ANNALES SCIENTIFIQUES DE L'É.N.S.

J. DUFRESNOY
CH. PISOT

Sur un ensemble fermé d'entiers algébriques

Annales scientifiques de l'É.N.S. 3e série, tome 70, nº 2 (1953), p. 105-133
<http://www.numdam.org/item?id=ASENS_1953_3_70_2_105_0>

SUR UN ENSEMBLE FERMÉ
D'ENTIERS ALGÉBRIQUES

PAR MM. J. DUFRESNOY ET CH. PISOT.

INTRODUCTION

Nous nous proposons d'étudier dans cet article un ensemble S d'entiers algébriques particuliers θ qui semblent devoir jouer un rôle fondamental en théorie des nombres. D'une part, ils permettent de préciser la structure des corps finis de nombres algébriques et d'obtenir des relations nouvelles entre corps différents. D'autre part, ils sont en liaison étroite avec l'approximation rationnelle, donc se rattachent aussi à certaines parties de la théorie des séries trigonométriques.

Les zéros d'un polynome à coefficients entiers, dont le terme du plus haut degré a comme coefficient ± 1, ont un produit dont le module est au moins égal à 1. Sauf dans le cas où tous les zéros sont sur $|z| = 1$, il y a donc un zéro au moins situé dans la région $|z| > 1$. Nous allons porter notre attention sur le cas où le polynome a un zéro et un seul dans la région $|z| > 1$, tous ses autres zéros (s'il y en a) étant *intérieurs* au cercle unité.

Le zéro de plus grand module est nécessairement réel et, quitte à changer z en $-z$, on peut toujours supposer qu'il est supérieur à 1. Nous désignerons ce zéro par θ et nous écrirons le polynome correspondant

$$P(z) \equiv p_0 + p_1 z + \ldots + p_{s-1} z^{s-1} + \varepsilon z^s,$$

où p_0 est un entier positif et $\varepsilon = \pm 1$.

Nous représenterons par S l'ensemble des nombres θ. L'étude de cet ensemble a été entreprise par plusieurs auteurs [1]; dans le présent travail nous allons la poursuivre, ce qui nous conduira à des résultats nouveaux.

---

(1) CH. PISOT, *Ann. R. Sc. Norm. Sup. Pisa*, sér. II, t. 7, 1938, p. 205-248; R. SALEM, *Duke Math. J.*, t. 11, 1944, p. 103-108 et t. 12, 1945, p. 153-172; C. L. SIEGEL, *Duke Math. J.*, t. 11, 1944, p. 597-602.

Remarquons d'abord que le polynome $P(z)$ est *irréductible* [2], car s'il se décomposait en un produit de facteurs, l'un de ceux-ci aurait tous ses zéros intérieurs au cercle unité et son terme de plus haut degré aurait comme coefficient ± 1, ce qui est impossible. Au polynome $P(z)$, nous associerons le polynome

$$Q(z) \equiv \varepsilon z^s P\left(\frac{1}{z}\right) \equiv 1 + q_1 z + \ldots + q_{s-1} z^{s-1} + q_s z^s.$$

Les polynomes $P(z)$ et $Q(z)$ étant irréductibles sont sans zéros communs ou ils sont identiques. Ce dernier cas exige que $P(z)$ ait $\frac{1}{\theta}$ comme seul zéro intérieur au cercle unité, donc que $s = 2$, $p_0 = 1$ et $\varepsilon = 1$, c'est-à-dire que

$$P(z) \equiv 1 + p_1 z + z^2, \qquad \text{avec} \quad p_1 \leqq -3;$$

les nombres θ correspondants, à savoir $\theta = \frac{-p_1 + \sqrt{p_1^2 - 4}}{2}$, croissent avec $-p_1$ et tendent vers $+\infty$ quand p_1 tend vers $-\infty$. Ces nombres θ particuliers seront écartés dans nos raisonnements généraux (sans que nous le précisions explicitement) et devront toujours être étudiés à part.

Suivant une idée de M. Salem, à chaque nombre θ de S nous ferons correspondre la fraction rationnelle $\frac{P(z)}{Q(z)}$. Nous établirons que *les fonctions* $\frac{P(z)}{Q(z)}$ *correspondant à un ensemble borné de nombres* θ *de* S *constituent une famille normale de fonctions méromorphes dans* $|z| < 1$. En utilisant une méthode due à l'un de nous [3], nous montrerons que *les fonctions limites sont des fractions rationnelles*. Nous retrouverons, en passant, un résultat remarquable de M. Salem : l'ensemble S est fermé; le nombre 1 n'appartient pas à son ensemble dérivé S'. Nous établirons ensuite le critère suivant :

Pour qu'un nombre θ *de* S *appartienne à* S' *il faut et il suffit qu'il existe un polynome* $A(z)$ *à coefficients entiers tel que, sur* $|z| = 1$, *on ait* $|A(z)| \leqq |P(z)|$, *l'égalité n'étant vérifiée qu'en un nombre fini de points.*

De ce critère, nous tirerons les deux conséquences suivantes :

1° *Les puissances entières* θ^n *des nombres* θ *de* S *appartiennent, pour* $n \geqq 2$, *à l'ensemble* S';

2° *Les nombres* θ *de* S *qui sont totalement réels appartiennent à* S'.

La seconde partie de notre travail est consacrée à l'étude des petits éléments de S. On voit aussitôt que le nombre $\theta_0 = \frac{1 + \sqrt{5}}{2}$, racine de l'équation

---

(2) Dans l'ensemble des polynomes à coefficients entiers.

(3) Pisot, *loc. cit.*

$1+z-z^2=0$, appartient à S'. M. Siegel a signalé l'intérêt qui s'attacherait à la détermination du plus petit élément de l'ensemble S' et il a indiqué qu'il n'avait pu décider si ce plus petit élément était θ_0. Nous établissons qu'il en est bien ainsi. Notre démonstration, assez compliquée dans le détail, repose essentiellement sur le critère cité plus haut et sur une proposition qui se déduit du lemme de Schwarz. Cette proposition nous permet aussi de déterminer aisément les quatre plus petits éléments de l'ensemble S [4].

Nos principaux résultats ont déjà été résumés dans deux Notes [5].

PROPRIÉTÉS GÉNÉRALES DE L'ENSEMBLE S.

La fraction rationnelle $\frac{P(z)}{Q(z)}$, associée au nombre θ de l'ensemble S, jouit des propriétés suivantes :

1° elle a un module égal à 1 sur $|z|=1$;

2° elle a un pôle et un seul dans la région $|z|<1$; c'est le pôle simple $z=\frac{1}{\theta}$;

3° dans $|z|<\frac{1}{\theta}$, elle peut être développée en série de puissances :

$$\frac{P(z)}{Q(z)}=\sum_{n=0}^{\infty} u_n z^n, \tag{1}$$

où les u_n sont des entiers;

4° dans $|z|\leq 1$, après mise en évidence du pôle $z=\frac{1}{\theta}$, elle peut être développée sous la forme

$$\frac{P(z)}{Q(z)}=\frac{\lambda}{1-\theta z}+\sum_{n=0}^{\infty} \varepsilon_n z^n. \tag{2}$$

En rapprochant les relations (1) et (2) on obtient immédiatement

$$u_n=\lambda\theta^n+\varepsilon_n. \tag{3}$$

Enfin, si l'on calcule la valeur moyenne de $\left|\frac{P(z)}{Q(z)}(1-\theta z)\right|^2$ sur $|z|=1$, on trouve, en utilisant la relation (1),

$$u_0^2+\sum_{n=1}^{\infty}(u_n-\theta u_{n-1})^2=1+\theta^2; \tag{4}$$

---

[4] M. Siegel (*loc. cit.*) avait déterminé les deux plus petits éléments et prévu les deux suivants. Notre travail démontre l'exactitude de cette prévision.

[5] *C. R. Acad. Sc.*, t. 235, 1952, p. 1592-1593 et t. 236, 1953, p. 30-31.

tandis que, si l'on calcule la valeur moyenne de $\left|\frac{P(z)}{Q(z)}\right|^2$ sur $|z| = 1$, on trouve, en utilisant la relation (2),

$$\frac{\lambda^2}{\theta^2 - 1} + \sum_{n=0}^{\infty} \varepsilon_n^2 = 1. \tag{5}$$

Cette dernière relation entraîne l'inégalité

$$\lambda < \sqrt{\theta^2 - 1} < \theta, \tag{6}$$

utilisée par M. Salem. Mais cet auteur ne semble pas avoir remarqué que l'on a aussi

$$\lambda > \frac{1}{2(\theta + 1)}. \tag{7}$$

Pour établir ce dernier point, on tire de (3) et (5)

$$|u_0 - \lambda| = |\varepsilon_0| < 1,$$

d'où, puisque $u_0 = p_0 \geqq 1$,

$$\lambda > 0 \qquad \text{et} \qquad u_0 < \lambda + 1.$$

Si l'on avait $\lambda \leqq \frac{1}{2(\theta + 1)}$, λ serait inférieur à $\frac{1}{4}$, donc u_0 serait égal à 1; l'inégalité (4) entraînerait alors

$$|u_1 - \theta| < \theta,$$

d'où $u_1 \geqq 1$ et, compte tenu de (3) et (5),

$$\frac{\lambda^2}{\theta^2 - 1} + (1 - \lambda)^2 + (1 - \lambda\theta)^2 < 1,$$

soit

$$\frac{\lambda^2 \theta^4}{\theta^2 - 1} - 2\lambda(1 + \theta) + 1 < 0,$$

en contradiction avec l'hypothèse faite.

Des inégalités (6) et (7) on déduit

$$\sqrt{\theta^2 - 1} > \frac{1}{2(\theta + 1)},$$

ce qui montre que la borne inférieure de l'ensemble S est supérieure à 1, résultat que M. Salem a établi par une autre méthode.

Étude des suites convergentes de nombres de S.

Considérons une suite de nombres θ_μ de S tendant vers une limite finie θ'; l'ensemble des nombres λ_μ qui leur sont associés, est borné inférieurement et supérieurement, de sorte qu'on peut toujours supposer, quitte à extraire de la suite précédente une suite partielle, que les λ_μ tendent vers une limite finie non nulle λ'. En appliquant la relation (2) au nombre θ_μ nous obtenons

$$\frac{P_\mu(z)}{Q_\mu(z)} = \frac{\lambda_\mu}{1-\theta_\mu z} + \sum_{n=0}^{\infty} \varepsilon_{\mu,n} z^n.$$

Les fonctions $\sum \varepsilon_{\mu,n} z^n$, holomorphes pour $|z| \leqq 1$, sont bornées en module dans leur ensemble sur $|z| = 1$ puisqu'on a, sur ce cercle,

$$\left|\sum \varepsilon_{\mu,n} z^n\right| \leqq 1 + \frac{\lambda_\mu}{\theta_\mu - 1} \qquad \text{qui tend vers} \qquad 1 + \frac{\lambda'}{\theta' - 1}.$$

Il en résulte que les fonctions $\sum \varepsilon_{\mu,n} z^n$ constituent une famille normale. Les fonctions $\frac{P_\mu(z)}{Q_\mu(z)}$ constituent donc, dans $|z| < 1$, une famille normale de fonctions méromorphes. De la suite $\frac{P_\mu(z)}{Q_\mu(z)}$ nous pouvons donc extraire une suite partielle convergente dans $|z| < 1$, suite partielle que nous désignerons encore par $\frac{P_\mu(z)}{Q_\mu(z)}$ pour ne pas alourdir inutilement les notations. Quand μ tend vers l'infini, on a alors

$$\theta_\mu \to \theta', \qquad \lambda_\mu \to \lambda' \neq 0, \qquad \varepsilon_{\mu,n} \to \varepsilon'_n, \qquad u_{\mu,n} \to u'_n, \tag{8}$$

et la fonction limite $R(z)$, qui est méromorphe dans $|z| < 1$, présente les développements

$$\begin{cases} R(z) = \sum_{n=0}^{\infty} u'_n z^n & \text{dans} \quad |z| < \frac{1}{\theta'}; \\ R(z) = \frac{\lambda'}{1-\theta' z} + \sum_{n=0}^{\infty} \varepsilon'_n z^n & \text{dans} \quad |z| < 1. \end{cases} \tag{9}$$

Il résulte de (8) que les u'_n sont des entiers et que, pour un n fixé, on a $u_{\mu,n} = u'_n$ dès que μ est assez grand.

