple (ρ, σ) tel que

$$\tau_K = \xi_\rho \xi_\sigma + K(\xi_\rho + \xi_\sigma)$$

Le nombre des entiers K est égal à m+1, et le nombre des couples (ρ,σ) est égal à m, de sorte qu'au moins un des couples (ρ,σ) correspond à deux entiers K et λ tels que $0 \leq \lambda < K \leq m$. Alors on a

$$\tau_K = \xi_\rho \xi_\sigma + K(\xi_\rho + \xi_\sigma) \text{ et } \tau_\lambda = \xi_\rho \xi_\sigma + \lambda(\xi_\rho + \xi_\sigma)$$

donc

$$\xi_\rho + \xi_\sigma = \frac{\tau_K - \tau_\lambda}{K - \lambda} \text{ et } \xi_\rho \xi_\sigma = \frac{K\tau_\lambda - \lambda\tau_K}{K - \lambda}$$

par conséquent

$$\xi_\rho^2 - \frac{\tau_K - \tau_\lambda}{K - \lambda}\xi_\rho + \frac{K\tau_\lambda - \lambda\tau_K}{K - \lambda} = 0,$$

d'où il suit que le membre de gauche de (8) est égal à zéro. Ainsi nous trouvons au lieu de (8) une équation en τ_0 de degré $< n$, qui possède n racines différentes τ_0 ; en effet $\tau_0 = \xi_\rho \xi_\sigma$ suffit, où ξ_ρ et ξ_σ sont des quantités indéfinies avec $0 \leq \sigma < \rho \leq n$.

De cette manière on voit que dans le membre de gauche de (8) seulement l'exposant $\mu_0 = 0$ figure.

De la même manière on obtient $\mu_1 = 0, \ldots, \mu_m = 0$, de sorte que le membre de droite de (8) est une constante et donc égal à zéro.

Si l'on remplace $\alpha_1, \ldots, \alpha_m, \tau_0, \ldots, \tau_n$ respectivement par $a_1, \ldots, a_m, t_0, \ldots t_n$, le membre de gauche de (8) se transforme en ξ, donc

$$\xi = \sum c_{\mu_0, \ldots, \mu_m} t_0^{\mu_0} \ldots t_n^{\mu_n}$$

on obtient les coefficients $c_{\mu_0, \ldots, \mu_n}$ en remplaçant dans $\gamma_{\mu_0, \ldots, \mu_n}$ les coefficients $\alpha_1, \ldots, \alpha_m$ par $a_1, \ldots, a_m$. En vertu de $\gamma_{\mu_1, \ldots \mu_n} = 0$ on voit $c_{\mu_0, \ldots, \mu_n} = 0$, donc $\xi = 0$.

Démontrons ensuite que chaque équation $A(X) = 0$ de degré n dont les coefficients appartiennent à Ω, possède exactement n racines appartenant à $\Omega(i)$ coincident ou non. Cette assertion est évidente pour $n = 1$ de sorte que nous pouvons supposer que $n \geq 2$ et que la proposition est déja démontrée si n est remplacé par un plus petit nombre naturel.

Nous savons que l'équation $A(X) = 0$ possède une racine r appartenant à $\Omega(i)$, de sorte que $A(X)$ est divisible par $X - r$. Si r est un élément de Ω, on peut écrire $A(X) = (X-r)B(X)$, où les coefficients de $B(X)$ appartiennent à Ω. D'après notre hypothèse $B(X) = 0$ possède n-1 racines appartenants à $\Omega(i)$, de sorte que $A(X)$ en possède exactement n.

Si r n'appartient pas à Ω, l'équation $A(X) = 0$ ne possède pas seulement la racine r mais également la racine conjuguée $\bar{r}$ et on peut écrire $A(X) = (X - r)(X - \bar{r})B(X)$, où les coefficients de

B(X) sont des éléments de Ω. D'après notre hypothèse B(X) possède n-2 racines appartenant à $\Omega(i)$, de sorte que A(X) en possède exactement n.

