Séminaire Delange-Pisot-Poitou. Théorie des nombres

JOHN WILLIAM SCOTT CASSELS

Sommes de racines de l'unité

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 9, n° 2 (1967-1968), exp. n° 23, p. 1-16

<http://www.numdam.org/item?id=SDPP_1967-1968__9_2_A7_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
9e année, 1967/68, n° 23

13 mai 1968

SOMMES DE RACINES DE L'UNITÉ

par John William Scott CASSELS

1. - Soit $\underset{\sim}{Q}(N)$ le corps engendré par les racines n-ièmes de l'unité, et soit $\underset{\sim}{Q}(\infty) = \bigcup_N \underset{\sim}{Q}(N)$. Rappelons que $\underset{\sim}{Q}(N)$ est galoisien de degré $\Phi(N)$ (fonction d'Euler) et que

$$\underset{\sim}{Q}(M) \cap \underset{\sim}{Q}(N) = \underset{\sim}{Q}(L) \quad , \tag{1.1}$$

où

$$L = (M , N) \quad . \tag{1.2}$$

On sait que les racines N-ièmes de l'unité engendrent les entiers de $\underset{\sim}{Q}(N)$ comme groupe additif, c'est-à-dire que chaque entier $\theta \in \underset{\sim}{Q}(N)$ a la forme

$$\theta = \sum_\rho n_\rho \rho \ , \qquad n_\rho \in \underset{\sim}{Z} \ , \quad \rho^N = 1 \quad . \tag{1.3}$$

Si $2|N$, nous pouvons supposer que les $n_\rho \geqslant 0$, parce que $(-\rho)^N = 1$. Par conséquent, chaque entier θ de $\Omega(\infty)$ (entier cyclotomique) a la forme

$$\theta = \sum_{j=1}^{k} \rho_j \ , \qquad \rho_j \in \underset{\sim}{P} \ , \tag{1.4}$$

où $\underset{\sim}{P}$, dorénavant, désignera l'ensemble des racines de l'unité.

Dans la première partie de ma conférence, je donnerai des résultats de H. B. MANN [5] et de A. SCHINZEL [7] sur l'unicité de la représentation (1.4). Dans la deuxième partie, j'exposerai des travaux de H. DAVENPORT et A. SCHINZEL [3], A. JONES [4] et moi-même [2], sur le comportement des valeurs absolues des conjugués des θ de la forme (1.4). Ces travaux sont inspirés par des expériences numériques de R. M. ROBINSON [6].

Pour achever cette introduction, nous énonçons deux lemmes banaux qui sont néanmoins fondamentaux pour presque tout ce qui suit. La lettre p désigne toujours un nombre premier.

LEMME 1.1. - *Soit* $N = p^L N_0 = pN_1$ *où* $p \nmid N_0$ *et* $L > 1$. *Soit* σ *une racine* p^L*-ième primitive de l'unité. Chaque* $\beta \in \underset{\sim}{Q}(N)$ *est uniquement de la forme*

$$\beta = \sum_{j=0}^{p-1} \alpha_j \sigma^j \ , \qquad \alpha_j \in \underset{\sim}{Q}(N_1) \quad . \tag{1.5}$$

Si β est entier, les α_j sont entiers.

Car $\Omega(N) = \Omega(N_1)(\sigma)$ est une extension de degré p .

LEMME 1.2. - Soit $N = pN_1$ où $p \nmid N_1$, et soit σ une racine p-ième de l'unité. Chaque $\beta \in \underset{\sim}{Q}(N)$ a la forme

$$\beta = \sum_{j=0}^{p-1} \alpha_j \sigma^j , \qquad \alpha_j \in \underset{\sim}{Q}(N_1) \quad . \tag{1.6}$$

Si (1.6) est une telle représentation, toute autre représentation a la forme

$$\beta = \sum \alpha'_j \sigma^j \quad , \tag{1.7}$$

où

$$\alpha_0 - \alpha'_0 = \alpha_1 - \alpha'_1 = \ldots = \alpha_{p-1} - \alpha'_{p-1} \quad . \tag{1.8}$$

Si β est entier, on peut choisir les α_j entiers.

En effet, $\Omega(N) = \Omega(N_1)(\sigma)$ est une extension de degré $p - 1$ et

$$\sigma^0 + \sigma^1 + \ldots + \sigma^{p-1} = 0 \quad . \tag{1.9}$$

Notons que dans les deux cas, si $\rho \in \underset{\sim}{Q}(N)$ est une racine de l'unité, nous avons une représentation $\rho = \alpha\sigma^j$, où $j = j(\rho)$, et $\alpha = \alpha_j$ est une racine de l'unité.

