ARKIV FÖR MATEMATIK Band 3 nr 47

Communicated 14 May 1958 by LENNART CARLESON

On homomorphisms and orthogonal systems

By MATTS ESSÉN

1. Let G be a compact topological group, and let D be a subgroup of the group of all continuous homomorphisms T of G onto G. We define a class of functions A_D: $f \in A_D$ if for any two homomorphisms belonging to D

$$\int_G f(T_1 x)\,\overline{f(T_2 x)}\,dx = 0, \tag{1.00}$$

whenever $f(T_1 x)$ and $f(T_2 x)$ are different functions; and if

$$\int_G f(T_1 x)\,\overline{f(T_2 x)}\,dx = 1 \tag{1.01}$$

whenever $f(T_1 x)$ and $f(T_2 x)$ are identical. (We have especially $\int_G |f(x)|^2\,dx = 1$).

$$f(x) \text{ is continuous.} \tag{1.02}$$

We can also say that $\{f(Tx)\}$ is an orthonormal system.

We can now formulate the following problem: when does the fact that $f(x) \in A_D$ imply that $f(x)$ is a character or a simple combination of characters? We shall treat two special groups. In the first case, the group G is the topological group dual to the real line under the discrete topology. All functions $f(x) \in A_D$ are almost periodic, and Lemma 2 gives the tool we need for the proof of Theorem 1, which is the main result of the paper. In the second case, the group G is the unit circle under the usual topology. By using Theorem 1 we obtain a result for periodic functions with derivatives of all orders (Theorem 2). In this case we shall also investigate what happens when the orthonormal system $\{f(Tx)\}$ is complete (Theorem 3).

2. Let G be the topological group dual to the real line under the discrete topology [1], and let the group D consist of those homomorphisms of G, which, when $x \in G$ is real, have the form $Tx = ax$ (a is a real non-zero number). On the real line, the class of continuous functions on G is identical with the class of almost periodic functions, and we have

$$\int_G f(x)\,dx = \lim_{T\to\infty} \frac{1}{2T} \int_{-T}^{+T} f(x)\,dx = M\{f(x)\}.$$

We can now define this special class, which we shall call A_0, in a less abstract way. We say that the almost periodic function $f(x) \in A_0$, if

$$M\{f(ax)\overline{f(bx)}\}=0, \quad \text{if} \quad a\neq b \quad \text{and} \quad ab\neq 0, \tag{2.00}$$

and if

$$M\{|f(x)|^2\}=1. \tag{2.01}$$

Let

$$f(x)\sim \sum_{-\infty}^{+\infty} a_k e^{i\lambda_k x}.$$

Condition (2.00) then implies that

$$\sum_{a\lambda_\nu=b\lambda_\mu} a_\nu \bar{a}_\mu=0, \quad \text{if} \quad a\neq b \quad \text{and} \quad ab\neq 0$$

(Parseval's relation for almost periodic functions), or simpler

$$\sum_{\lambda_\nu=u\lambda_\mu} a_\nu \bar{a}_\mu=0, \quad \text{if} \quad u\neq 1 \quad \text{and} \quad u\neq 0. \tag{2.02}$$

Condition (2.01) implies that

$$\sum_{-\infty}^{+\infty}|a_k|^2=1. \tag{2.03}$$

Lemma 1. *Let* $f\in A_0$. *Then* $M\{f(x)\}=0$.

Proof. Let $\lambda_o=0$. We obtain from (2.02)

$$|a_0|^2+\sum_{\lambda_\nu=u\lambda_\mu}{}' a_\nu \bar{a}_\mu=0, \quad \text{if} \quad u\neq 1 \quad \text{and} \quad 0.$$

(Σ' means that the sum is taken over all non-zero indices ν and μ.)

$\{\lambda_\nu/\lambda_\mu\}'$ is a countable sequence of real numbers, and we can choose a number u different from all these numbers. Thus $|a_0|^2=0$ and the lemma is proved.