D'autre part, l'inégalité (4) appliquée à θ_μ, entraîne pour un N fixé quelconque

$$u_{\mu,0}^2 + \sum_{n=1}^{N} (u_{\mu,n} - \theta_\mu u_{\mu,n-1})^2 < 1 + \theta_\mu^2;$$

d'où, en faisant tendre μ vers l'infini,

$$u_0'^2 + \sum_{n=1}^{N} (u'_n - \theta' u'_{n-1})^2 \leqq 1 + \theta'^2;$$

cette relation étant satisfaite quel que soit N, il en résulte immédiatement

$$u_0'^2 + \sum_{n=1}^{\infty} (u'_n - \theta' u'_{n-1})^2 \leqq 1 + \theta'^2. \tag{4 bis}$$

A partir de (5), on obtiendrait de même

$$\frac{\lambda'^2}{\theta'^2-1}+\sum_{n=0}^{\infty}\varepsilon_n'^2 \leqq 1. \tag{5 bis}$$

La relation (3), enfin, entraîne

$$u'_n = \lambda'\theta'^n + \varepsilon'_n. \tag{3 bis}$$

En s'appuyant sur la relation (4 *bis*), on montre [6] que le déterminant

$$\begin{vmatrix} u'_0 & u'_1 & \dots & u'_n \\ u'_1 & u'_2 & \dots & u'_{n+1} \\ \dots & \dots & \dots & \dots \\ u'_n & u'_{n+1} & \dots & u'_{2n} \end{vmatrix}$$

tend vers zéro quand n augmente indéfiniment. Or, c'est un entier ; il est donc nul dès que n est assez grand. Il résulte alors d'un théorème de Kronecker que, à partir d'un certain rang, les u'_n sont liés par une récurrence linéaire, homogène, à coefficients constants. Fatou a montré que pour une telle suite d'entiers u'_n, on peut toujours prendre une relation de récurrence à coefficients entiers, le coefficient du terme de plus grand indice étant $+1$.

La fonction $R(z)$, donnée par (9), est donc une fraction rationnelle à coefficients entiers, qui s'écrit

$$R(z) \equiv \frac{A(z)}{Q^*(z)},$$

avec $Q^*(0)=1$. Nous pouvons supposer cette fraction rationnelle irréductible [7]. D'autre part, d'après sa définition, $R(z)$ a dans $|z|<1$ un pôle et un seul, à savoir $z=\frac{1}{\theta'}$.

Nous allons montrer maintenant que, sur $|z|=1$, on a $|R(z)|\leqq 1$. En effet, pour tout point z intérieur au cercle unité,

$$\left|\frac{P_\mu(z)}{Q_\mu(z)}\,\frac{1-\theta_\mu z}{z-\theta_\mu}\right| \leqq 1, \tag{10}$$

puisqu'il s'agit du module d'une fonction holomorphe et que le module est égal à 1 sur $|z|=1$. Laissant z fixe, faisons augmenter μ indéfiniment; la relation (10) donne

$$\left|R(z)\frac{1-\theta' z}{z-\theta'}\right| \leqq 1 \qquad \text{pour} \quad |z|<1.$$

---

[6] La méthode suivie ici, qui a été utilisée par R. Salem (*loc. cit.*), a été exposée pour la première fois par Ch. Pisot (*loc. cit.*).

[7] S'il n'en était pas ainsi, on formerait le P. G. C. D. du numérateur et du dénominateur et l'on mettrait ce P. G. C. D. sous forme d'un polynome à coefficients entiers, premiers entre eux dans leur ensemble. $A(z)$ et $Q^*(z)$ seraient divisibles par ce P. G. C. D. et l'on sait (théorème de Gauss) que les quotients seraient à coefficients entiers.

Faisons alors tendre z vers une valeur quelconque de module 1 ; la dernière relation entraîne

$$|R(z)| \leqq 1 \quad \text{pour} \quad |z| = 1. \tag{11}$$

La fonction $R(z)$ n'a donc pas de pôle sur $|z|=1$. Il en résulte que le polynome $Q^\star(z)$ a un zéro et un seul, $z=\frac{1}{\theta'}$, dans $|z|<1$, tous ses autres zéros étant de modules strictement supérieurs à 1. Puisque $Q^\star(0)=1$, le nombre θ' appartient donc à S (8) et le polynome $Q(z)$ qui lui est associé est justement le polynome $Q^\star(z)$. Nous écrirons donc θ au lieu de θ', $Q(z)$ au lieu de $Q^\star(z)$ et u_n au lieu de u'_n.

Caractérisation des nombres de l'ensemble dérivé S'.

Établissons que, dans (11), l'égalité ne peut avoir lieu qu'en un nombre fini de points. L'égalité, pour $|z|=1$, se traduit, en effet, par

$$A(z)\,A\left(\frac{1}{z}\right) - Q(z)\,Q\left(\frac{1}{z}\right) = 0$$

et cette équation algébrique n'a qu'un nombre fini de racines, à moins qu'elle ne soit identiquement vérifiée, auquel cas on aurait $|R(z)|=1$ pour $|z|=1$. Il nous reste à montrer que cette dernière hypothèse ne peut se réaliser.

Soient σ, σ_μ et σ'_μ les valeurs moyennes sur $|z|=1$ de $|R(z)(1-\theta z)^2|^2$, de $|R(z)(1-\theta_\mu z)(1-\theta z)|^2$ et de $\left|\frac{P_\mu(z)}{Q_\mu(z)}(1-\theta_\mu z)(1-\theta z)\right|^2$; nous obtenons (en convenant de poser, pour simplifier l'écriture, $u_{\mu,-2}=u_{\mu,-1}=u_{-2}=u_{-1}=0$)

$$\sigma = \sum_{n=0}^{\infty} [u_n - 2\theta u_{n-1} + \theta^2 u_{n-2}]^2, \tag{12}$$

$$\sigma_\mu = \sum_{n=0}^{\infty} [u_n - (\theta_\mu + \theta)\, u_{n-1} + \theta_\mu \theta\, u_{n-2}]^2, \tag{13}$$

$$\sigma'_\mu = \sum_{n=0}^{\infty} [u_{\mu,n} - (\theta_\mu + \theta)\, u_{\mu,n-1} + \theta_\mu \theta\, u_{\mu,n-2}]^2, \tag{14}$$

avec

$$\sigma'_\mu = 1 + (\theta_\mu + \theta)^2 + \theta_\mu^2 \theta^2.$$

Étant donné $\varepsilon > 0$, on peut, d'après (12), trouver N tel que

$$\sum_{n=N+1}^{\infty} | u_n - 2\theta u_{n-1} + \theta^2 u_{n-2}]^2 < \varepsilon. \tag{15}$$

(8) Nous retrouvons ici le résultat fondamental de M. Salem : l'ensemble S est fermé.

D'autre part, d'après sa définition, σ_μ tend vers σ quand μ augmente indéfiniment; on peut donc trouver m tel que $\mu > m$ entraîne

$$(16) \qquad |\sigma_\mu - \sigma| < \varepsilon,$$

et aussi (puisque N est fixé et que θ_μ tend vers θ)

$$(17) \qquad \left| \sum_{n=0}^{N} [u_n - (\theta_\mu + \theta) u_{n-1} + \theta_\mu \theta \, u_{n-2}]^2 - \sum_{n=0}^{N} [u_n - 2\theta \, u_{n-1} + \theta^2 u_{n-2}]^2 \right| < \varepsilon.$$

De (12), (13), (15), (16) et (17), on déduit aussitôt

$$(18) \qquad \sum_{n=N+1}^{\infty} [u_n - (\theta_\mu + \theta) u_{n-1} + \theta_\mu \theta \, u_{n-2}]^2 < 3\varepsilon \qquad \text{pour} \quad \mu > m.$$

Si nous choisissons pour μ une valeur assez grande (et supérieure à m) nous aurons

$$u_{\mu,n} = u_n \qquad \text{pour} \quad n < M$$

et

$$u_{\mu,M} \neq u_M,$$

où M est un nombre supérieur à N. De l'inégalité

$$|u_M - (\theta_\mu + \theta) u_{M-1} + \theta_\mu \theta \, u_{M-2}| < \sqrt{3\varepsilon},$$

conséquence immédiate de (18), on déduit alors, si l'on a pris au début $\varepsilon < \frac{1}{3}$,

$$(19) \qquad |u_{\mu,M} - (\theta_\mu + \theta) u_{\mu,M-1} + \theta_\mu \theta \, u_{\mu,M-2}| > 1 - \sqrt{3\varepsilon}.$$

De (13), (14), (18) et (19), on tire

$$\sum_{n=M}^{\infty} [u_{\mu,n} - (\theta_\mu + \theta) u_{\mu,n-1} + \theta_\mu \theta \, u_{\mu,n-2}]^2 - \sum_{n=M}^{\infty} [u_n - (\theta_\mu + \theta) u_{n-1} + \theta_\mu \theta \, u_{n-2}]^2$$
$$= \sigma'_\mu - \sigma_\mu \geqq (1 - \sqrt{3\varepsilon})^2 - 3\varepsilon.$$

Faisons tendre μ vers l'infini; $\sigma'_\mu = 1 + (\theta_\mu + \theta)^2 + \theta_\mu^2 \theta^2$ tend vers $1 + 4\theta^2 + \theta^4$, tandis que σ_μ tend vers σ. La dernière inégalité entraîne

$$\sigma \leqq 1 + 4\theta^2 + \theta^4 - (1 - \sqrt{3\varepsilon})^2 + 3\varepsilon,$$

d'où, puisque ε est arbitrairement petit,

$$\sigma \leqq 4\theta^2 + \theta^4.$$

Cette inégalité montre en particulier que l'on ne peut avoir $|R(z)| = 1$ pour $|z| = 1$, car, s'il en était ainsi, σ, d'après sa définition, aurait pour valeur $1 + 4\theta^2 + \theta^4$.