2. - Une relation

$$\sum_{j=0}^{k} \rho_j = 0 , \qquad \rho_j \in \underset{\sim}{P} \tag{2.1}$$

s'appelle minimale, s'il n'y a pas de sous-ensemble propre non-vide K de $\{0 , 1 , \ldots , k\}$ tel que

$$\sum_{j \in K} \rho_j = 0 \quad . \tag{2.2}$$

Des relations (2.1), nous pouvons supposer que $\rho_0 = 1$, en remplaçant les ρ_j par $\rho_0^{-1} \rho_j$. Le théorème, qui suit, permet d'énoncer toutes les relations (2.1) minimales avec $\rho_0 = 1$ pour un k fixe donné à l'avance et démontre qu'il y en a un nombre fini seulement. Nous désignons dorénavant par $N(\rho)$ l'ordre de la racine ρ de l'unité.

THÉORÈME 2.1 (MANN [5]). - Soit (2.1) une relation minimale avec $\rho_0 = 1$, et posons

$$N = \text{p. p. c. m. } (N(\rho_j)) \quad . \tag{2.3}$$

Alors N n'est pas divisible par le carré d'un nombre premier (quadratfrei), et tout facteur premier de N est $\leqslant k+1$.

La démonstration de MANN est élégante.

1er cas. - Supposons que $p^2 | N$, et utilisons les notations $N = p^L N_0 = pN_1$ et σ du lemme 1.1. Nous avons

$$\rho_j = \tau_j \sigma^{i(j)} \quad . \tag{2.4}$$

où $\tau_j \in \underset{\sim}{Q}(N_1)$ et $0 \leqslant i(j) < p$. Par conséquent,

$$0 = \sum \rho_j = \sum_{i=0}^{p-1} T_i \sigma^i \quad . \tag{2.5}$$

où

$$T_i = \sum_{i(j)=i} \tau_j \in \underset{\sim}{Q}(N_1) \quad . \tag{2.6}$$

D'après le lemme 1.1, nous avons

$$T_i = 0 \quad . \tag{2.7}$$

L'ensemble $\{j \mid i(j) = 0\}$ est un sous-ensemble de $\{0 , 1 , \ldots , k\}$ (parce que $p^L \| N$) et non vide (parce qu'il contient 0). Par conséquent, (2.1) n'est pas minimale, ce qui est contradictoire.

2e cas. - Supposons que $p \| N$, où $p > k+1$. Utilisons les notations $N = pN_1$ et σ du lemme 1.2, et les notations (2.4), (2.5), (2.6) ci-dessus. Puisque $p > k+1$, il existe un i_0 tel que $\{j \mid i(j) = i_0\}$ est vide, et par conséquent

$$T_{i_0} = 0 \quad . \tag{2.8}$$

D'après le lemme 1.2, l'équation (2.5) implique

$$T_0 = T_1 = \ldots = T_{p-1} \quad . \tag{2.9}$$

La relation

$$T_0 = 0 \tag{2.10}$$

est encore en contradiction avec l'hypothèse que (2.1) soit minimale.

Par des méthodes semblables, on peut démontrer le théorème suivant.:

THÉORÈME 2.2 (SCHINZEL [7]). - Soient $\theta \in Q(\infty)$ et $k \in \underset{\sim}{Z}^+$ fixes. Les trois conditions suivantes sont équivalentes :

(a) Il existe un nombre infini de représentations

$$\theta = \sum_{j=1}^{k} \rho_j , \qquad \rho_j \in \underset{\sim}{P} \ ; \tag{2.11}$$

(b) Il existe une relation

$$\theta = \sum_{j=1}^{k-2} \lambda_j , \qquad \lambda_j \in \underset{\sim}{P} \ ; \tag{2.12}$$

(c) Il existe une relation

$$\theta = \sum_{j=1}^{\ell} \mu_j , \qquad \mu_j \in \underset{\sim}{P} , \quad \ell \leqslant k - 2 \ . \tag{2.13}$$

Démonstration.

(b) $\Longrightarrow$ (c). C'est évident.

(c) $\Longrightarrow$ (b) . Soit $\nu^3 = 1$, $\nu \neq 1$. Puisque

$$1 + \nu + \nu^2 = 0 , \qquad 1 + (-1) = 1 \ , \tag{2.14}$$

il existe pour chaque $m \geqslant 1$ une relation

$$\sum_{0}^{m} \nu_j = 1 , \qquad \nu_j \in \{1 , -1 , -\nu , -\nu^2\} \in \underset{\sim}{P} \ . \tag{2.15}$$

Si $\ell \neq k - 2$ dans (2.13), nous posons $m = k - 2 - \ell$,

$$\begin{cases} \lambda_j = \mu_j & (j < \ell) \\ \lambda_j = \mu_\ell \ \nu_{j-\ell} & (\ell \leqslant j \leqslant k - 2) \end{cases} \ .$$

(b) $\rightarrow$ (a) . Il suffit de prendre

$$\begin{cases} \rho_j = \lambda_j & (j \leqslant k - 2) \\ \rho_{k-1} = -\rho_k \in \underset{\sim}{P} \ . \end{cases}$$