2.1. We shall now show that it is sufficient to treat the case, when the Fourier series of $f(x)$ contains terms with positive frequencies only. We can always assume that this series contains terms with the frequencies λ_k and $-\lambda_k$ (if that is not the case, we can insert a new term $a_k^{(-)}e^{-i\lambda_k x}$ with $a_k^{(-)}=0$). We can then renumber the terms in such a way that $\lambda_{-k}=-\lambda_k$ for all indices k, and that λ_k is positive, if k is positive. Let us study the even function

$$g_1(x)=f(x)+f(-x)$$

and the odd function

$$g_2(x)=f(x)-f(-x).$$

The function $g_1(x)$ is then represented by a cosine series with positive frequencies $\{\lambda_k\}_1^\infty$, and coefficients $\{b_k\}_1^\infty$. From (2.02) and (2.03), we get that

$$\sum_{\lambda_\nu=u\lambda_\mu} b_\nu \bar{b}_\mu=0, \quad \text{if} \quad u\neq 1 \quad \text{and} \quad 0, \tag{2.10}$$

and

$$\sum_1^\infty |b_k|^2=4. \tag{2.11}$$

We now define another function: Let $h_1(x)$ have the Fourier series $\sum_1^\infty b_k e^{i\lambda_k x}$. By (2.10) and (2.11), $h_1(x)/2\in A_0$. There is a one-one correspondence between

$g_1(x)$ and $h_1(x)$. In the same way, we can substitute a function $h_2(x)$ with Fourier series $\sum_1^\infty c_k e^{i\lambda_k x}$ for $g_2(x)$, which has the Fourier sine series $\sum_1^\infty c_k \sin \lambda_k x$, such that $h_2(x)/2 \in A_0$. Let us say that $h(x)$ belongs to the class A_1, if $h(x) \in A_0$ and if $h(x)$ has a Fourier series of the form $\sum_1^\infty a_k e^{i\lambda_k x}$, where $\lambda_k > 0$.

If conversely we start from two arbitrary functions $h_1(x) \in A_1$ and $h_2(x) \in A_1$, we obtain two new functions $g_1(x)$ and $g_2(x)$ (even and odd, respectively), which added give a function which belongs to A_0 (from $h_1(x) = a e^{inx}$ and $h_2(x) = e^{imx}$, where $|a| = |b| = 1$, we get the function $a \cos mx + b \sin nx$, which belongs to A_1). It is evidently sufficient to study functions belonging to A_1.

2.2. Let $f(x) \in A_1$ and let $f(x)$ have the Fourier series $\sum_1^\infty a_k e^{i\lambda_k x}$. The corresponding sum (2.02), where all frequencies are positive, can be interpreted as a convolution, where the operation multiplication is used instead of the usual operation addition. This leads us to the following lemma.

Lemma 2. *Let* $\sum_1^\infty |a_k|$ *be convergent. Let*

$$f(x) = \sum_1^\infty a_k e^{i\lambda_k x}$$

and

$$F(iy) = \sum_1^\infty a_k e^{-iy \log \lambda_k}.$$

Then $f(x) \in A_1$ *if and only if* $|F(iy)| \equiv 1$.

Proof. If we apply Parseval's relation to $F(iy)e^{ity}$ and $\overline{F(iy)}$, we obtain

$$M\{|F(iy)|^2 e^{ity}\} = \sum_{\lambda_\nu = e^t \lambda_\mu} a_\nu \bar{a}_\mu. \tag{2.20}$$

Let $f(x) \in A_1$. Then the sum (2.02) is 0 if $u \neq 1$, and 1 if $u = 1$. Thus

$$M\{|F(iy)|^2 e^{ity}\} = 0, \tag{2.21}$$

if $t \neq 0$, and

$$M\{|F(iy)|^2\} = 1. \tag{2.22}$$

This gives $|F(iy)|^2 \equiv 1$, and the necessity of the condition is proved.

Let now $|F(iy)| \equiv 1$. It follows from (2.20) that the sum (2.02) is 0 except when $u = 1$, and that $\sum_1^\infty |a_k|^2 = 1$. The sufficiency is proved.

2.3 Theorem 1. *Let* $f(x) \sim \sum_1^\infty a_k e^{i\lambda_k x}$, *let* $f(x) \in A_1$ *be such that*

$$\sum_1^\infty |a_k| \lambda_k^x = M(x) \tag{2.30}$$

is convergent for $-\infty < x < \infty$, *and let the sequence* $\{\lambda_k\}_1^\infty$ *at most have one of the points* 0 *and* ∞ *as accumulation point. Then* $f(x)$ *consists of one oscillation only. An assumption that* $M(x)$ *is finite only when* $x > b$ *or when* $x < b$, *is not sufficient to ensure this.*

In the proof of Theorem 1, the following theorem by H. Bohr is used [2].

Let the almost periodic function $f(z)$ have only negative frequencies, and suppose that the set of frequencies does not contain its upper bound. Then $f(z)$ takes the value 0 in every right half plane.

We can assume that all frequencies $\{\lambda_k\}_1^\infty$ of $f(x)$ either are $\geqslant 1$ or $\leqslant 1$.