Si l'on remarque enfin que, sur $|z| = 1$, on a $|P(z)| = |Q(z)|$, on obtient le théorème suivant :

THÉORÈME 1. — *Pour qu'un nombre θ de l'ensemble S appartienne à l'ensemble dérivé S', il faut et il suffit qu'il existe un polynome $A(z)$ à coefficients entiers tel que, si $P(z)$ est le polynome associé à θ, on ait, sur $|z|=1$, l'inégalité $|A(z)|\leqq|P(z)|$, l'égalité n'étant vérifiée qu'en un nombre fini de points.*

Nous venons, en effet, de voir que la condition est nécessaire (9). Montrons qu'elle est suffisante. Supposons donc qu'il existe un tel polynome $A(z)$. S'il y a, sur $|z|=1$, des points où $|A(z)|=|P(z)|$, ces points sont en nombre fini; nous les désignerons par $z_k=e^{2\pi i\varphi_k}$ $(k=1, 2, \ldots, p)$ et nous poserons $\frac{Q(z_k)}{A(z_k)}=e^{2\pi i\omega_k}$. Pour chaque valeur de k, l'expression $n\varphi_k-\omega_k$, où n est un entier positif, ne prendra une valeur entière que pour une valeur de n au plus, si φ_k est irrationnel. Si φ_k est rationnel, z_k est racine de l'unité, donc zéro d'un certain polynome $E_k(z)$ irréductible, avec $E_k(0)=1$; on peut toujours supposer que c'est pour les valeurs $1, 2, \ldots, q$ de k qu'il en est ainsi.

Considérons alors les équations

$$Q(z)-z^n A(z)=0, \tag{20}$$

où n a une valeur entière assez grande. Une telle équation ne peut avoir pour racines sur $|z|=1$ que certains des nombres $z_1, z_2, \ldots, z_q$ et ces racines ne peuvent être multiples (10). Si, pour une valeur de n, cela a effectivement lieu, le premier membre de l'équation (20) se décompose en un produit de facteurs distincts, comprenant certains des polynomes $E_1(z)$, $E_2(z)$, $\ldots$, $E_q(z)$ et un polynome $Q_n(z)$ ne se réduisant pas à une constante et ne s'annulant pas sur $|z|=1$.

Il résulte du théorème de Rouché que l'équation

$$Q(z)-\rho z^n A(z)=0$$

a une racine et une seule dans $|z|<1$ lorsque la constante ρ a un module inférieur à 1. En faisant tendre ρ vers 1, on en déduit que l'équation (20) a au plus une racine dans $|z|<1$. Le polynome $Q_n(z)$ a donc au plus un zéro de module inférieur à 1. Mais $Q_n(0)=1$; par conséquent (*voir* l'Introduction) le polynome $Q_n(z)$ a un zéro et un seul de module inférieur à 1 et ce polynome est irréductible. Ce zéro est donc l'inverse $\frac{1}{\theta_n}$ d'un nombre θ_n de l'ensemble S.

---

(9) Il importe de remarquer qu'aucune difficulté ne peut provenir de l'existence des éléments de S appartenant à la catégorie particulière signalée dans l'introduction. Ceux-ci sont en nombre fini dans tout intervalle borné, de sorte que, sauf peut-être un nombre fini d'entre eux, les θ_μ n'appartiennent pas à cette catégorie.

(10) On ne peut, en effet, avoir

$$Q'(z_k)-z_k^n A'(z_k)-nz_k^{n-1}A(z_k)=0$$

si n est assez grand, car alors

$$n|A(z_k)|>|Q'(z_k)|+|A'(z_k)|.$$

L'équation (20) a $\frac{1}{\theta_n}$ comme racine unique dans $|z|<1$. Il en résulte, d'une part, que ces nombres θ_n sont tous différents, car, sinon, $Q(z)$ et $A(z)$ auraient un zéro commun; $Q(z)$ étant irréductible, $A(z)$ serait donc divisible par $Q(z)$; le quotient, polynome à coefficients entiers, devrait avoir un module au plus égal à 1 sur $|z|=1$, l'égalité n'étant pas toujours satisfaite; ce qui est impossible. D'autre part, dans tout domaine fermé intérieur au cercle unité, le premier membre de (20), quand n tend vers l'infini, tend uniformément vers $Q(z)$ qui présente $\frac{1}{\theta}$ comme zéro; il en résulte que θ_n tend vers θ; le nombre θ est donc bien un élément limite. Le théorème 1 est complètement démontré.

Premières applications.

Voici deux applications de la condition suffisante énoncée dans le théorème 1.

Théorème 2. — *Les puissances entières θ^n des nombres θ de l'ensemble* S *appartiennent, pour $n \geq 2$, à l'ensemble dérivé* S'.

Soit θ un nombre de S, $P(z)$ et $Q(z)$ les polynomes associés. Désignons par $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$ les racines $n^{\text{ièmes}}$ de l'unité. On voit immédiatement que $Q(z)Q(\zeta z)Q(\zeta^2 z)\ldots Q(\zeta^{n-1}z)$ est un polynome à coefficients entiers et que c'est un polynome en z^n. Nous le noterons $Q^\star(z^n)$. Le polynome $Q^\star(z)$ a pour zéros les puissances $n^{\text{ièmes}}$ de $\frac{1}{\theta}$ et de ses conjugués; puisque $Q^\star(0)=1$, le nombre θ^n appartient à S et $Q^\star(z)$ est le polynome Q qui lui est associé.

Soit h l'un des nombres $0, 1, 2, \ldots, n-1$; considérons l'expression

$$\frac{1}{n}\sum_{k=0}^{n-1}\zeta^{-hk}\frac{P(\zeta^k z)}{Q(\zeta^k z)}.$$

En vertu de (1), elle a comme développement, au voisinage de l'origine, $\sum_m u_{h+mn}z^{h+mn}$; comme, d'autre part, c'est une fraction rationnelle, on a

$$\frac{1}{n}\sum_{k=0}^{n-1}\zeta^{-hk}\frac{P(\zeta^k z)}{Q(\zeta^k z)} \equiv z^h\frac{A_h(z^n)}{Q^\star(z^n)},$$

où A_h est un polynome à coefficients entiers, non identiquement nul car, en vertu de (3) et (5), on a $|u_p-\lambda\theta^p|<1$, ce qui montre que les u_{h+mn} ne peuvent être tous nuls.

De la dernière identité, on déduit aisément que, pour $|z|=1$,

$$|A_0(z)|^2+|A_1(z)|^2+\ldots+|A_{n-1}(z)|^2=|Q^\star(z)|^2.$$

Nous avons ainsi mis en évidence n polynomes $A(z)$ différents, satisfaisant aux conditions du théorème 1. En général, les polynomes que nous venons de trouver ne sont d'ailleurs pas les seuls.

THÉORÈME 3. — *Les nombres θ de l'ensemble S qui sont totalement réels appartiennent à l'ensemble dérivé S'.*

On entend par nombre algébrique totalement réel, un nombre dont tous les conjugués sont réels. Supposons donc que le polynome $P(z)$ ait tous ses zéros réels et montrons qu'on peut alors trouver un polynome $A(z)$ satisfaisant aux conditions du théorème 1.

Première méthode. — Soient α_j les zéros de $P(z)$, parmi lesquels se trouve θ. Sur $|z|=1$, on a, en posant $z=e^{i\varphi}$,

$$w = \operatorname{Log}|P(z)|^2 = \sum \operatorname{Log}(1+\alpha_j^2 - 2\alpha_j\cos\varphi);$$

d'où

$$\frac{dw}{d\varphi} = 2\sin\varphi \sum \frac{\alpha_j}{1+\alpha^2 - 2\alpha_j\cos\varphi}$$

et

$$\frac{d^2w}{d\varphi^2} - \frac{dw}{d\varphi}\operatorname{cotg}\varphi = -4\sin^2\varphi \sum \left(\frac{\alpha_j}{1+\alpha_i^2 - 2\alpha_j\cos\varphi}\right)^2.$$

Il en résulte que, si $\frac{dw}{d\varphi}$ s'annule pour une valeur de φ non multiple de π, on a $\frac{d^2w}{d\varphi^2} < 0$: pour une telle valeur de φ, la fonction de w passe par un maximum. Le minimum absolu de w est donc atteint pour $\varphi = 0$ ou $\varphi = \pi$. Or $P(1)$ et $P(-1)$ sont des entiers non nuls. Par conséquent, sur $|z|=1$, on a $|P(z)| \geqq 1$, l'égalité ne pouvant avoir lieu qu'aux points $z = \pm 1$. Nous avons ainsi trouvé un polynome $A(z) \equiv 1$.

Deuxième méthode. — Sur $|z|=1$, on a

$$\left|\frac{z-\alpha_j}{z-1}\right| \geqq \frac{1+\alpha_j}{2} \qquad \text{si} \quad \alpha_j > 0$$

et

$$\left|\frac{z-\alpha_j}{z+1}\right| \geqq \frac{1-\alpha_j}{2} \qquad \text{si} \quad \alpha_j < 0,$$

de sorte que, si p des α_j sont positifs et q sont négatifs,

$$|P(z)| \geqq |z-1|^p |z+1|^q \prod \frac{1+|\alpha_j|}{2},$$

l'égalité ne pouvant avoir lieu qu'aux points $z = \pm 1$. En remarquant que

$$\prod \frac{1+|\alpha_j|}{2} > \left|\prod \alpha_j\right|^{\frac{1}{2}} \geqq 1,$$

on voit que nous avons ainsi mis en évidence un autre polynome

$$A(z) \equiv (z-1)^p (z+1)^q,$$

pour lequel on a même l'inégalité stricte $|A(z)| < |P(z)|$ sur $|z| = 1$.

Corollaire. — *Les nombres* θ *de l'ensemble* S *qui sont du premier et du second degré appartiennent à l'ensemble dérivé* S'.

Ces nombres sont très faciles à trouver. Les nombres θ du premier degré sont les entiers supérieurs à 1. Quant aux nombres θ du second degré, ils correspondent aux polynomes

$$P(z) \equiv \varepsilon(z^2 + q_1 z + q_2)$$

qui ont un zéro compris entre -1 et $+1$ et un zéro supérieur à $+1$, ce qui se traduit par $1 - q_1 + q_2 > 0$ et $1 + q_1 + q_2 < 0$; ils sont donc donnés par la formule

$$\theta = \frac{-q_1 + \sqrt{q_1^2 - 4q_2}}{2},$$

où les entiers q_1 et q_2 vérifient $q_1 + |1 + q_2| < 0$.

Le plus petit de ceux de ces nombres correspondant à une valeur fixée de q_1 est celui pour lequel q_2 est le plus grand possible; on trouve

$$q_2 = -q_1 - 2 \qquad \text{et} \qquad \theta = \frac{-q_1 + \sqrt{q_1^2 + 4q_1 + 8}}{2},$$

q_1 étant un entier négatif; ce nombre θ est, à son tour, le plus petit possible quand $q_1 = -1$ et il vaut alors

$$\theta_0 = \frac{1 + \sqrt{5}}{2}.$$

Tel est le plus petit nombre de l'ensemble S' que le corollaire précédent nous permette de découvrir.