(a) $\rightarrow$ (c) . Fixons une représentation

$$\theta = \sum_{j=1} \rho_j^* , \qquad \rho_j^* \in \underset{\sim}{P} \ , \tag{2.16}$$

et considérons l'infinité des relations

$$\sum_{j=1}^{k} \rho_j^* + \sum_{j=1}^{k} (-\rho_j) = 0 \ . \tag{2.17}$$

Elles ne sont pas nécessairement minimales. Posons

$$(2.18) \qquad \begin{cases} N^* = \text{p. p. c. m. } (N(\rho_j^*)) \\ N = \text{p. p. c. m. } (N(\rho_j)) \end{cases} ,$$

et considérons les deux cas suivants :

1er cas. - Il existe p , $L > 1$ tels que $p^L \| N$, $p^L \nmid N^*$. Comme dans le premier cas de la démonstration du théorème précédent, nous avons

$$(2.19) \qquad \sum_{j=1}^{k} \rho_j^* + \sum_{\rho_j \in \underset{\sim}{Q}(N_1)} (-\rho_j) = 0 ,$$

puisque $\rho_j^* \in \underset{\sim}{Q}(N_1)$, c'est-à-dire

$$\theta = \sum_{\rho_j \in \underset{\sim}{Q}(N_1)} \rho_j .$$

Nous avons

$$\text{Card}\{j \mid \rho_j \in \underset{\sim}{Q}(N_1)\} \leqslant k - 2 ,$$

parce que $\{j \mid \rho_j \in \underset{\sim}{Q}(\rho)\}$ n'est pas vide, et

$$\sum_{\rho_j \notin \underset{\sim}{Q}(\rho)} \rho_j = 0 .$$

2e cas. - Il existe $p > 2k$ tel que $p \mid N$, $p \nmid N^*$. Ce cas se démontre comme le deuxième cas de la démonstration précédente. Les détails sont laissés au lecteur à titre d'exercice.

Comme il existe une infinité de représentations (2.11), nous avons nécessairement un des deux cas ci-dessus pour une représentation convenablement choisie.

C. Q. F. D.

La démonstration de SCHINZEL [7] est tout-à-fait différente. Il considère les représentations (2.11) minimales (dans le sens évident) pour lesquels il démontre la majoration

$$(2.20) \qquad N < d(2\log d + 200k^2 \log 2k)^{20k^2} ,$$

où d est le degré de θ sur $\underset{\sim}{Q}$. Le membre de droite de (2.20) dépend seulement de θ et k , pas de la représentation. Par conséquent, toutes les représentations (2.11) de θ , sauf un nombre fini, ne sont pas minimales. Une représentation non minimale donne (2.13). La démonstration de (2.20) est assez compliquée.

3. - Nous considérons maintenant les valeurs absolues des entiers cyclotomiques. Pour un nombre β algébrique quelconque, posons, comme d'habitude,

$$|\overline{\beta}| = \max|\beta'| \quad , \tag{3.1}$$

où β' parcourt les conjugués de β . Si $\beta \neq 0$ est un entier, nous avons

$$\prod |\beta'| = |\text{Norm } \beta| \in \underset{\sim}{Z} \neq 0 \ ,$$

et par conséquent,

$$|\overline{\beta}| \geqslant 1 \quad . \tag{3.2}$$

Un théorème ultraclassique ([1]) de KRONECKER dit que $|\overline{\beta}| = 1$, pour un entier β , implique que β est une racine de l'unité. Il existe des entiers β qui ne sont pas racines de l'unité, et pour lesquels $|\overline{\beta}|$ est arbitrairement proche de 1 , par exemple $\beta = 2^{1/n}$. A. SCHINZEL et H. ZASSENHAUS [8] ont émis le conjecture qu'il existe un $c > 0$ (Weltkonstante !) tel que $|\overline{\beta}| \geqslant 1 + \frac{c}{n}$ pour un entier β de degré n , qui n'est pas une racine de l'unité. Cependant, ils n'ont pu démontrer que des résultats bien plus faibles (voir aussi CASSELS [1]). Pour les entiers cyclotomiques, on a des résultats beaucoup plus forts.

THÉORÈME 3.1 (R. M. ROBINSON [6]). - Soit β un entier cyclotomique qui n'est pas une racine de l'unité. Alors

$$|\overline{\beta}| \geqslant 2^{1/2} \quad . \tag{3.3}$$

La constante $2^{1/2}$ est la meilleure possible comme on le voit sur l'exemple des entiers cyclotomiques

$$(*) \qquad 1 + i \ , \qquad \tfrac{1}{2}(1 + (-7)^{1/2}) \ , \qquad \tfrac{1}{2}((-3)^{1/2} + 5^{1/2}) \quad .$$

La démonstration de ROBINSON est si amusante que je la donne ici, quoique je démontrerai quelque chose de plus fort dans le paragraphe 4. De façon générale, ROBINSON considère les β pour lesquels $|\overline{\beta}|^2 \leqslant 4$.