Let us first assume that no smallest frequency λ_k exists, and that all frequencies λ_k are $\geqslant 1$. Consider the function

$$F(z)=\sum_1^\infty a_k e^{-z\log\lambda_k}.$$

(2.30) implies that this series is absolutely convergent for all z, and $F(z)$ is thus an entire function. Since $\sum_1^\infty |a_k|$ is convergent, Lemma 2 gives that $|F(iy)|\equiv 1$. The almost periodic function $F(z)$ has only negative frequencies, and their upper bound is not assumed. It follows from Bohr's theorem that there exists a $z_0=x_0+iy_0$ such that $F(z_0)=0$. We know that $|F(iy)|\equiv 1$, that is to say that the values that $F(z)$ takes on the imaginary axis, are situated on the unit circle. Schwarz's reflection principle implies that

$$F(x_0+iy_0)\,\overline{F(-x_0+iy_0)}=1.$$

But $F(z)$ is an entire function, and $F(z_0)=0$, which gives a contradiction. We conclude that a smallest frequency exists, e.g. λ_1. The Fourier coefficient a_1 is different from zero.

Consider $G(z)=e^{z\log\lambda_1}F(z)$. Evidently $|G(iy)|\equiv 1$, and

$$|G(z)|\leqslant\sum_1^\infty |a_k|\left(\frac{\lambda_k}{\lambda_1}\right)^{-x}.$$

Thus $G(z)$ converges uniformly to a_1, when $x\to+\infty$, and $G(z)$ is an entire function which is bounded in every right half plane. Suppose that $G(z)$ is not identically constant. Then there exists a sequence of numbers $\{z_n\}_1^\infty$ with $Re(z_n)\to-\infty$, such that $|G(z_n)|\to\infty$. Schwarz's principle gives

$$G(x_n+iy_n)\,\overline{G(-x_n+iy_n)}=1.$$

This is only possible if $a_1=0$, which is a contradiction. We conclude that $G(z)$ is identically constant, that $F(z)=a_1e^{-z\log\lambda_1}$, and that $f(x)=a_1e^{i\lambda_1 x}$. The first part of the theorem is proved, when $\lambda_k\geqslant 1$.

If $\lambda_k\leqslant 1$ for all k, we can consider the sequence $\{1/\lambda_k\}_1^\infty=\{\lambda_k'\}_1^\infty$ and the function

$$F_1(z)=\sum_1^\infty a_k e^{-z\log\lambda_k'},$$

which can be treated in exactly the same way as $F(z)$ in the previous part of the proof. The first part of the theorem follows.

We prove the second part of the theorem by constructing a nontrivial function $f(x)$, which belongs to A_1. We start from an analytic function with absolute value one on the unit circle. Take for instance

$$\frac{z-a}{1-\bar{a}z} = -a + (1-|a|^2)\sum_{k=1}^{\infty} z^k \bar{a}^{k-1}, \quad |a|<1.$$

Let us put $z = e^{-w\log 2}$ $(w = u+iv)$. We get

$$F(w) = -a + (1-|a|^2)\sum_{k=1}^{\infty} \bar{a}^{k-1} e^{-w\log 2^k}. \tag{2.31}$$

This series is convergent (even absolutely convergent) for $u > (\log|a|)/(\log 2)$ and divergent elsewhere. We also have $|F(iv)| \equiv 1$. Then by Lemma 2

$$f(x) = -a e^{ix} + (1-|a|^2)\sum_{k=1}^{\infty} \bar{a}^{k-1} e^{ix2^k} \tag{2.32}$$

belongs to A_1. Theorem 1 follows.

3. We shall now investigate the case, when G is the unit circle under the usual topology. Let D be the group of all continuous homomorphisms of G, i.e. $Tx = nx \pmod{2\pi}$, where n is an integer. The characters of G have the form e^{inx}. The function $f(x) \in A_D$, if

$$\frac{1}{2\pi}\int_0^{2\pi} f(nx)\,\overline{f(mx)}\,dx = \delta_{n,m} \tag{3.00}$$

(n and m are non-zero integers), and if $f(x)$ is a continuous function with period 2π.

3.1. The argument in 2.1 applies in particular to periodic functions, and it is therefore sufficient to consider functions belonging to A_D, which have Fourier series of the form $\sum_1^{\infty} a_k e^{ikx}$. Let us call this class of functions A_2.