PROPRIÉTÉS DES PETITS ÉLÉMENTS DE L'ENSEMBLE S.

Le but essentiel de l'étude qui va suivre est de démontrer que ce nombre θ_0, racine de $1 + z - z^2 = 0$, est le plus petit élément de l'ensemble S'.

Applications du lemme de Schwarz.

Lemme 1. — *Soit* $C(z) \equiv c_0 + c_1 z + \ldots + c_k z^k$ *un polynome à coefficients entiers, tel que* $c_0 \geqq 1$ *et que* $|C(z)| \leqq |Q(z)|$ *sur* $|z| = 1$. *Si* $\theta < 2$, *on a* $c_0 = 1$; *si* $\theta < \theta_0$, *on a de plus* $c_1 = q_1 + 1$ *à moins que* $C(z) \equiv Q(z)$.

En effet, la fonction

$$\varphi(z) \equiv \frac{C(z)}{Q(z)} \frac{1-\theta z}{\theta - z}$$

est holomorphe pour $|z| \leqq 1$ et elle a, sur $|z| = 1$, un module au plus égal à 1. Il en résulte, en particulier, que $|\varphi(0)| \leqq 1$, soit $|c_0| \leqq \theta$. Si $\theta < 2$, on a donc $c_0 = 1$.

Si cette condition est réalisée, $\varphi(0) = \frac{1}{\theta}$. Suivant une méthode classique, nous considérerons alors la fonction

$$\varphi_1(z) \equiv \frac{1}{z} \frac{\varphi(z) - \varphi(0)}{1 - \varphi(z)\varphi(0)};$$

elle est holomorphe pour $|z| \leqq 1$ et elle a, sur $|z| = 1$, un module au plus égal à 1; il en résulte que $|\varphi_1(0)| \leqq 1$, soit $|\varphi'(0)| \leqq 1 - |\varphi(0)|^2$, l'égalité ne pouvant avoir lieu que si $\varphi_1(z)$ est une constante de module 1, cas que nous écartons momentanément. Un calcul simple donne

$$\varphi'(0) = \frac{c_1 - q_1}{\theta} - \left(1 - \frac{1}{\theta^2}\right),$$

d'où l'inégalité

$$\left| \frac{c_1 - q_1}{\theta} - \left(1 - \frac{1}{\theta^2}\right) \right| < 1 - \frac{1}{\theta^2},$$

soit

$$0 < \frac{c_1 - q_1}{\theta} < 2\left(1 - \frac{1}{\theta^2}\right).$$

Si $\theta \leqq \theta_0$, on a $\theta\left(1 - \frac{1}{\theta^2}\right) \leqq 1$, d'où $c_1 = q_1 + 1$ puisque c_1 et q_1 sont des entiers.

Il reste à étudier le cas particulier où φ_1 est une constante K de module 1. On a alors

$$\varphi(z) \equiv \frac{\varphi(0) + Kz}{1 + K\varphi(0)z}, \qquad \text{avec} \quad \varphi(0) = \frac{1}{\theta},$$

d'où

$$\frac{C(z)}{Q(z)} \equiv \frac{\theta - z}{1 - \theta z} \frac{1 + K\theta z}{\theta + Kz}.$$

Les polynomes $C(z)$ et $Q(z)$ sont donc de même degré. Puisque $Q(z)$ est irréductible et que $C(0) = Q(0) = 1$, deux cas seulement sont possibles :

ou bien $C(z) \equiv Q(z)$, cas banal écarté dans l'énoncé du lemme;

ou bien $C(z)$ et $Q(z)$ sont premiers entre eux; mais alors $Q(z)$ est au plus du second degré et nous avons montré plus haut que cela ne peut avoir lieu si $\theta < \theta_0$.

On peut poursuivre l'étude précédente et, en supposant toujours $\theta < \theta_0$, trouver des limitations pour les coefficients c_2, c_3, ... Faisons-le dans le cas [11] $C(z) \equiv P(z)$.

Rappelons la relation (1)

$$\frac{P(z)}{Q(z)} = \sum_{n=0}^{\infty} u_n z^n;$$

on en déduit

$$\varphi(z) = \sum_{n=0}^{\infty} d_n z^n,$$

avec

$$\begin{aligned}
d_0 &= \frac{u_0}{\theta},\\
d_1 &= \frac{1}{\theta}\left[u_1 + \left(\frac{1}{\theta} - \theta\right)u_0\right],\\
d_2 &= \frac{1}{\theta}\left[u_2 + \left(\frac{1}{\theta} - \theta\right)\left(u_1 + \frac{u_0}{\theta}\right)\right],\\
d_3 &= \frac{1}{\theta}\left[u_3 + \left(\frac{1}{\theta} - \theta\right)\left(u_2 + \frac{u_1}{\theta} + \frac{u_0}{\theta^2}\right)\right],\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots
\end{aligned}$$

et le lemme 1 montre que $u_0 = u_1 = 1$.

On peut remarquer que, la fonction $\varphi(z)$ étant holomorphe et de module au plus égal à 1 dans $|z| \leqq 1$, il en sera de même, pour tout entier positif k, de la fonction

$$\psi_k(z) = \sum_{n=0}^{\infty} d_{nk} z^n, \qquad \text{puisque} \quad \psi_k(z^k) \equiv \frac{1}{k}\sum \varphi(\zeta_j z),$$

les ζ_j étant les racines $k^{\text{ièmes}}$ de l'unité. L'inégalité classique

$$|\psi'_k(0)| \leqq 1 - |\psi_k(0)|^2$$

donne

$$|d_k| \leqq 1 - |d_0|^2.$$

Si l'on applique ce résultat pour $k = 2$ et 3, on obtient aussitôt

$$\frac{1}{\theta}\left(\theta - \frac{1}{\theta}\right) \leqq u_2 \leqq \left(\theta - \frac{1}{\theta}\right)\left(2 + \frac{1}{\theta}\right), \tag{21}$$

$$\left(\theta - \frac{1}{\theta}\right)\left(u_2 - 1 + \frac{1}{\theta} + \frac{1}{\theta^2}\right) \leqq u_3 \leqq \left(\theta - \frac{1}{\theta}\right)\left(u_2 + 1 + \frac{1}{\theta} + \frac{1}{\theta^2}\right). \tag{22}$$

Ces inégalités peuvent être améliorées en suivant un algorithme classique que nous ne ferons qu'amorcer : on forme la fonction $\varphi_1(z)$, déjà utilisée, et l'on exprime

$$|\varphi'_1(0)| \leqq 1 - |\varphi_1(0)|^2,$$

---

[11] Il peut sembler que ce soit là un cas très particulier. Il n'en est rien, car nous montrerons plus loin que, pour $\theta < \theta_0$, le seul polynome $C(z)$ satisfaisant aux conditions du lemme 1 est le polynome $P(z)$, le cas banal $C(z) \equiv Q(z)$ étant écarté.

ce qui conduit à une double inégalité plus précise que (21); nous n'en retiendrons qu'une partie, à savoir

$$d_2 \leq 1 - d_0^2 - \frac{d_1^2}{1-d_0},$$

soit

$$(23) \qquad u_2 \leq \left(\theta - \frac{1}{\theta}\right)\left(2 + \frac{1}{\theta}\right) - \frac{1}{\theta - 1}\left(1 + \frac{1}{\theta} - \theta\right)^2 = \frac{\theta^3 - \theta^2 - 1}{\theta(\theta - 1)} + 2.$$

Le polynome $1 + z^2 - z^3$, présente un zéro réel et un seul, $\theta^\star$, qui est supérieur à 1; ses deux autres zéros sont par suite imaginaires conjugués et de module inférieur à 1. Le nombre $\theta^\star$ appartient donc à S. Par simple substitution, on s'assure que $\theta^\star < \theta_0$.

Pour $\theta < \theta_0$, la double inégalité (21) entraîne

$$0 < u_2 < 2 + \frac{1}{\theta} < 3,$$

donc $u_2 = 1$ ou $u_2 = 2$; la relation (23) montre que seul le cas $u_2 = 1$ se réalise si $\theta < \theta^\star$. Pour $u_2 = 1$, la double inégalité (22) entraîne

$$0 < u_3 \leq 2\theta + 1 - \frac{1}{\theta} - \frac{1}{\theta^2} - \frac{1}{\theta^3} < 2\theta_0 + 1 - \frac{1}{\theta_0} - \frac{1}{\theta_0^2} - \frac{1}{\theta_0^3} = 3,$$

donc $u_3 = 1$ ou $u_3 = 2$; tandis que pour $u_2 = 2$, la double inégalité (22) entraîne

$$1 < u_3 \leq 3\theta + 1 - \frac{2}{\theta} - \frac{1}{\theta^2} - \frac{1}{\theta^3} < 3\theta_0 + 1 - \frac{2}{\theta_0} - \frac{1}{\theta_0^2} - \frac{1}{\theta_0^3} = 4,$$

donc $u_3 = 2$ ou $u_3 = 3$. Résumons ces résultats :

Lemme 2. — *Les nombres* θ *de* S *qui sont inférieurs à* θ_0, *se répartissent en deux familles; pour la première famille, on a*

$$\frac{P(z)}{Q(z)} = 1 + z + z^2 + u_3 z^3 + \ldots, \qquad \textit{avec} \quad u_3 = 1 \quad \textit{ou} \quad 2;$$

pour la seconde famille, on a

$$\frac{P(z)}{Q(z)} = 1 + z + 2z^2 + u_3 z^3 + \ldots, \qquad \textit{avec} \quad u_3 = 2 \quad \textit{ou} \quad 3.$$

Les nombres θ *inférieurs à* $\theta^\star$ *appartiennent à la première famille.*

Étude d'une famille particulière de nombres θ.

On peut déterminer aisément tous les nombres θ de la première famille du lemme 2. En effet, de

$$Q(z) \equiv 1 + q_1 z + q_2 z^2 + \ldots,$$

on déduit alors

$$P(z) \equiv 1 + (q_1 + 1)z + (q_2 + q_1 + 1)z^2 + \ldots,$$

d'où

$$(1 - z^2)\,P(z) - (1 + z - z^2)\,Q(z) \equiv z^2 + \ldots.$$

D'après le théorème de Rouché (puisque $|1 - z^2| < |1 + z - z^2|$ sur $|z| = 1$), le premier membre a, dans $|z| < 1$, deux zéros; l'expression du second membre montre que ceux-ci sont confondus en $z = 0$ et que les autres zéros ont un produit des modules au plus égal à 1; ces derniers ne peuvent donc être situés que sur $|z| = 1$; comme le premier membre ne peut s'annuler sur $|z| = 1$, on en conclut que ces autres zéros n'existent pas; d'où

$$(1 - z^2)\,P(z) - (1 + z - z^2)\,Q(z) \equiv z^2.$$

Si, dans cette identité, on change z en $\frac{1}{z}$ et qu'on multiplie par $-\varepsilon z^{s+2}$, on obtient

$$(1 - z^2)\,Q(z) - (1 - z - z^2)\,P(z) \equiv -\varepsilon z^s.$$

Des deux dernières relations, on tire

$$\text{(24)}\qquad \begin{aligned} P(z) &\equiv 1 - z^2 - \varepsilon z^{s-2}(1 + z - z^2), \\ Q(z) &\equiv 1 - z - z^2 - \varepsilon z^{s-2}(1 - z^2) \end{aligned}$$

et l'on devra avoir $s > 2$. Le théorème de Rouché permet de vérifier que $Q(z)$ a bien un zéro et un seul intérieur au cercle unité; de $Q(0) = 1$, $Q(1) = -1$, on déduit que ce zéro est compris entre 0 et 1. Le polynome $P(z)$ défini par (24) a donc pour zéro un nombre θ de l'ensemble S.