Il est clair que chaque équation A(X) = 0 de degré n dont les coefficients appartiennent à Ω, possède exactement n racines appartenant à $\Omega(i)$, puisque l'équation $A(X).\overline{A}(X) = 0$, dont les coefficients appartiennent à Ω, possède exactement 2n racines appartenant à $\Omega(i)$. Chaque élément U + iV de $\Omega(i)$ possède la propriété que U et V sont des éléments de Ω et satisfont à une équation algébrique dont les coefficients appartiennent à Φ. Comme il est connu '), U + iV satisfait également à une équation algébrique dont les coefficients appartiennent à Φ.

Ainsi le théorème fondamental de l'algèbre est démontré.

Il est superflu de remarquer que les théorèmes connus de Rolle, Budan-Fourier, Descartes, Sturm etc. peuvent être maintenant démontrés sans l'aide d'aucun axiome de continuité.

Des considérations intuitionistes.

L'intuitioniste accepte le raisonnement précédent, parce que chaque assertion peut être vérifiée par un nombre fini d'opérations. Cependant il ne peut pas prendre pour Φ l'ensemble des nombres réels à cause du fait, que cet ensemble n'est pas ordonné. Je déduirai une généralisation du théorème fondamental de l'algèbre, qui ne possède pas cet

inconvénient. Nous verrons qu'aucun axiome de continuité n'est nécessaire dans les mathématiques intuitionistes.

Si U + iV désigne un élément arbitraire du corps $\Omega(i)$, construit ci-dessus, où U et V sont des éléments de Ω, j'appelle module de $|U + iV|$ le nombre $\sqrt{U^2 + V^2}$. Le module est positif ou nul selon que U + iV est ou non différent de zéro. On a $|a+b| \leq |a| + |b|$ et $|ab| = |a||b|$.

J'appelle suite convergente une suite $(a_0, a_1 \ldots)$ formée par des éléments de $\Omega(i)$, telle qu'on puisse faire correspondre à chaque élément positif ε de Ω un nombre naturel N avec la propriété que l'inégalité $|a_m - a_n| < \varepsilon$ soit valable pour chaque entier $m \geq N$ et pour chaque entier $n \geq N$.

Je dis que deux suites convergentes $a^* = (a_0, a_1, \ldots)$ et $b^* = (b_0, b_1, \ldots)$ sont égales si l'on peut faire correspondre à chaque nombre positif ε de Ω un nombre naturel N avec la propriété que l'inégalité $|a_m - b_n| < \varepsilon$ soit valable pour chaque entier $m \geq N$ en pour chaque entier $n \geq N$.

Il est clair que cette notion d'égalité est réflexive, symétrique et transitive.

Je dis que deux suites convergentes a^* et b^* sont différentes, et on notera $a^* \neq b^*$, s'il est possible de trouver un élément positif δ de Ω tel qu'on puisse faire correspondre à chaque nombre naturel N deux entiers $m \geq N$ et $n \geq N$ avec $|b_m - a_n| > \delta$
La notion d'inégalité est symétrique. Il est évident

que $a^* \neq b^*$ et $b^* = c^*$ entraînent $a^* \neq c^*$.
Il est exclu que les deux relations $a^* = b^*$ et $a^* \neq b^*$ sont vérifiées en même temps. Elles ne sont pas nécessairement complémentaires c'est-à-dire que nous n'avons pas toujours le droit de dire qu'au moins une de ces deux relations est valable.