Posons

$$(**) \qquad \gamma = |\beta|^2 - 2 \ .$$

([1]) Un résultat est "classique", suivant l'usage courant du mot en France, s'il est connu depuis plus de 5 ans. Je propose à l'Académie Française le mot "ultraclassique" pour la signification (ultra)classique du mot "classique".

Parce que le groupe de Galois d'une extension cyclotomique est abélien, les conjugués γ' de γ sont de la forme

$$\gamma' = |\beta'|^2 - 2 \ ,$$

où β' est un conjugué de β . Par conséquent,

(*) $$|\overline{\gamma}| \leqslant 2 \ .$$

Parce que γ est réel, un théorème connu de Kronecker ([2]) implique que

$$\gamma = 2\cos(2\pi r/N) \ , \qquad r \ , N \in \underset{\sim}{Z} \ , \ (r \ , N) = 1 \ .$$

D'après (**), nous avons

(**) $$|\overline{\beta}|^2 = \sup(2 + \gamma')$$

$$= \sup_{(s,N)=1} (2 + 2\cos(2\pi s/N)) \ .$$

Par conséquent, ou bien $|\overline{\beta}|^2 = 1$ (c'est-à-dire β est une racine de l'unité), ou bien $|\overline{\beta}|^2 \geqslant 2$.

Nous dirons que deux entiers β_1 , β_2 , cyclotomiques, sont <u>équivalents</u> s'il existe une racine ρ de l'unité et un conjugué β_2' de β_2 tels que

(3.4) $$\beta_1 = \rho\beta_2 \ .$$

C'est bien une relation d'équivalence, et l'on a

(3.5) $$|\overline{\beta_1}| = |\overline{\beta_2}|$$

pour des β_1 , β_2 équivalents.

Par les méthodes du paragraphe 4, on démontre sans peine que (*) sont les seuls cas, à une équivalence près, où le signe d'égalité est nécessaire. L'équation (**) montre alors que $|\overline{\beta}|^2 \geqslant 3$ pour tout autre nombre cyclotomique β

Dans le même papier [6], ROBINSON signale des calculs de $|\overline{\beta}|$ pour des entiers cyclotomiques β , et se permet des conjectures qui ont fait le point de départ des travaux de H. DAVENPORT et A. SCHINZEL [3], A. JONES [4], et moi-même [2].

Le théorème suivant a été conjecturé par RONBINSON [6].

([2]) <u>Démonstration du théorème de Kronecker</u>. - Posons $\delta^2 + \gamma\delta + 1 = 0$. (*) implique que $|\delta'| = 1$ pour tous les conjugués δ' de δ . D'après le théorème de Kronecker, cité ci-dessus, ceci implique que δ est une racine de l'unité, disons $\delta = \exp(2\pi ir/n)$ et $\gamma = \delta + \overline{\delta}$.

THÉORÈME 3.2 (DAVENPORT et SCHINZEL [3]). - Soit β la somme de n racines de l'unité $(n \leqslant 3)$. Les β, pour lesquels

$$|\beta|^2 \leqslant 5 \quad , \tag{3.6}$$

sont précisément les β qui satisfont à une des trois conditions suivantes :

(A) β est représentable comme somme de n racines de l'unité $(n \leqslant 2)$;

(B) β est équivalent à

$$1 + \rho + i\rho^{-1} \quad , \qquad (i^2 = -1) \tag{3.7}$$

pour une racine ρ de l'unité convenable ;

(C) β est équivalent à un élément d'un ensemble fini.

C'est évident que (A) implique

$$|\beta| \leqslant 2 < 5^{1/2} \quad ,$$

et que (B) implique

$$|\beta|^2 = 1 + 4\cos^2 2\pi\theta \leqslant 5 \quad ,$$

où $\theta = \exp 2\pi i\theta$. Il reste (seulement !) à "marcher" dans le sens inverse. La démonstration de DAVENPORT et SCHINZEL [3] est assez pénible et utilise les méthodes analytique de VINOGRADOFF. Il n'ont pas réussi à donner l'ensemble fini exceptionnel de (C).

A. JONES [4] a donné une démonstration beaucoup plus simple, et a déterminé l'ensemble exceptionnel de (C) en utilisant la géométrie des nombres. Avec les mêmes méthodes, il a démontré aussi le théorème qui suit.

THÉORÈME 3.3 (A. JONES [4]). - Soit

$$D \in \underset{\sim}{R} \quad , \qquad D < 9 \tag{3.8}$$

donné à l'avance. Il existe un $H = H(D) \in \underset{\sim}{Z}$ tel que les β, qui sont la somme de n racines de l'unité $(n \leqslant 3)$ et pour lesquels

$$|\beta|^2 \leqslant D \quad , \tag{3.9}$$

satisfont à une des conditions suivantes :

(A') β est la somme de n racines de l'unité $(n \leqslant 2)$;

(B') β est équivalent à

$$1 + \rho_1 + \rho_2 \quad , \qquad \rho_1 \, , \, \rho_2 \in \underset{\sim}{P} \quad , \tag{3.10}$$

où

$$\rho_1^{h_1}\ \rho_2^{h_2} = 1 \tag{3.11}$$

pour des h_1 , $h_2 \in \underset{\sim}{Z}$ convenables, avec

$$0 < \max\{|h_1| , |h_2|\} \leqslant H \ ; \tag{3.12}$$

(C') β est équivalent à un élément d'un ensemble fini (qui dépend évidemment de D).