En formant $P(\theta_0)$, on voit que ce nombre θ est inférieur à θ_0 si $\varepsilon = -1$. Plaçons-nous dans ce cas et désignons par θ_{s-2} le nombre θ qui est zéro du polynome (24). Par substitution, on voit que θ_{s-2} croît avec s et que $\theta_3 < \theta^* < \theta_4$. La dernière propriété énoncée dans le lemme 2 entraîne donc la proposition suivante :

Les quatre plus petits éléments de S *sont* $\theta_1 < \theta_2 < \theta_3 < \theta^*$, *où*

θ_1	*est racine de*	$1 + z - z^3 = 0,$
θ_2	» »	$1 + z^3 - z^4 = 0,$
θ_3	» »	$1 - z^2 + z^3 + z^4 - z^5 = 0,$
θ^*	» »	$1 + z^2 - z^3 = 0.$

Recherche du plus petit élément de S′.

Nous avons vu que $\theta_0 = \frac{1 + \sqrt{5}}{2}$ est un élément de S′. Nous allons montrer maintenant qu'un nombre θ inférieur à θ_0 ne peut appartenir à S′. Soient $P(z)$ et $Q(z)$ les polynomes associés à θ; en vertu du théorème 1, il nous suffira de prouver qu'il n'existe pas de polynome $A(z)$ à coefficients entiers tel que $|A(z)| \leq |Q(z)|$ sur $|z| = 1$, l'égalité n'ayant pas lieu partout. Après quelques généralités, nous démontrerons l'impossibilité de l'existence d'un tel polynome $A(z)$ dont le degré sera successivement supposé supérieur, inférieur et enfin égal à celui de $Q(z)$.

Généralités.

Rappelons tout d'abord que tout nombre $\theta < \theta_0$ est de degré $s \geqq 3$. Dans la suite cette inégalité interviendra à plusieurs reprises sans que nous l'indiquions explicitement.

Nous prendrons $A(z)$ sous la forme

$$A(z) \equiv a_0 + a_1 z + \ldots + a_h z^h, \qquad \text{avec} \quad a_0 > 0.$$

En vertu des conditions qui lui sont imposées par le théorème 1, le polynome $A(z)$ est nécessairement distinct de $P(z)$ et de $Q(z)$. Comme $\theta < \theta_0$, le lemme 1 montre que

$$(25) \qquad a_0 = 1, \qquad a_1 = q_1 + 1.$$

Le polynome

$$B(z) \equiv \varepsilon'(a_h + a_{h-1} z + \ldots + a_1 z^{h-1} + a_0 z^h) \equiv \varepsilon' z^h A\left(\frac{1}{z}\right),$$

où $\varepsilon' = \pm 1$ est tel que $\varepsilon' a_h > 0$, vérifie aussi $|B(z)| \leqq |Q(z)|$ sur $|z| = 1$. Le lemme 1 donne donc encore

$$(26) \qquad \varepsilon' a_h = 1, \qquad \varepsilon' a_{h-1} = q_1 + 1.$$

Enfin, le polynome $P(z)$ vérifie $|P(z)| = |Q(z)|$ sur $|z| = 1$; donc, en vertu du lemme 1, on a aussi

$$(27) \qquad \varepsilon q_s = 1, \qquad \varepsilon q_{s-1} = q_1 + 1,$$

d'où

$$(28) \qquad Q(z) \equiv 1 + q_1 z + q_2 z^2 + \ldots + q_{s-2} z^{s-2} + \varepsilon(q_1 + 1) z^{s-1} + \varepsilon z^s.$$

Posons alors

$$(29) \qquad A(z) - Q(z) \equiv z\,U(z), \qquad B(z) - Q(z) \equiv z\,V(z).$$

Les relations (25) et (26) montrent que $U(0) = V(0) = 1$.

Puisque, sur $|z| = 1$, on a $|A(z)| \leqq |Q(z)|$ et $|B(z)| \leqq |Q(z)|$, il résulte du théorème de Rouché que, si $|\rho| < 1$, les équations $\rho A(z) - Q(z) = 0$ et $\rho B(z) - Q(z) = 0$ ont exactement autant de racines dans $|z| < 1$ que $Q(z) = 0$, c'est-à-dire *une* racine. En raison de la continuité des racines de ces équations quand $\rho \to 1$, on voit que les polynomes (29) ont au plus un zéro dans $|z| < 1$. Or, ces polynomes s'annulent effectivement pour $z = 0$. Les modules des zéros des polynomes $U(z)$ et $V(z)$ sont donc tous au moins égaux à 1; par suite leur produit est au moins égal à 1. D'autre part, ce produit est l'inverse d'un entier;

il est donc égal à 1 et tous les zéros de $U(z)$ et de $V(z)$ se trouvent sur $|z|=1$. On a, par conséquent,

$$U(z) \equiv \varepsilon'' z^u U\left(\frac{1}{z}\right), \qquad V(z) \equiv \varepsilon''' z^v V\left(\frac{1}{z}\right), \qquad \text{avec} \quad \varepsilon'' = \pm 1, \qquad \varepsilon''' = \pm 1, \tag{30}$$

u et v étant les degrés de U et V.

LEMME 3. — *Les zéros de* $U(z)$ *et de* $V(z)$ *sont tous simples.*

En effet, pour $|\rho| < 1$ et $|z| = 1$,

$$|\arg(\rho A - Q) - \arg Q| < \frac{\pi}{2}. \tag{31}$$

Si $U(z) = 0$ a une racine ζ d'ordre 2 au moins, deux racines au moins de $\rho A - Q = 0$ tendent vers ζ quand $\rho \to 1$. Ces racines sont toutes deux dans la région $|z| > 1$, car la seule racine de $\rho A - Q = 0$ dans $|z| \leqq 1$ tend vers zéro. Au voisinage de cette valeur ζ, l'argument de $\rho A - Q$, pour ρ voisin de 1, variera au moins d'une quantité voisine de 2π. Au contraire, $\arg Q(z)$ variera très peu. Il y a donc contradiction avec l'inégalité (31).

Signalons enfin le résultat suivant :

LEMME 4. — *L'équation* $Q(z) \pm z^m P(z) = 0$, *où* m *est un entier positif ou négatif possède au moins* $|m+s-2|$ *racines distinctes sur* $|z| = 1$.

En effet, $\left|\frac{z^m P}{Q}\right| = 1$ sur $|z| = 1$; si $\arg z$ augmente de 2π, $\arg\left(\frac{z^m P}{Q}\right)$ augmente de $(m+s-2)2\pi$ et prend donc au moins $|m+s-2|$ fois une valeur déterminée, en particulier la valeur zéro ou π.

Étude du cas $h > s$.

D'après (29), U et V sont de degré $h-1$ et $\varepsilon'' = \varepsilon''' = \varepsilon'$. Le changement de z en $\frac{1}{z}$ dans (29) donne, après multiplication par $\varepsilon' z^h$,

$$B(z) - \varepsilon\varepsilon' z^{h-s} P(z) \equiv U(z), \qquad A(z) - \varepsilon\varepsilon' z^{h-s} P(z) \equiv V(z).$$

En ajoutant ces relations aux relations (29), on obtient

$$A + B - Q - \varepsilon\varepsilon' z^{h-s} P \equiv (1+z) U \equiv (1+z) V,$$

d'où

$$U \equiv V \qquad \text{et} \qquad A - Q \equiv zU \equiv zV \equiv z(A - \varepsilon\varepsilon' z^{h-s} P)$$

et enfin

$$A \equiv \frac{Q - \varepsilon\varepsilon' z^{h-s+1} P}{1 - z}.$$

L'équation $Q + \varepsilon\varepsilon' z^{h-s+1} P = 0$, d'après le lemme 4, a au moins

$|(h-s+1)+s-2|=h-1$ racines ζ distinctes sur $|z|=1$. Pour une telle valeur ζ, on a

$$A(\zeta)=\frac{2}{1-\zeta}Q(\zeta);$$

or, $|A(\zeta)|\leqq|Q(\zeta)|$, donc $\zeta=-1$ et $h-1\leqq 1$. Mais $h\leqq 2$ est incompatible avec l'hypothèse $h>s\geqq 3$.

Étude du cas $h<s$.

D'après (29), U et V sont alors de degrés $s-1$ et $\varepsilon''=\varepsilon'''=-\varepsilon$. Le changement de z en $\frac{1}{z}$ dans (29) donne, après multiplication par $-\varepsilon z^s$,

$$P(z)-\varepsilon\varepsilon' z^{s-h}B(z)\equiv U(z), \qquad P(z)-\varepsilon\varepsilon' z^{s-h}A(z)\equiv V(z).$$

En retranchant de ces relations les relations (29) multipliées par $\varepsilon\varepsilon' z^{s-h}$, on obtient

$$P-\varepsilon\varepsilon' z^{s-h}(A+B-Q)\equiv(1-\varepsilon\varepsilon' z^{s-h+1})U\equiv(1-\varepsilon\varepsilon' z^{s-h+1})V,$$

d'où

(32) $\qquad U\equiv V \quad$ et $\quad A-Q\equiv zU\equiv zV\equiv z(P-\varepsilon\varepsilon' z^{s-h}A)$

et enfin

(33) $$A\equiv\frac{Q+zP}{1+\varepsilon\varepsilon' z^{s-h+1}}.$$

L'équation $Q-zP=0$ a, d'après le lemme 4, *au moins* $s-1$ racines distinctes ζ sur $|z|=1$. Comme

$$|A(\zeta)|=\left|\frac{2}{1+\varepsilon\varepsilon'\zeta^{s-h+1}}\right||Q(\zeta)|\leqq|Q(\zeta)|,$$

on a

$$1-\varepsilon\varepsilon'\zeta^{s-h+1}=0$$

pour toutes ces racines; donc $s-h+1\geqq s-1$, c'est-à-dire $h\leqq 2$, et toutes les racines de module 1 de $Q-zP=0$ sont aussi racines de $1-\varepsilon\varepsilon' z^{s-h+1}=0$.

On a d'ailleurs, d'après (32),

$$Q-zP\equiv A-zU-z(\varepsilon\varepsilon' z^{s-h}A+U)\equiv A(1-\varepsilon\varepsilon' z^{s-h+1})-2zU.$$

Toutes les racines de module 1 de $Q-zP=0$, sont donc racines de $U=0$. Or, U est de degré $s-1$; il en résulte que $Q-zP$ a *exactement* $s-1$ zéros distincts de module 1. Examinons successivement les trois cas $h=2, 1, 0$.