Considérons le cas particulier où tous les éléments des deux suites convergentes $a^* = (a_0, a_1, \ldots)$ et $b^* = (b_0, b_1, \ldots)$ appartiennent à Ω. Je dis que b^* est supérieur à a^* et que a^* est inférieur à b^*, et on écrira $b^* > a^*$ ou $a^* < b^*$, si Ω contient un élément positif δ, tel qu'on puisse faire correspondre à tout nombre naturel N deux entiers $m \geq N$ et $n \geq N$ avec $b_m - a_n > \delta$.
Les relations $>$ et $<$ sont transitives; les trois relations $>$ $=$ et $<$ ne sont pas nécessairement complémentaires.
Si les suites $a^* = (a_0, a_1, \ldots)$ et $b^* = (b_0, b_1, \ldots)$ dont les éléments appartiennent à $\Omega(i)$, sont convergentes, les suites $(a_0 + b_0, a_1 + b_1, \ldots)$ et $(a_0 b_0, a_1 b_1, \ldots)$ le sont également. Ces deux suites sont appelées respectivement la somme $a^* + b^*$ et le produit $a^* b^*$ des deux suites a^* et b^*. L'addition et la multiplication satisfont aux règles usuels de calcul de sorte que les suites convergentes dont les éléments appartiennent à $\Omega(i)$ forment un anneau. Je désignerai cet anneau par Ω^*.

Si $a^* = (a_0, a_1, \ldots)$ est un élément de Ω^*, la suite $(|a_0|, |a_1|, \ldots)$ est également convergente, je

dirai que cette série est le module $|a^*|$ de a^*. Si $|a|<p$ et $|b|<q$, on a $|a+b|<p+q$ et $|ab|<pq$.

Pour la démonstration de la généralisation du théorème fondamental de l'algèbre, annoncée dans l'introduction, j'aurai besoin de deux lemmes.

Lemme 1.

Soient ε et M deux éléments positifs de Ω. Si les coefficients des deux polynomes

$A(X) = X^n + a_1 X^{n-1} + \ldots + a_n$ et

$B(X) = X^n + b_1 X^{n-1} + \ldots + b_n$ appartiennent à Ω et satisfont aux inégalités

$$(9)\quad |a_\rho| < M^\rho ;\ |b_\rho| < M^\rho ;\ |b_\rho - a_\rho| < \varepsilon M^\rho \quad (\rho = 1, \ldots, n),$$

le polynome A(X) possède au moins un zéro et B(X) au moins un zéro tels que leur différence soit en valeur absolue inférieure à $c_1 M \varepsilon^{\frac{1}{n}}$. Dans ce lemme et dans le suivant $c_1, c_2, \ldots, c_3$ désignent des nombres naturels, convenablement choisis, dépendant seulement du degré n.

Pour la démonstration nous considérons le produit

$$P = \prod_{\rho,\sigma=1}^{n} (\alpha_\rho - \beta_\sigma).$$

où $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n$ désignent les zéros respectivement de A(X) et de B(X).

Posons $b_\rho = a_\rho + p_\rho$. Le produit P est une fonction rationnelle entière et symétrique de $\alpha_1, \ldots, \alpha_n$ et aussi de $\beta_1, \ldots \beta_n$ et peut donc être écrit comme une fonction rationnelle entière des éléments $a_1, \ldots, a_n, p_1, \ldots, p_n$. Cette fonction s'annule, si

tous les éléments $p_1, \ldots, p_n$ sont égaux à zéro. Par conséquent chaque terme, figurant dans cette fonction rationnelle est divisible par au moins un des éléments $p_1, \ldots, p_n$. Un terme $p_\sigma q$, qui est divisible par p_σ possède le poids n^2, à supposer que a_ρ et p_ρ ont le poids ρ. Par conséquent q possède le poids $n^2 - \rho$ et donc en vertu de (9) un module $< c_2 M^{n^2-\rho}$. Ainsi on voit que la fonction rationnelle dont il s'agit ici, est composée de termes; chacune a une module $< c_2 M^{n^2} \varepsilon$ et le nombre de ces termes est $\leq c_3$, donc

$$|P| < c_1^{n^2} \cdot M^{n^2} \varepsilon .$$

Puisque le produit P possède n^2 facteurs, au moins un de ces facteurs est en valeur absolue inférieur à $c_1 M \varepsilon^{\frac{1}{n^2}}$.