Theorem 2. *Let $f(x) \in A_2$, and let $f(x)$ have derivatives of all orders for $-\infty < x < \infty$. Then $f(x)$ consists of one oscillation only. This conclusion cannot be drawn from an assumption of the existence of a finite number of derivatives.*

Proof. Let $f(x)$ have the Fourier series $\sum_1^{\infty} a_k e^{ikx}$, and let $f(x)$ have M periodic derivatives. Then $|a_k| \leqslant B(M)/k^M$ for all k. Assume $f(x)$ has derivatives of all orders. Then the series

$$\sum_1^{\infty} |a_k|k^M \leqslant B(M+2)\sum_1^{\infty}\frac{1}{k^2}$$

is convergent for all M. But $f(x) \in A_1$, for when n and m are integers, (3.00) implies that

$$\sum_{n\nu=m\mu} a_\nu \bar{a}_\mu = 0, \quad \text{if} \quad n \neq m \quad \text{and} \quad nm \neq 0,$$

and that

$$\sum_1^{\infty} |a_k|^2 = 1.$$

If u is irrational, then

$$\sum_{\nu-u\mu} a_\nu \bar{a}_\mu = 0.$$

(2.02) and (2.03) thus are fulfilled, and $f(x) \in A_1$. We can use Theorem 1, and the first part of the theorem is proved. The function (2.32) belongs to A_2, has M periodic derivatives if $|a| < 2^{-M}$ and thus gives the counterexample we need for the proof of the second part of the theorem.

3.2. Consider the orthonormal system $\{f(nx)\}_{n=-\infty}^{+\infty}$, which we will call F.

Theorem 3. *The system F is complete in $L^2(G)$ if and only if $f(x) = a e^{ix} + b e^{-ix}$, where*

$$\begin{cases} |a|^2 + |b|^2 = 1 \\ Re\,(a\bar{b}) = 0. \end{cases}$$

Proof. Let $f(x) \sim \sum_{-\infty}^{+\infty} a_k e^{ikx}$. Lemma 1 implies that $a_0 = 0$. Expand the function $(1/2\pi) e^{ix}$ in the system F.

$$\frac{1}{2\pi} \int_0^{2\pi} e^{ix} \overline{f(nx)}\, dx = \begin{cases} 0 & \text{if } |n| \geqslant 2. \\ \bar{a}_1 & \text{if } n = 1. \\ \bar{a}_{-1} & \text{if } n = -1. \end{cases}$$

Since G is complete, we can use Parseval's formula, which gives

$$\frac{1}{2\pi} \int_0^{2\pi} |e^{ix}|^2\, dx = |a_1|^2 + |a_{-1}|^2.$$

From $\sum_{-\infty}^{+\infty} |a_k|^2 = 1$, it follows that $a_k = 0$, when $|k| \geqslant 2$. Thus $f(x) = a e^{ix} + b e^{-ix}$. From

$$\frac{1}{2\pi} \int_0^{2\pi} f(x) \overline{f(-x)}\, dx = 0$$

it follows that $Re\,(a\bar{b}) = 0$, and the necessity of the condition is proved. The sufficiency follows from

$$e^{ix} = \bar{a} f(x) + \bar{b} f(-x).$$

REFERENCES

1. L. H. LOOMIS, An Introduction to Abstract Harmonic Analysis § 41 E. New York, 1953.
2. H. BOHR, Zur Theorie der Fastperiodischen Funktionen. Acta Mathematica *47*, 273 (1926).

Tryckt den 19 september 1958

Uppsala 1958. Almqvist & Wiksells Boktryckeri AB

ARKIV FÖR MATEMATIK Band 3 nr 48

Communiqué le 10 septembre 1958

Sur l'équation $x^5+y^5=z^5$

Par TRYGVE NAGELL

1. Dirichlet a le premier montré que l'équation

$$x^5 + y^5 = z^5 \tag{1}$$

est impossible en nombres entiers différents de zéro. Le but de cette Note est de montrer que l'équation (1) est impossible en nombres entiers dans le corps quadratique engendré par $\sqrt{5}$. Ce résultat est, bien entendu, compris dans le théorème général de Kummer sur l'équation de Fermat. En effet, il résulte de ce théorème que l'équation (1) est impossible dans le corps du quatrième degré engendré par $e^{2\pi i/5}$.

2. Dans le corps $\mathbf{K}(\sqrt{5})$ une base des nombres entiers est donnée par $1, \frac{1}{2}(1+\sqrt{5})$. Dans la suite nous désignons ce corps par $\mathbf{K}$. Le nombre des classes d'idéaux est égal à 1. L'unité fondamentale (celle qui est > 1) est le nombre $\varepsilon = \frac{1}{2}(1+\sqrt{5})$, dont la norme est égale à -1. Le nombre $\lambda = \sqrt{5}$ est un nombre premier dans le corps.