1° *Étude de $h=2$.* — Ici $Q-zP$ est divisible par $1-\varepsilon\varepsilon' z^{s-1}$ et d'autre part, d'après (33), $Q+zP\equiv(1+\varepsilon\varepsilon' z^{s-1})A$. Par identification des coefficients des termes constants, des termes en z et des termes en z^{s+1}, on obtient

$$Q-zP\equiv(1-\varepsilon\varepsilon' z^{s-1})[1+(q_1-1)z+\varepsilon' z^2],$$
$$Q+zP\equiv(1+\varepsilon\varepsilon' z^{s-1})[1+(q_1+1)z+\varepsilon' z^2].$$

On en tire

$$Q \equiv 1 + q_1 z + \varepsilon' z^2 + \varepsilon\varepsilon' z^s, \qquad \text{d'où} \qquad \varepsilon' = +1.$$

L'inégalité $Q(1) < 0$, soit $Q(1) \leqq -1$, entraîne $q_1 \leqq -3 - \varepsilon \leqq -2$. D'autre part, en vertu de (28), le coefficient de z^{s-1} dans Q doit être $\varepsilon(q_1 + 1)$. Pour $s \geqq 4$, on a donc $\varepsilon(q_1 + 1) = 0$, d'où $q_1 = -1$, en contradiction avec $q_1 \leqq -2$. Pour $s = 3$, on a $\varepsilon(q_1 + 1) = 1$, d'où $q_1 = -1 + \varepsilon$, ce qui exige $\varepsilon = -1$ et $q_1 = -2$; finalement,

$$Q(z) \equiv 1 - 2z + z^2 - z^3 \equiv (1 - z - z^2)(1 - z + z^2 - z^3) - z^5,$$

d'où

$$Q\left(\frac{1}{\theta_0}\right) = -\theta_0^{-5} < 0,$$

en contradiction avec l'hypothèse $\theta < \theta_0$.

2° *Étude de* $h = 1$. — Ici $A \equiv 1 + \varepsilon' z$, donc, d'après (25), $\varepsilon' = q_1 + 1$, d'où $q_1 = -1 + \varepsilon'$. Soit η celui des zéros de $1 - \varepsilon\varepsilon' z^s$ qui n'est pas zéro de $Q - zP$; η est réel (donc $\eta = \pm 1$), sinon son imaginaire conjugué, lui non plus, ne serait pas zéro de $Q - zP$.

On a alors

$$(1 - \eta z)(Q - zP) \equiv (1 - \varepsilon\varepsilon' z^s)[1 - (\eta - q_1 + 1)z - \varepsilon' \eta z^2]$$

et, d'après (33),

$$(1 - \eta z)(Q + zP) \equiv (1 + \varepsilon\varepsilon' z^s)[1 - (\eta - q_1 - 1)z - \varepsilon' \eta z^2].$$

On en tire

$$(1 - \eta z)Q \equiv 1 - (\eta - q_1)z - \varepsilon' \eta z^2 + \varepsilon\varepsilon' z^{s+1},$$

d'où, en identifiant les termes de plus haut degré, $\varepsilon' = -\eta$. En tenant compte aussi de $q_1 = -1 + \varepsilon'$, la dernière identité s'écrit

$$(1 + \varepsilon' z)Q(z) \equiv 1 + (2\varepsilon' - 1)z + z^2 + \varepsilon\varepsilon' z^{s+1}.$$

Pour $z = \varepsilon'$, on obtient

$$2Q(\varepsilon') = 4 - \varepsilon' + \varepsilon(\varepsilon')^{s+2} > 0$$

et, par suite, $\varepsilon' = -1$. Il en résulte

$$(1 - z)Q(z) \equiv 1 - 3z + z^2 - \varepsilon z^{s+1} \equiv (1 - z - z^2)(1 - 2z) - 2z^3 - \varepsilon z^{s+1}.$$

La substitution de $\frac{1}{\theta_0}$ donne

$$\left(1 - \frac{1}{\theta_0}\right) Q\left(\frac{1}{\theta_0}\right) = -2\theta_0^{-3} - \varepsilon\theta_0^{-(s+1)} < 0,$$

en contradiction avec l'hypothèse $\theta < \theta_0$.

3° *Étude de* $h=0$. — Ici $A\equiv 1$, donc $\varepsilon'=+1$ et, d'après (25), $q_1+1=0$, soit $q_1=-1$. Le binome $1-\varepsilon z^{s+1}$ a deux zéros non communs avec $Q-zP$; ce sont donc les zéros d'un polynome à coefficients entiers $1+cz+\eta z^2$, avec $\eta=\pm 1$, et l'on a

$$(1+cz+\eta z^2)(Q-zP)\equiv(1-\varepsilon z^{s+1})[1+(c-2)z+\eta z^2].$$

D'autre part, (33) donne

$$(1+cz+\eta z^2)(Q+zP)\equiv(1+\varepsilon z^{s+1})(1+cz+\eta z^2).$$

On en tire

$$(1+cz+\eta z^2)Q\equiv 1+(c-1)z+\eta z^2+\varepsilon z^{s+2}.$$

L'égalité des coefficients de z^{s+1} donne $\varepsilon\eta(q_1+1)+\varepsilon c=0$, d'où, comme $q_1=-1$, $c=0$; l'égalité des coefficients de z^{s+2} donne $\eta=1$. Pour $z=1$, il vient alors $2Q(1)=1+\varepsilon$, en contradiction avec le fait que $Q(1)<0$.

Étude du cas $h=s$.

Les relations (29) montrent que les degrés u et v de U et V ne dépassent pas $s-1$. Si l'on avait $u=s-1$, les coefficients des termes en z^s vérifieraient $\varepsilon'-\varepsilon=\varepsilon''$, ce qui est impossible. Donc $u\leqq s-2$ et $\varepsilon'=\varepsilon$. Les relations (25), (26) et (27) montrent alors que le coefficient de z^{s-2} dans U est nul, donc que $u\leqq s-3$. On voit de même que $v\leqq s-3$.

Le changement de z en $\frac{1}{z}$ dans les relations (29) donne, après multiplication par εz^s et en tenant compte de ce que $\varepsilon'=\varepsilon$,

$$B(z)-P(z)\equiv\varepsilon\varepsilon'' z^{s-u-1}\,U(z),\qquad A(z)-P(z)\equiv\varepsilon\varepsilon''' z^{s-v-1}\,V(z),$$

soit

$$B-P\equiv zXU,\qquad A-P\equiv zYV, \tag{34}$$

en posant

$$X(z)\equiv\varepsilon\varepsilon'' z^{s-u-2},\qquad Y(z)\equiv\varepsilon\varepsilon''' z^{s-v-2}. \tag{35}$$

On a alors, en ajoutant les relations (29) et (34),

$$A+B-Q-P\equiv z(1+X)U\equiv z(1+Y)V,$$

d'où

$$(1+X)U\equiv(1+Y)V. \tag{36}$$

Il existe, par suite, deux polynomes $U^\star(z)$ et $V^\star(z)$, premiers entre eux, avec $U^\star(0)=V^\star(0)=1$, et deux polynomes $W(z)$ et $D(z)$ tels que

$$U\equiv U^\star W,\qquad V\equiv V^\star W,\qquad 1+X\equiv V^\star D,\qquad 1+Y\equiv U^\star D. \tag{37}$$

D'un autre côté, les relations (29) et (34) donnent

$$AB-PQ\equiv zV[zU+(1+Y)Q],$$

d'où, en tenant compte des relations (37),

$$AB - PQ \equiv z U^\star V^\star W(zW + DQ). \tag{38}$$

Puisque

$$B(z) \equiv \varepsilon z^s A\left(\frac{1}{z}\right) \quad \text{et} \quad P(z) \equiv \varepsilon z^s Q\left(\frac{1}{z}\right),$$

on a, pour $|z| = 1$ $\left(\text{car alors } z \text{ et } \frac{1}{z} \text{ sont imaginaires conjugués}\right)$,

$$AB - PQ \equiv \varepsilon z^s(|A|^2 - |Q|^2). \tag{39}$$

Or, $|A| \leqq |Q|$ sur $|z| = 1$; le premier membre de (39), quand il n'est pas nul, a donc même argument que $(-\varepsilon z^s)$. Il en résulte, en particulier, que les zéros de $AB - PQ$ situés sur $|z| = 1$ ont une multiplicité paire.

Enfin, d'après le lemme 3, les zéros de U et V qui sont, comme on sait, tous sur $|z| = 1$, sont simples. Il en est de même, d'après (37), des zéros de $U^\star$, $V^\star$ et W; de plus ces zéros sont tous différents. Les zéros de $AB - PQ$ situés sur $|z| = 1$ ayant une multiplicité paire, (38) montre que $zW + DQ$ est divisible par $U^\star V^\star W$. Il existe donc deux polynomes $D^\star(z)$ et $G(z)$ avec $D^\star(0) = G(0) = 1$ tels que

$$D \equiv D^\star W \quad \text{et} \quad z + D^\star Q \equiv U^\star V^\star G. \tag{40}$$

La relation (38) s'écrit alors

$$AB - PQ \equiv z U^{\star 2} V^{\star 2} W^2 G. \tag{41}$$

En tenant compte de (39), (37) et (36), on en déduit que, pour $|z| = 1$,

$$\varepsilon z^s(|A|^2 - |Q|^2) = zUV\frac{(1+X)(1+Y)}{D^2}G = z\left[\frac{U(1+X)}{D}\right]^2 G. \tag{42}$$

Les identités (30) et (35) entraînent

$$U(z)[1 + X(z)] \equiv \varepsilon'' z^u U\left(\frac{1}{z}\right)\varepsilon\varepsilon'' z^{s-u-2}\left[1 + X\left(\frac{1}{z}\right)\right] \equiv \varepsilon z^{s-2} U\left(\frac{1}{z}\right)\left[1 + X\left(\frac{1}{z}\right)\right].$$

La relation (42) peut donc se mettre sous la forme

$$\varepsilon z^s D^2(|A|^2 - |Q|^2) = \varepsilon z^{s-1}|U(1+X)|^2 G \quad \text{sur} \quad |z| = 1.$$

Nous en déduisons que

$$\arg G = \arg(-zD^2) \quad \text{sur} \quad |z| = 1. \tag{43}$$

Lemme 5. — *Le polynome* $D(z)$ *ne peut pas se réduire à une constante.*

En effet, si $D(z)$ était une constante, celle-ci aurait pour valeur $D(0) = 1$; les relations (40) et (37) entraîneraient successivement

$$D^\star \equiv W \equiv 1, \qquad U^\star \equiv U, \qquad V^\star \equiv V, \qquad 1 + X \equiv V, \qquad 1 + Y \equiv U$$

et, enfin, d'après (40),

$$z + Q \equiv UVG \equiv (1 + X)(1 + Y)G. \tag{44}$$

Puisque $1 + X \equiv V$, on a $u + v = s - 2$; d'après (44), G est donc du second degré, soit $G(z) \equiv 1 + gz + \varepsilon\varepsilon''\varepsilon''' z^2$. Comme $D \equiv 1$, la relation (43) montre que, sur $|z| = 1$, on a $\arg G = \arg(-z)$, donc $g + \frac{1}{z} + \varepsilon\varepsilon''\varepsilon''' z$ réel, négatif ou nul. Il en résulte que $\varepsilon\varepsilon''\varepsilon''' = +1$ et $g \leqq -2$. Par suite, (44) s'écrit

$$Q(z) \equiv [1 + X(z)][1 + Y(z)](1 + gz + z^2) - z. \tag{45}$$

Pour $z = \frac{1}{\theta_0}$, on a

$$0 < 1 + X\left(\frac{1}{\theta_0}\right) \leqq 1 + \frac{1}{\theta_0} = \theta_0$$

et, de même,

$$0 < 1 + Y\left(\frac{1}{\theta_0}\right) \leqq \theta_0.$$

Enfin $G\left(\frac{1}{\theta_0}\right) \leqq \left(1 - \frac{1}{\theta_0}\right)^2 = \theta_0^{-4}$, car $g \leqq -2$. De (45) on déduit

$$Q\left(\frac{1}{\theta_0}\right) \leqq \theta_0^{-2} - \theta_0^{-1} < 0,$$

en contradiction avec $\theta < \theta_0$. Le lemme 5 est ainsi établi.