Lemme 2.

Si les conditions du lemme précédent sont remplies avec $\varepsilon < 1$, alors on peut numéroter les zéros $\alpha_1, \ldots, \alpha_n$ de A(X) et les zéros $\beta_1, \ldots, \beta_n$ de B(X) de telle facon qu'on ait

$$|\beta_1 - \alpha_1| < c_4 M \varepsilon^{\frac{1}{n^2}} ; |\beta_2 - \alpha_2| < c_4 M \varepsilon^{\frac{1}{n^2(n-1)^2}}; \ldots$$

$$|\beta_n - \alpha_n| < c_4 M \varepsilon^{\frac{1}{n^2(n-1)^2 \ldots 1^2}}$$

D'après le lemme précédent on peut supposer que $n \geq 2$, que le lemme est déjà démontré pour n-1 au lieu de n et qu'on a

(10) $$|\beta_1 - \alpha_1| < c_1 M \varepsilon^{\frac{1}{n^2}}$$

Posons $a_o = 1$; $A(X) = (X - \alpha_1) \sum_{\rho=0}^{n-1} U_\rho X^{n-1-\rho}$ et

$$B(X) = (X - \beta_1) \sum_{\rho=0}^{n-1} V_\rho X^{n-1-\rho}$$

nous avons

$$u_\rho = \sum_{\lambda=0}^{\rho} a_\lambda F_{\rho\lambda}(\alpha_1) \qquad \text{et} \quad v_\rho = \sum_{\lambda=0}^{\rho} b_\lambda F_{\rho\lambda}(\beta_1)$$

où $F_{\rho\lambda}(X)$ est un polynome de degré $\leq \rho - \lambda$. Par conséquent

$$v_\rho - u_\rho = \sum_{\lambda=0}^{\rho} \{(b_\lambda - a_\lambda) w_{\rho\lambda} + b_\lambda t_{\rho\lambda}\},$$

où

$$w_{\rho\lambda} = F_{\rho\lambda}(\alpha_1) \text{ et } t_{\rho\lambda} = F_{\rho\lambda}(\beta_1) - F_{\rho\lambda}(\alpha_1).$$

Nous avons $|\alpha_1| < 3M$. En effet, si non, nous aurions $|\alpha_1| > 2M$, donc

$$2^n |a_1 \alpha_1^{n-1} + \ldots + a_n| < |\alpha_1|^n (2^{n-1} + \ldots + 1) < 2^n |\alpha_1|^n,$$

de sorte que α_1 ne serait pas une racine de l'équation $A(X) = 0$. De la même manière on obtient $|\beta_1| < 3M$. Ainsi nous trouvons

$$|w_{\rho\lambda}| < c_5 M^{\rho-\lambda} \text{ et } |t_{\rho\lambda}| \leq c_6 |\beta_1 - \alpha_1| M^{\rho-\lambda-1} < c_6 c_1 \varepsilon^{\frac{1}{n^2}} M^{\rho-\lambda}$$

Par conséquent on a pour $\rho = 1, 2, \ldots, n$

$$|v_\rho - u_\rho| < c_7 M^\rho (\varepsilon + \varepsilon^{\frac{1}{n^2}}) < \varepsilon^{\frac{1}{n^2}} (c_8 M)^\rho$$

en vertu de $\varepsilon < 1$.

D'après le lemme à démontrer, appliqué avec n-1 au lieu de n, avec $\varepsilon^{\frac{1}{n^2}}$ au lieu de ε et avec $c_8 M$ au lieu de M on peut numéroter les zéros $\alpha_2, \ldots \alpha_n$, $\beta_2, \ldots, \beta_n$ respectivement de $\sum_{\rho=0}^{n-1} u_\rho X^{n-1-\rho}$ et $\sum_{\rho=0}^{n-1} v_\rho X^{n-1-\rho}$ de telle façon que les $2^{\text{ième}}$ $3^{\text{ième}}$ ... ...$n^{\text{ième}}$ inégalités, figurant dans (10) soient remplies. Ainsi le lemme est démontré.