Dans la suite du paragraphe 3, j'esquisserai la démonstration du théorème 3.3. Dans le paragraphe 4, j'étudierai les principes d'une démonstration prouvant que le théorème 3.2 reste valable pour les entiers β cyclotomiques, qui ne sont pas sommes des n racines de l'unité $(n \leqslant 3)$.

[En revanche, le théorème 3.3 "canule" pour les β cyclotomiques généraux, comme le démontre les

$$\beta = (1 + i)(1 + \rho) , \qquad \rho \in \underset{\sim}{P} , \tag{3.13}$$

tels que $|\beta|^2 \leqslant 8$.]

Démonstration du théorème 3.3. - Sans restreindre à la généralité, nous supposerons que

$$\beta = 1 + \rho_1 + \rho_2 , \qquad \rho_1 , \rho_2 \in \underset{\sim}{P} . \tag{3.14}$$

Posons

$$\rho_j = \exp 2\pi i\theta_j , \qquad (j = 1 , 2) , \tag{3.15}$$

où

$$\theta_j = u_j/v_j , \qquad u_j , v_j \in \underset{\sim}{Z} , \qquad (u_j , v_j) = 1 , \qquad v_j > 0 . \tag{3.16}$$

Les conjugués de β sont les

$$\beta' = 1 + \rho_1^r + \rho_2^r , \tag{3.17}$$

où

$$r \in \underset{\sim}{Z} , \qquad (r , v_1 v_2) = 1 . \tag{3.18}$$

Choisissons $\delta > 0$, tel que

$$|1 + 2\exp 2\pi i\delta|^2 > D . \tag{3.19}$$

Il est évident que le théorème 3.3 est une conséquence immédiate du théorème qui suit. [Comme d'habitude, nous écrivons

$$\|x\| = \inf_{n \in \underset{\sim}{Z}} |x + n| \ . \ ] \tag{3.20}$$

THÉORÈME 3.3 (bis). - Soit $\frac{1}{2} > \delta > 0$ donné à l'avance. Il existe un $H = H(\delta) \in \underset{\sim}{Z}$ tel que tout couple (θ_1 , θ_2) satisfait à, au moins, une des conditions suivantes :

(a) Il existe un r qui satisfait à (3.18) pour lequel

$$\|r\theta_1\| < \delta \ , \qquad \|r\theta_2\| < \delta \ ; \tag{3.21}$$

(b) Il existe $h_1 , h_2 \in \underset{\sim}{Z}$ tels que

$$h_1 \theta_1 + h_2 \theta_2 \equiv 0 \pmod 1 \ , \tag{3.22}$$

$$0 < \max|h_j| \leqslant H \ ; \tag{3.23}$$

(c) Le couple (θ_1 , θ_2) est congru modulo 1 à un élément d'un ensemble fixe.

Notons que l'on peut faire disparaître la condition (c) en remplaçant H par une constante plus grande. Mais la démonstration donne naturellement les trois conditions. Notons également que (3.17), (3.19) et (3.21) impliquent

$$|\overline{\beta}|^2 \geqslant |\beta'|^2 > D \ .$$

Démonstration du théorème 3.3 (bis). - Nous démontrerons le théorème sous la condition

$$H = 2([\delta^{-1}] + 1) \ . \tag{3.24}$$

Soit Λ_0 le réseau des points entiers dans l'espace numérique $\underset{\sim}{R}^2$ (coordonnées x , y), et soit Λ le réseau engendré par les points de Λ_0 et le point (θ_1 , θ_2). L'indice de Λ_0 dans Λ est

$$w = v_1 \, v_2 \ / \ \text{p. g. c. d.} \ (v_1 , v_2) \ , \tag{3.25}$$

[v_1 , v_2 donnés par (3.16)], et par conséquent,

$$\det(\Lambda) = w^{-1} \ . \tag{3.26}$$

D'après un théorème ultraclassique de MINKOVSKI, il existe une base

$$x^{(j)} = (x^{(j)} , y^{(j)}) \ , \qquad (j = 1 , 2) \tag{3.27}$$

de Λ telle que

$$0 < \lambda_1 \leqslant \lambda_2 \ , \qquad \lambda_1 \, \lambda_2 \leqslant \det(\Lambda) = w^{-1} \ , \tag{3.28}$$

où

$$\lambda_j = \max\{|x^{(j)}|\ ,\ |y^{(j)}|\}\ , \qquad (j = 1\ ,\ 2)\ . \tag{3.29}$$

En particulier, (3.28) implique

$$\lambda_1 \leqslant w^{-1/2}\ . \tag{3.30}$$

1er cas.

$$\lambda_1 \leqslant Hw^{-1} \tag{3.31}$$

Nous avons

$$xy^{(1)} - yx^{(1)} \equiv 0 \pmod{w^{-1}}\ .$$

pour tout $(x\ ,\ y) \in \Lambda$, en particulier

$$\theta_1 y^{(1)} - \theta_2 x^{(1)} \equiv 0 \pmod{w^{-1}}\ . \tag{3.32}$$

Posons $wx^{(1)} = h_2 \in \underset{\sim}{Z}$, $wy^{(1)} = -h_1 \in \underset{\sim}{Z}$. Alors, (3.31) (resp. (3.32)) donnent (3.23) (resp. (3.22)), et nous avons l'énoncé (b) du théorème.