Par définition, le polynome $D(z)$ est le P. G. C. D. des deux binomes

$$1 + X \equiv 1 + \varepsilon\varepsilon'' z^{s-u-2} \qquad \text{et} \qquad 1 + Y \equiv 1 + \varepsilon\varepsilon''' z^{s-v-2}.$$

L'application de l'algorithme d'Euclide montre que $D(z)$ est de la forme $D(z) \equiv 1 + \eta z^d$ où d entier $\geqq 1$ et $\eta = \pm 1$.

Posons

$$D(z) \equiv 1 - Z(z), \qquad \text{avec} \quad Z(z) \equiv -\eta z^d. \tag{46}$$

Les relations (37) entraînent alors

$$1 + X \equiv V^* D \equiv 1 - Z^n, \qquad 1 + Y \equiv U^* D \equiv 1 - Z^m, \tag{47}$$

où $m \geqq 1$, $n \geqq 1$, sont des entiers.

Revenant à (40), nous définirons la fraction rationnelle $F(z)$ par

$$zF(z) \equiv z + D^*(z)Q(z) \equiv U^*(z)V^*(z)G(z). \tag{48}$$

De (46), nous tirons $D^2 \equiv -Z\left(2 - Z - \frac{1}{Z}\right)$, d'où, d'après (43),

$$\arg G = \arg(zZ) \qquad \text{sur} \quad |z| = 1. \tag{49}$$

Les relations (48) et (49) montrent que

$$\arg F = \arg(U^*V^*Z), \qquad \text{sur} \quad |z| = 1. \tag{50}$$

D'autre part, des identités (46) et (47) on tire

$$U^\star \equiv \frac{1-Z^m}{1-Z} \quad \text{et} \quad V^\star \equiv \frac{1-Z^n}{1-Z}.$$

Pour $Z=1$, c'est-à-dire pour les zéros de $D(z)$, les polynomes $U^\star$ et $V^\star$ prennent donc les valeurs m et n. Compte tenu de (50), nous en déduisons le résultat suivant :

LEMME 6. — *Pour tous les zéros de* $D(z)$, *on a* $U^\star = m$, $V^\star = n$ *et* F *est réel positif ou nul.*

Faisons alors décrire à z, dans le sens direct, le cercle $|z|=1$. D'après (46), $\arg Z$ est croissant. Il en est de même de

$$\arg(U^\star) = \arg\left(\frac{1-Z^m}{1-Z}\right) \quad \text{et} \quad \arg(V^\star) = \arg\left(\frac{1-Z^n}{1-Z}\right),$$

du moins sur les arcs où ces derniers arguments sont continus. Il en sera donc ainsi de $\arg F(z)$. Soit (Γ) la courbe décrite par $w=F(z)$; elle est continue et le point $w=F(z)$ ne peut traverser le demi-axe réel positif que du bas vers le haut.

La relation (48) montre que, sur $|z|=1$, les seuls nombres pour lesquels $F(z)=1$ sont les zéros δ_i de $D^\star(z)$, car $Q(z)\neq 0$. Soit alors (γ_ε) la courbe déduite du cercle $|z|=1$, en remplaçant les arcs intérieurs aux cercles de rayon ε, centrés aux divers points δ_i, par les arcs de ces petits cercles situés dans $|z|\leqq 1$. Lorsque z parcourt la courbe (γ_ε) dans le sens direct, $w=F(z)$ décrira une courbe (Γ_ε) ne passant pas par le point $w=1$ et ne différant de (Γ) que dans le voisinage de ce point.

De plus, si ε croît à partir de la valeur zéro, la courbe (Γ_ε), d'abord confondue avec (Γ), se déplace vers sa gauche (relativement au sens dans lequel elle est parcourue); de sorte que la partie $w>1$ de l'axe réel sera toujours coupée en allant du bas vers le haut, et elle le sera le même nombre n de fois par (Γ_ε) que par (Γ) si ε est assez petit. Or, dans le domaine intérieur à (γ_ε), la fonction $\frac{D^\star Q}{z} \equiv F(z)-1$ a un pôle $(z=0)$ et un zéro $\left(z=\frac{1}{\theta}\right)$; il en résulte que $\arg[F(z)-1]$ revient à sa valeur initiale quand z décrit (γ_ε); on a donc $n=0$. Par conséquent, (Γ) ne peut couper l'axe réel en un point d'abscisse supérieure à 1.

Or, d'après le lemme 6 et la relation (40), $F(z)$ est réel positif ou nul pour tous les zéros ζ de $W(z)$, ces derniers zéros étant distincts des zéros δ_i de $D^\star(z)$. Donc $F(\zeta)\neq 1$, et finalement $0\leqq F(\zeta)<1$. Mais ζ étant zéro de W, on a $D(\zeta)=0$, donc, d'après le lemme 6,

$$U^\star(\zeta)=m \quad \text{et} \quad V^\star(\zeta)=n.$$

La relation (48) donne alors

$$\zeta F(\zeta) = mn G(\zeta), \qquad \text{d'où} \qquad |G(\zeta)| = \frac{1}{mn} F(\zeta) < 1.$$

Considérons un zéro ζ_1 de W et tous ses conjugués ζ_j; le nombre $\left|\prod G(\zeta_j)\right|$ est inférieur à 1; c'est un entier rationnel, car ζ_1 est entier algébrique; donc il est nul. Par suite, pour un certain indice j_0, on a $G(\zeta_{j_0}) = 0$. On en conclut que le polynome $G(z)$ est divisible par le polynome irréductible ayant pour zéro ζ_{j_0}, donc aussi tous les ζ_j. Il en résulte que $G(z)$ est divisible par $W(z)$.

Mais d'après (41), $G(z)$ est un diviseur de $AB - PQ$; ce dernier polynome n'a, sur $|z| = 1$, que des zéros de multiplicité paire. D'après le lemme 3 et l'identité (37), les zéros de $W(z)$ sont tous simples et situés sur $|z| = 1$; $G(z)$ est donc divisible par $W^2(z)$. Les relations (40) et (37) donnent alors

$$z + D^* Q \equiv U^* V^* G \equiv U^* V^* W^2 H = UVH, \tag{51}$$

où $H(z)$ est un polynome avec $H(0) = 1$.

Montrons que $D^*(z)$ ne peut se réduire à une constante. En effet, si $D^*(z)$ était une constante, celle-ci aurait pour valeur $D^*(0) = 1$. On aurait, d'après (40), $D \equiv W$; d'après (37),

$$U \equiv U^* W \equiv U^* D \equiv 1 + Y; \qquad V \equiv V^* W \equiv V^* D \equiv 1 + X$$

et, d'après (51),

$$z + Q \equiv UVH, \qquad G \equiv W^2 H \equiv D^2 H.$$

Le polynome H serait donc du second degré et la relation (43) montrerait que $\arg H = \arg(-z)$ sur $|z| = 1$. La démonstration s'achève alors comme celle du lemme 5.

Pour poursuivre l'étude, nous utiliserons le lemme suivant :

LEMME 7. — *Soient $\eta_1, \ldots, \eta_n$ des nombres de module 1 ; alors* $\left|\prod_{k \neq h} (\eta_h - \eta_k)\right| \leqq n^n$.

En effet, on peut toujours supposer les $\eta_1, \ldots, \eta_n$ rangés dans l'ordre de leurs indices sur le cercle $|z| = 1$. Soit m un entier fixe avec $1 \leqq m \leqq n - 1$; posons

$$\eta_{n+k} = \eta_k \qquad \text{et} \qquad 2\omega_{m,h} = \arg(\eta_{h+m}) - \arg(\eta_h), \qquad \text{avec} \quad 0 \leqq \omega_{m,h} < \pi.$$

On a

$$|\eta_{h+m} - \eta_h| = 2 \sin \omega_{m,h}.$$

Posons encore

$$\rho_m = \prod_{h=1}^{n} |\eta_{h+m} - \eta_h| = 2^n \sin(\omega_{m,1}) \ldots \sin(\omega_{m,n});$$

alors

$$\operatorname{Log} \rho_m = n \operatorname{Log} 2 + \sum_{h=1}^{n} \operatorname{Log} \sin(\omega_{m,h}).$$

La fonction $y = -\operatorname{Log} \sin x$ est convexe pour $0 < x < \pi$, car $y'' = \frac{1}{\sin^2 x} > 0$. On a donc

$$\frac{1}{n} \sum_{h=1}^{n} \operatorname{Log} \sin(\omega_{m,h}) \leqq \operatorname{Log} \sin\left(\frac{1}{n} \sum_{h=1}^{n} \omega_{m,h}\right) = \operatorname{Log} \sin \frac{m\pi}{n}.$$

Par suite

$$\rho_m \leqq 2^n \left(\sin \frac{m\pi}{n}\right)^n \quad \text{et} \quad \left|\prod_{k \neq h} (\eta_h - \eta_k)\right| = \rho_1 \rho_2 \ldots \rho_{n-1} \leqq \rho^n,$$

avec

$$\rho = 2^{n-1} \sin \frac{\pi}{n} \sin \frac{2\pi}{n} \ldots \sin \frac{(n-1)\pi}{n}.$$

Or

$$\rho = \prod_{m=1}^{n-1} \left[i\left(e^{-i\frac{m\pi}{n}} - e^{i\frac{m\pi}{n}}\right)\right] = \prod_{m=1}^{n-1} (1 - \zeta^m), \qquad \text{où} \quad \zeta = e^{\frac{2i\pi}{n}}.$$

Ce dernier produit est égal à la valeur pour $z = 1$ de la dérivée de $z^n - 1$, c'est-à-dire à n; ce qui démontre le lemme.