Passons maintenant à la démonstration de la généralisation du théorème fondamental.

Traitons d'abord le cas particulier $a_0^* = 1$. Le coefficient a_ρ^* ($\rho = 1, \ldots, n$) est une suite convergente $(a_{\rho 0}, a_{\rho 1}, \ldots)$. Il suit de la convergence que les éléments $a_{\rho m}$ sont bornés, de sorte qu'on obtient pour chaque entier $m \geqq 0$

$$|a_{\rho m}| < M^\rho \quad (\rho = 1, 2, \ldots, n),$$

où M désigne un nombre convenablement choisi, indépendant de ρ et de m.

Parce que la suite $a_\rho^* = (a_{\rho 0}, a_{\rho 1}, \ldots)$ est convergente, on peut faire correspondre à chaque élément positif ε de Ω un entier positif N, tel que les inégalités

$$|a_{\rho m} - a_{\rho t}| < \varepsilon \quad (\rho = 1, \ldots, n)$$

soient valables pour chaque entier $m \geqq N$ et chaque entier $t \geqq N$. Ainsi on peut faire correspondre à tout entier positif N un élément positif $\varepsilon(N)$ de Ω tel que les inégalités

$$|a_{\rho m} - a_{\rho t}| < \varepsilon(N) \quad (\rho = 1, \ldots, n)$$

soient valables pour chaque entier $m \geqq N$ et chaque entier $t \geqq N$, et que $\varepsilon(N)$ soit inférieur à un élément quelconque fixe de Ω, si N est suffisamment grand. L'élément $\delta(N)$ défini par

$$\delta(N) = \{\varepsilon(N)\}^{\frac{1}{n^2(n-1)^2 \cdots 1^2}},$$

est donc également inférieur à un élément quelconque fixe de Ω, si N est suffisamment grand. Je

choisis les entiers positifs $N_1, N_2, \ldots$ croissant indéfiniment de telle façon qu'on ait

$$\delta(N_1) < 1 \quad \text{et} \quad \delta(N_{h+1}) \leq \tfrac{1}{2}\delta(N_h) \quad (h = 1, 2, \ldots)$$

Les racines de l'équation

$$(11) \qquad z^n + a_{1m} z^{n-1} + \ldots + a_{nm} = 0$$

seront ordonnées d'une manière arbitraire pour $m = 0, 1, \ldots, N_1$. D'après le lemme précédent nous pouvons ordonner les racines de cette équation de telle façon qu'on ait pour $\rho = 1, \ldots, n$.

$$|\alpha_{\rho m} - \alpha_{\rho N_1}| < c_4 M \delta(N_1) \quad (N_1 < m \leq N_2),$$

$$|\alpha_{\rho m} - \alpha_{\rho N_2}| < c_4 M \delta(N_2) \quad (N_2 < m \leq N_3),$$

etc. Ainsi nous trouvons pour $m \geq N_h$

$$|\alpha_{\rho m} - \alpha_{\rho N_h}| < c_4 M \{\delta(N_h) + \delta(N_{h+1}) + \ldots\}$$
$$< 2c_4 M \delta(N_h),$$

donc pour $m \geq N_h$ et $t \geq N_h$

$$|\alpha_{\rho m} - \alpha_{\rho t}| < 4c_4 M \delta(N_h).$$

Puisque le membre de droite est inférieur à un élément positif quelconque de Ω, si N_h est suffisamment grand, la suite $\alpha_\rho^* = (\alpha_{\rho 1}, \alpha_{\rho 2}, \ldots)$ est convergente. L'identité

$$A_\sigma(X) = (X - \alpha_{\sigma 1}) \ldots (X - \alpha_{\sigma n})$$

nous donne par passage à la limite

$$A^*(X) = (X - \alpha_1^*) \ldots (X - \alpha_n^*)$$

Après avoir traité le cas particulier avec $a_0^* = 1$ je considère le cas général avec l'équation

$A^*(X) = a_o^* X^n + \ldots + \alpha_n^* = 0$, où au moins un des coefficients est différent de zéro.