Il nous reste seulement le cas suivant :

2e cas.

$$\lambda_1 \geqslant Hw^{-1}\ , \tag{3.33}$$

ce qui implique

$$\lambda_1 \leqslant w^{-1/2}\ ; \qquad \lambda_2 \leqslant H^{-1} \leqslant \tfrac{1}{2}\delta\ , \tag{3.34}$$

d'après (3.28), (3.24) et (3.30). Soient

$$x^{(j)} \equiv r_j(\theta_1\ ,\ \theta_2) \pmod{\Lambda_0}\ ,$$

de sorte que $(r_1\ ,\ r_2\ ,\ w) = 1$ parce que $x^{(1)}\ ,\ x^{(2)}$ est une base.

D'après un théorème connu depuis Adam et Eve, il existe un $v \in \underset{\sim}{Z}$ satisfaisant à

$$(vr_1 + r_2\ ,\ w) = 1\ , \qquad |v| < \tfrac{1}{2}\,\delta w^{1/2} \tag{3.35}$$

pourvu que

$$w \geqslant w_0 = w_0(\delta)\ . \tag{3.36}$$

Les $w < w_0$ donne l'ensemble exceptionnel fixe de la partie (c) de l'énoncé. Si $w \geqslant w_0$, l'entier $r = vr_1 + r_2$ satisfait aux conditions de la partie (a) de

l'énoncé par (3.28), (3.32) et (3.35).

C. Q. F. D.

La démonstration de JONES [4] du théorème 3.2 est essentiellement la démonstration du théorème 3.3 ci-dessus pour un δ convenable, suivie par la considération de $|\overline{\beta}|$ pour les β qui satisfont à (3.10), (3.11), (3.12) (pas difficile, au moins en principe). Cependant, il a "dû" utiliser beaucoup d'astuces pour abréger le calcul (par exemple : utilisation d'ellipses dans le théorème de Minkowski), ce qui obscurcit la marche générale de la démonstration.

4. - Je viens de démontrer (sauf erreur !) que les conclusions du théorème 3.2 sont aussi valables pour les entiers cyclotomiques β qui ne sont pas la somme de n racines de l'unité $(n \leqslant 3)$ (CASSELS [2]). Ces β paraissent être assez difficiles à manier, quoique en général ils satisfont sans doute à des estimations bien plus fortes que les estimations voulues.

L'idée de base est d'utiliser le carré moyen

$$\mathfrak{M}(\beta) = \sum_{\beta'} |\beta'|^2 \Big/ \sum_{\beta'} 1 \quad , \tag{4.1}$$

pour les conjugués β' de β. Bien entendu,

$$|\overline{\beta}|^2 \geqslant \mathfrak{M}(\beta) \quad . \tag{4.2}$$

La fonction $\mathfrak{M}(\beta)$ de β est bien plus facile à manier que $|\overline{\beta}|$. La démonstration de mon théorème est trop compliquée pour que je la donne ici : elle exige des estimations assez délicates. Je veux maintenant utiliser des méthodes semblables pour démontrer quelques résultats plus forts que le théorème 3.1 de ROBINSON [6].

Commençons par quelques lemmes triviaux.

LEMME 4.1.

$$\mathfrak{M}(\beta) \geqslant 1 \tag{4.3}$$

pour un entier β algébrique. Car $|\text{Norm } \beta| \geqslant 1$.

LEMME 4.2. - Utilisons les notations du lemme 1.1. Alors

$$\mathfrak{M}(\beta) = \sum_{j=0}^{p-1} \mathfrak{M}(\alpha_j) \quad . \tag{4.4}$$

Démonstration. - Nous avons

$$\sum_{\substack{\beta' \text{ conjugué} \\ \text{de } \beta \text{ sur } \mathbb{Q}(N_1)}} |\beta'|^2 = \sum_{\xi^p=1} \Big|\sum_{j=0}^{p-1} \alpha_j \xi^j \sigma^j\Big|^2$$

$$= \sum_{j=0}^{p-1} |\alpha_j|^2 \quad ;$$

d'où (4.4) en prenant les moyennes des conjugués pour $\mathbb{Q}(N_1)/\mathbb{Q}$.