Les relations (37) et (40) donnent

$$1 + Y \equiv 1 + \varepsilon\varepsilon''' z^{s-\nu-2} \equiv U^\star D \equiv U^\star D^\star W \equiv UD^\star.$$

Soient $a \geqq 1$ le degré et δ_i les zéros de $D^\star(z)$; on a $s - \nu - 2 = u + a \geqq 1$. Soient ξ_j les zéros de $U(z)$, (si $u = 0$, il n'y a pas de ξ_j). Les nombres δ_i et ξ_j sont tous différents et $|\delta_i| = |\xi_j| = 1$, car ils constituent l'ensemble des zéros de $1 + Y$. On a

$$\prod_i (z - \delta_i) \prod_j (z - \xi_j) \equiv \pm (1 + \varepsilon\varepsilon''' z^{s-\nu-2}) \tag{52}$$

$\left(\text{si } u = 0, \text{ le facteur} \prod_j (z - \xi_j) \text{ est à remplacer par } 1\right)$. En dérivant les deux membres de (52) par rapport à z et en remplaçant ensuite z par δ_k, k étant un indice fixe, on obtient

$$\prod_{i \neq k} (\delta_k - \delta_i) \prod_j (\delta_k - \xi_j) = \pm \varepsilon\varepsilon'''(u + a)\, \delta_k^{u+a-1},$$

d'où

$$\left|\prod_{i \neq k} (\delta_k - \delta_i)\right| |U(\delta_k)| = u + a.$$

Formons le produit membre à membre de ces relations pour toutes les valeurs de k, et appliquons le lemme 7 : il vient

$$(u+a)^a = \left|\prod_{i\neq k}(\delta_k-\delta_i)\right|\left|\prod_{k=1}^{a}\mathrm{U}(\delta_k)\right| \leqq a^a\left|\prod_{k=1}^{a}\mathrm{U}(\delta_k)\right|.$$

Or $\dfrac{u+a}{a}\geqq 1$, l'égalité n'ayant lieu que pour $u=0$. On a donc $\left|\prod_{k=1}^{a}\mathrm{U}(\delta_k)\right|\geqq 1$, l'égalité n'ayant lieu que pour $u=0$. On verrait de même que $\left|\prod_{k=1}^{a}\mathrm{V}(\delta_k)\right|\geqq 1$, l'égalité n'ayant lieu que pour $v=0$. Enfin $\mathrm{H}(z)$ est un polynome à coefficients entiers et les δ_k sont des entiers algébriques conjugués; $\prod_{k=1}^{a}\mathrm{H}(\delta_k)$ est donc un entier rationnel.

Or l'égalité (51) donne, pour $z=\delta_k$, zéro de $\mathrm{D}^*(z)$,

$$\delta_k = \mathrm{U}(\delta_k)\mathrm{V}(\delta_k)\mathrm{H}(\delta_k), \qquad \text{donc} \quad 1=\prod_{k=1}^{a}|\,\mathrm{U}(\delta_k)\mathrm{V}(\delta_k)\mathrm{H}(\delta_k)\,|.$$

Les inégalités que nous venons d'obtenir montrent que cette relation exige $u=v=0$, donc

$$\mathrm{U}(z)\equiv\mathrm{V}(z)\equiv 1.$$

Il ne nous reste donc plus qu'à étudier le cas $\mathrm{U}\equiv\mathrm{V}\equiv 1$. Les relations (29), (30), (34) et (35) montrent que $\varepsilon''=\varepsilon'''=1$, que $\mathrm{X}\equiv\mathrm{Y}\equiv\varepsilon z^{s-2}$ et que

$$(53)\qquad \mathrm{A}\equiv\mathrm{B}\equiv\mathrm{Q}+z\equiv\mathrm{P}+\varepsilon z^{s-1}.$$

Pour $k\neq 1$ et $k\neq s-1$, on a donc $q_k=\varepsilon q_{s-k}$; d'autre part rappelons la relation (27)

$$q_{s-1}=\varepsilon(q_1+1).$$

On a

$$\frac{\mathrm{P}}{\mathrm{Q}}\equiv\frac{\mathrm{Q}+z-\varepsilon z^{s-1}}{\mathrm{Q}}=1+z+u_2z^2+u_3z^3+\ldots,$$

avec

$$(54)\qquad u_2=-q_1;\qquad u_3=q_1^2-q_2-\varepsilon\ \text{ si }\ s=3;\qquad u_3=q_1^2-q_2\ \text{ si }\ s\geqq 4.$$

Le lemme 2 nous apprend enfin que

$$(55)\qquad u_2=-q_1=1\ \text{ ou }\ 2\qquad\text{et}\qquad u_3\leqq 3.$$

L'inégalité $|\mathrm{A}|\leqq|\mathrm{Q}|$ sur $|z|=1$ s'écrit $|\mathrm{Q}+z|\leqq|\mathrm{Q}|$, donc

$$(56)\qquad \begin{cases}\mathcal{R}\left(\dfrac{\mathrm{Q}}{z}+\dfrac{1}{2}\right)=\mathcal{R}\left[\dfrac{1}{z}+\left(q_1+\dfrac{1}{2}\right)+q_2z+\ldots+\varepsilon(q_1+1)z^{s-2}+\varepsilon z^{s-1}\right]\leqq 0\\ \text{sur}\ |z|=1.\end{cases}$$

Écrivons cette relation pour tous les zéros de $1 - \varepsilon z^{s-1}$ et sommons; il vient

$$q_1 + \frac{1}{2} + 1 \leqq 0, \qquad \text{d'où} \qquad q_1 \leqq -2.$$

Mais, d'après (55), on a $q_1 = -1$ ou -2; par suite

$$q_1 = -2. \tag{57}$$

De plus (54), (55) et (57) donnent alors

$$\begin{cases} \text{pour } s = 3 : & u_3 = 4 - q_2 - \varepsilon \leqq 3, \qquad \text{donc } q_2 \geqq 1 - \varepsilon; \\ \text{pour } s \geqq 4 : & u_3 = 4 - q_2 \leqq 3, \qquad \text{donc } q_2 \geqq 1. \end{cases} \tag{58}$$

Or, si $s = 3$, on a $q_2 = \varepsilon(q_1 + 1) = -\varepsilon$ en vertu de (27) et de (57); il y a contradiction avec (58); par suite $s = 3$ est impossible.

Si $s = 4$, on a

$$Q(z) \equiv 1 - 2z + q_2 z^2 - \varepsilon z^3 + \varepsilon z^4, \qquad \text{donc} \quad Q(1) = q_2 - 1 \geqq 0$$

d'après (58), et par suite $s = 4$ est aussi impossible.

Il ne reste plus qu'à examiner $s \geqq 5$. En tenant compte de (57), on peut alors écrire la relation (56) sous la forme

$$\mathcal{R}\left[\frac{1}{z} - \frac{3}{2} + \ldots + \varepsilon q_3 z^{s-4} + \varepsilon q_2 z^{s-3} - \varepsilon z^{-2} + \varepsilon z^{s-1}\right] \leqq 0 \qquad \text{sur} \quad |z| = 1. \tag{56 bis}$$

Cette relation, sommée pour les zéros de $1 - \varepsilon z^{s-3}$ donne

$$\text{pour } s = 5 : \quad -\frac{3}{2} + q_2 + \varepsilon \leqq 0, \qquad \text{donc} \quad q_2 \leqq 1 - \varepsilon,$$

$$\text{pour } s \geqq 6 : \quad -\frac{3}{2} + q_2 \leqq 0, \qquad \text{donc} \quad q_2 \leqq 1.$$

Il en résulte, d'après (58), que

$$\text{pour } s = 5 : \quad q_2 = 1 \quad \text{ou} \quad 2, \qquad \varepsilon = -1, \tag{59}$$

$$\text{pour } s \geqq 6 : \quad q_2 = 1. \tag{60}$$

La relation (56 *bis*), sommée pour les zéros de $1 + \varepsilon z^{s-4}$ donne

$$\text{pour } s = 6 : \quad -\frac{3}{2} - q_3 - \varepsilon \leqq 0, \qquad \text{donc} \quad q_3 \geqq -1 - \varepsilon, \tag{61}$$

$$\text{pour } s = 7 : \quad -\frac{3}{2} - q_3 + \varepsilon \leqq 0, \qquad \text{donc} \quad q_3 \geqq -1 + \varepsilon, \tag{62}$$

$$\text{pour } s \geqq 8 : \quad -\frac{3}{2} - q_3 \leqq 0, \qquad \text{donc} \quad q_3 \geqq -1. \tag{63}$$

Enfin, remarquons que sur $|z| = 1$, la quantité

$$\left(z + 1 + \frac{1}{z}\right)^2 \equiv z^2 + 2z + 3 + \frac{2}{z} + \frac{1}{z^2}$$

est réelle et positive ou nulle. On peut donc multiplier par cette quantité le premier membre de (56 *bis*) sous le signe $\mathcal{R}$. En sommant pour les zéros de $1 - \varepsilon z^{s-1}$ l'inégalité ainsi obtenue, il vient, en tenant compte de (60),

$$(64) \qquad \text{pour } s \geqq 6 : \quad \left(2 - \frac{9}{2} + 2 + q_3\right) + (1 - 2 + 3) \leqq 0, \qquad \text{donc} \quad q_3 \leqq -2.$$

Pour $s \geqq 8$, cette inégalité est en contradiction avec (63).

Il ne subsiste donc que les cas suivants :

Cas $s = 5$. — On a, d'après (59), deux possibilités :

ou bien $q_2 = 1$; alors

$$Q(z) \equiv 1 - 2z + z^2 - z^3 + z^4 - z^5 \equiv (1 - z - z^2)(1 - z)(1 + z^2 + z^4) - z^7,$$

donc $Q\left(\frac{1}{\theta_0}\right) = -\theta_0^{-7} < 0$ en contradiction avec $\theta < \theta_0$;

ou bien $q_2 = 2$; alors

$$Q(z) \equiv 1 - 2z + 2z^2 - 2z^3 + z^4 - z^5 \equiv (1 - z + z^2)(1 - z - z^3),$$

en contradiction avec l'irréductibilité de Q.

Cas $s = 6$. — On a, d'après (60), (61) et (64),

$$q_2 = 1, \qquad q_3 = -2, \qquad \varepsilon = 1,$$

d'où

$$Q(z) \equiv 1 - 2z + z^2 - 2z^3 + z^4 - z^5 + z^6 \equiv (1 - z - z^2)(1 - z + z^2 - 2z^3 - 3z^5) - 2z^6 - 3z^7,$$

donc $Q\left(\frac{1}{\theta_0}\right) = -2\theta_0^{-6} - 3\theta_0^{-7} < 0$, en contradiction avec $\theta < \theta_0$.

Cas $s = 7$. — On a, d'après (60), (62) et (64),

$$q_2 = 1, \qquad q_3 = -2, \qquad \varepsilon = -1,$$

d'où

$$Q(z) \equiv 1 - 2z + z^2 - 2z^3 + 2z^4 - z^5 + z^6 - z^7 \equiv (1 - z - z^2)(1 - z + z^2 - 2z^3 + z^4 - 2z^5) - 3z^7,$$

donc $Q\left(\frac{1}{\theta_0}\right) = -3\theta_0^{-7} < 0$, en contradiction avec $\theta < \theta_0$.

Nous avons ainsi démontré que, si $\theta < \theta_0$, il n'existe pas de polynome $A(z)$ satisfaisant aux conditions du théorème 1. Le nombre $\theta_0 = \frac{1 + \sqrt{5}}{2}$ est donc le plus petit élément de l'ensemble S'.