Le coefficient de $A^*(X)$, qui est différent de zéro peut être écrit comme une forme linéaire à coefficients rationnels des n+1 éléments $A^*(p)$ où p parcourt les valeurs 0, 1,..., n. Par conséquent on peut choisir dans le système 0, 1,..., n au moins un nombre p tel que $A^*(p)$ soit différent de zéro.

Choisissons deux nombres naturels q et r tel que $pr - q \neq 0$ et posons

$$X = \frac{pW - q}{W - r} \quad \text{donc} \quad W = \frac{Xr - q}{X - p} .$$

Par cette substitution l'équation donnée se transforme en une équation de la forme

$$B^*(W) = b_o^* W^n + \ldots + b_n^* = 0, \text{ où } b_o^* = A^*(p) \neq 0.$$

D'après le cas particulier traité ci-dessus l'ensemble Ω^* contient n éléments $w_1^*, \ldots, w_n^*$ pour lesquelles $B^*(W) = b_o^* (W - w_1^*)\ldots(W - w_n^*)$. On a

$$\frac{W - w_\rho^*}{W - r} = K_\rho^* X + \lambda_\rho^*, \qquad (\rho = 1,..,n), \text{ si l'on pose}$$

$$K_\rho^* = \frac{r - w_\rho^*}{pr - q} \quad \text{et} \quad \lambda_\rho^* = \frac{pw_\rho^* - q}{pr - q} .$$

Ainsi on obtient

$$(12) \quad A^*(X) = b_o^* (K_1^* X + \lambda_1^*)\ldots(K_n^* X + \lambda_n^*)$$

de sorte que la généralisation demandée est démontrée.

Supposons finalement que

$a^*_\sigma \neq 0$ et $a^*_\tau \neq 0$ où $0 \leqq \sigma \leqq \tau \leqq n$,

et considérons un entier $\mu \geqq \sigma$ et $\leqq \tau$. Le coefficient a^*_σ peut être écrit comme la somme d'un nombre de termes, dont chacun est égal au produit de deux facteurs. Le premier de ces deux facteurs est b^*_o. L'autre facteur est un produit de σ éléments figurant dans le système $\lambda^*_1, \ldots, \lambda^*_n$ et de $n - \sigma$ éléments, figurant dans le système $K^*_1, \ldots, K^*_n$. Par conséquent au moins un des termes mentionnés a la propriété que le second facteur est différent de zéro, de sorte que le système $K^*_1, \ldots, K^*_n$ contient au moins $n - \sigma$ éléments différents de zéro. De la même manière le fait que a^*_τ n'est pas nul entraîne que le système $\lambda^*_1, \ldots, \lambda^*_n$ contient au moins τ éléments différents de zéro. Pour chaque ρ ($\rho = 1, \ldots, n$) au moins un des deux éléments K^*_ρ et λ^*_ρ est différent de zéro, puisque $A^*(X)$ possède au moins un coefficient $\neq 0$. On peut donc, pour tout entier $\mu \geqq \sigma$ et $\leqq \tau$, numéroter des facteurs dans la formule (12) de telle facon que tous les éléments $K^*_1, \ldots, K^*_\mu$ et $\lambda^*_{\mu+1}, \ldots, \lambda^*_n$ soient différents de zéro et nous trouvons alors

$$A^*(X) = c^*(X - \alpha^*_1)\ldots(X - \alpha^*_\mu)(1 - \beta^*_{\mu+1}X)\ldots(1 - \beta^*_n X).$$