LEMME 4.3. - Utilisons les notations du lemme 1.2. Alors,

$$(4.5) \qquad (p-1)\mathfrak{M}(\beta) = \sum_{i,j} \mathfrak{M}(\alpha_i - \alpha_j) \quad .$$

Démonstration. - Elle se fait de façon identique à celle du lemme 4.2.

COROLLAIRE 1. - Supposons en outre que β est entier et que

$$(4.6) \qquad \mathfrak{M}(\beta) < \frac{1}{4}(p+3) \quad .$$

Il existe un $\alpha \in \mathbb{Q}(N_1)$ pour lequel

$$\mathrm{Card}\{j \mid \alpha_j = \alpha\} \geqslant \frac{1}{2}(p+1) \quad .$$

Démonstration. - D'après (4.3) et (4.5), nous avons

$$(p-1)\mathfrak{M}(\beta) \geqslant \sum_{\alpha_i \neq \alpha_j} 1 \quad ,$$

d'où le résultat découle, par un raisonnement facile.

COROLLAIRE 2. - Même suppositions que pour le corollaire 1. Alors il existe une représentation

$$(4.7) \qquad \beta = \sum_{j=0}^{p-1} \alpha_j^* \sigma^j \quad , \qquad \alpha_j^* \in \mathbb{Q}(n_1)$$

de β pour laquelle $\frac{1}{2}(p-1)$ au plus des α_j^* sont non nuls.

Démonstration.

$$(4.8) \qquad \alpha_j^* = \alpha_j - \alpha \quad .$$

Nous écrirons désormais (4.7) sous la forme

$$(4.9) \qquad \beta = \sum_{j=1}^{X} \gamma_j \sigma^{r_j} \quad ,$$

où

$$(4.10)\quad X \leqslant \frac{1}{2}(p-1)\ ; \qquad 0 \neq \gamma_j \in \underset{\sim}{Q}(N_1)\ ; \qquad r_i \not\equiv r_j \pmod{p} \quad \text{pour} \quad i \neq j\ .$$

L'équation (4.5), avec ces notations, devient

$$(4.11_1)\qquad (p-1)\mathfrak{M}(\beta) = (p-X)\sum_j \mathfrak{M}(\gamma_j) + \sum_{i,j} \mathfrak{M}(\gamma_i - \gamma_j)$$

$$(4.11_2)\qquad \geqslant (p-X)\sum_j \mathfrak{M}(\gamma_j)$$

$$(4.11_3)\qquad \geqslant (p-X)X$$

Nous avons encore besoin d'une définition. Pour un entier β cyclotomique, posons $N(\beta) = N'$ si $\beta \in \underset{\sim}{Q}(N')$, mais $\beta \notin \underset{\sim}{Q}(N'')$ pour $0 < N'' < N'$. Nous disons que β est <u>minimal</u> si

$$N(\rho\beta) \geqslant N(\beta) \qquad (\text{tous les } \rho \text{ appartenant à } \underset{\sim}{P})\ .$$

Evidemment, tout β a la forme

$$\beta = \rho\beta^*\ , \qquad \rho \in \underset{\sim}{P}\ , \qquad \beta^* \text{ minimal.}$$

Enonçons maintenant les résultats principaux de ce paragraphe 4.

THÉORÈME 4.1. - <u>Soit</u> β <u>un entier cyclotomique</u>.

(i) $\mathfrak{M}(\beta) \geqslant \frac{3}{2}$ <u>si</u> β <u>n'est pas une racine de l'unité</u> ;

(ii) $\mathfrak{M}(\beta) \geqslant 2$ <u>si</u> β <u>n'est pas la somme de</u> n <u>racines de l'unité</u> $(n \leqslant 2)$.

<u>Démonstration</u>. - Sans restreindre à la généralité, nous supposons que β est minimal.

<u>1er cas</u> [(i) et (ii)]. - Il existe un p pour lequel $p^2 | N(\beta)$. Nous utilisons les notations des lemmes 4.2 et 1.1, avec $N = N(\beta)$. Deux des α_j au moins sont non nuls par la minimalité de β, et par conséquent, le lemme 4.1 donne

$$\mathfrak{M}(\beta) = \sum \mathfrak{M}(\alpha_j) \geqslant 2\ .$$

Nous supposerons donc, dans ce qui suit, que $N(\beta)$ est "quadratfrei". Nous démontrerons (i) puis nous utiliserons (i) pour la démonstration de (ii).

<u>2e cas</u> [(i) et (ii)]. - $N(\beta) = 3$, c'est-à-dire β est un entier de $\underset{\sim}{Q}(3)$. Alors

$$|\beta|^2 = \mathfrak{M}(\beta) = |\beta|^2 \geqslant 3\ ,$$

si β n'est pas une racine de l'unité.

3e cas [(i)]. - Il existe un $p \geqslant 5$ avec $p|N(\beta)$. D'après le lemme 4.3, corollaire 2, nous avons la situation (4.9), (4.10), (4.11), où $X \geqslant 2$ à cause de la minimalité de β . D'après (4.11_3) , nous avons

$$\mathfrak{M}(\beta) \geqslant \frac{(p - X)X}{p - 1} \geqslant \frac{(p - 2)2}{p - 1} \geqslant \frac{(5 - 2)2}{5 - 1} = \frac{3}{2} \quad .$$

Nous n'avons plus maintenant qu'à démontrer (ii), en utilisant (i).

4e cas [(ii)]. - $p \geqslant 5$, $X \geqslant 3$. Alors $p \geqslant 2X + 1 \geqslant 7$, et

$$\mathfrak{M}(\beta) \geqslant \frac{(p - X)X}{p - 1} \geqslant \frac{(7 - 3)3}{7 - 1} = 2 \quad .$$

5e cas [(ii)]. - $p \geqslant 5$, $X = 2$, $\gamma_1 = \gamma_2$. Si $\mathfrak{M}(\gamma_1) = \mathfrak{M}(\gamma_2) = 1$, l'équation (4.9) implique que β est la somme de deux racines de l'unité. Sinon nous avons $\mathfrak{M}(\gamma_1) = \mathfrak{M}(\gamma_2) \geqslant 3/2$ et (4.11_2) donne $\mathfrak{M}(\beta) \geqslant 9/4 > 2$.

6e cas [(ii)]. - $p \geqslant 5$, $X = 2$, $\gamma_1 \neq \gamma_2$. Si $\mathfrak{M}(\gamma_1) = \mathfrak{M}(\gamma_2) = 1$, nous avons une représentation comme somme de deux racines de l'unité. Sinon (4.11_1) nous donne

$$(p - 1)\mathfrak{M}(\beta) \geqslant (p - 2)(1 + \tfrac{3}{2}) + 1 \quad ,$$

i. e.

$$\mathfrak{M}(\beta) \geqslant \frac{5p - 3}{2(p - 1)} > 2 \quad .$$

C. Q. F. D.

Notons que les constantes dans le théorème 4.1 sont les meilleures possibles parce que

$$\mathfrak{M}(1 + \lambda) = \frac{3}{2} \quad , \qquad \text{où} \quad \lambda^5 = 1 \tag{4.12}$$

et

$$\mathfrak{M}(\tfrac{1}{2}(-3)^{1/2} + \tfrac{1}{2}5^{1/2}) = \mathfrak{M}(\tfrac{1}{2} + \tfrac{1}{2}(-7)^{1/2}) = 2 \quad . \tag{4.13}$$

Avec des méthodes analogues, on démontre qu'il existe des majorations plus fortes pour des β non équivalents aux β de (4.12), (4.13). [Les cas d'égalité sont "isolés".]

Notons aussi que le théorème 4.1(ii) implique le théorème 3.1, parce que le théorème 3.1 est banal pour les $\beta = \rho_1 + \rho_2$ $(\rho_1 , \rho_2 \in \underset{\sim}{P})$.

Je ne connais pas la plus grande constante M_3 telle que $\mathfrak{M}(\beta) \geqslant M_3$ si β n'est pas la somme des n racines de l'unité $(n \leqslant 3)$, mais je crois posséder une démonstration de l'existence d'une suite $M_m^* \to \infty$ $(m \to \infty)$ telle que

$$\mathfrak{M}(\beta) \geqslant M_m^* \ ,$$

ce qui entraîne que β_n n'est pas la somme des n racines de l'unité $(n \leqslant m)$, mais la vie de Paris est si mouvementée que je n'ai pas eu le temps pour la mettre au point.

Pour finir, notons que les sommes de Gauss donnent des β_n pour une infinité de valeurs de m qui sont somme de m racines de l'unité, pour lesquelles

$$|\beta_m|^2 = m + 1 \quad .$$

[Hypothèses non fingo !]

BIBLIOGRAPHIE

[1] CASSELS (J. W. S.). - On a problem of Schinzel and Zassenhaus, J. math. Sc., Delhi, t. 1, 1966, p. 1-8.

[2] CASSELS (J. W. S.). - On a conjecture of R. M. Robinson about cyclotomic integers (non publié).

[3] DAVENPORT (Harold) and SCHINZEL (André). - Diophantine approximation and sums of roots of unity, Math. Annalen, t. 169, 1967, p. 118-135.

[4] JONES (A.). - Papier à paraître dans les Proc. Cambridge phil. Soc. et d'autres papiers en cours de rédaction.

[5] MANN (Henry B.). - On linear relations between roots of unity, Mathematika, London, t. 12, 1965, p. 107-117.

[6] ROBINSON (Raphael M.). - Some conjectures about cyclotomic integers, Math. of Comput., t. 19, 1965, p. 210-217.

[7] SCHINZEL (André). - On sums of roots of unity, Acta Arithm., Warszawa, t. 11, 1966, p. 419-432.

[8] SCHINZEL (André) and ZASSENHAUS (Hans). - A refinement of two theorems of Kronecker, Mich. math. J., t. 12, 1965, p. 81-85.