Nous allons démontrer quelques lemmes sur les unités du corps.

Lemme 1. La condition nécessaire et suffisante pour que l'unité

$$E = \pm\varepsilon^M \quad (M = 0, \pm 1, \pm 2, \text{ etc.}) \tag{2}$$

soit congrue à un nombre rationnel modulo 5, est que M soit divisible par 5. Ici $\varepsilon = \frac{1}{2}(1+\sqrt{5})$.

Démonstration. On a $\varepsilon^2 = \frac{1}{2}(3+\sqrt{5})$, $\varepsilon^3 = 2+\sqrt{5}$, $\varepsilon^4 = \frac{1}{2}(7+3\sqrt{5})$ et $\varepsilon^5 = \frac{1}{2}(11+5\sqrt{5})$. Donc $\varepsilon^5 \equiv 3 \pmod 5$. Si E est congrue à un nombre rationnel modulo 5, et si $M = 5m+r$ avec $0 \leqslant r \leqslant 4$, il est évident que l'unité ε^r est aussi congrue à un nombre rationnel modulo 5. Donc on conclut que $r = 0$. D'autre part, si M est divisible par 5, on voit aisément que l'unité E est congrue à $\pm 3^{M/5}$ modulo 5.

Si on exige que l'unité E soit congrue à ± 1 modulo 5, il faut évidemment que M soit divisible par 10. Ainsi nous avons aussi

Lemme 2. Pour que l'unité E, donnée par (2), soit congrue à ± 1 modulo 5, il faut et il suffit que M soit divisible par 10.

3. Nous avons aussi besoin du lemme suivant:

Lemme 3. Soit E une unité dans $\mathbf{K}$ telle qu'on ait $E \equiv 1 \pmod 5$. Si le nombre

$$H=\frac{E^5-1}{5(E-1)} \tag{3}$$

est une unité, on a nécessairement $E=1$.

Démonstration. H est évidemment positif et aussi le nombre conjugé H'. Donc nous avons

$$H\cdot H'=+1. \tag{4}$$

Vu que $E\equiv 1 \pmod 5$ il résulte du Lemme 2 que la norme de E est égale à $+1$. Donc nous avons

$$E\cdot E'=+1. \tag{5}$$

Il suit de (3) et (5) qu'on a

$$H'=\frac{E'^5-1}{5(E'-1)}=\frac{1-E^5}{5E^4(1-E)}.$$

De (4) on aura alors $$HH'=1=\left(\frac{E^5-1}{E-1}\right)^2\cdot\frac{1}{25E^4}$$

d'où $$\frac{E^5-1}{E-1}=5E^2.$$

On voit aisément que cette équation admet, en dehors de la racine double $E=1$, les deux racines $E=\frac{1}{2}(-3\pm\sqrt{5})$. Comme aucune de ces racines n'est pas $\equiv 1 \pmod 5$, le lemme se trouve demontré.

4. Soit $\alpha=\frac{1}{2}(a+b\sqrt{5})$ un nombre entier dans **K** qui n'est pas divisible par $\sqrt{5}$. Ici a et b sont des nombres entiers rationnels, a non divisible par 5. Alors on voit aisément que

$$\alpha^5\equiv\frac{a^5}{2^5}\equiv -7a^5 \pmod{(\sqrt{5})^3}.$$

Or, la cinquième puissance d'un nombre entier rationnel, non divisible par 5, est congru à ou ± 1 ou ± 7 modulo 25. Donc nous avons le résultat :

Lemme 4. Si α est un nombre entier dans **K** qui n'est pas divisible par $\sqrt{5}$, le nombre α^5 est congru à ou ± 1 ou ± 7 modulo $(\sqrt{5})^3$.

Ajoutons qu'on a $$\alpha^4\equiv 1 \pmod{\sqrt{5}}$$

pour tous les entiers α non divisibles par $\sqrt{5}$.

5. Une conséquence immédiate du Lemme 4 est le

Lemme 5. Si l'équation $$x^5-y^5=z^5 \quad (xyz\neq 0) \tag{6}$$

est résoluble en nombres entiers x, y, z dans **K**, il faut que l'un des nombres x, y, z soit divisible par $\sqrt{5}$.

Ainsi on peut supposer dans (6) que z est divisible par $\sqrt{5}$. Nous pouvons aussi supposer que les nombres x, y, z sont premiers entre eux deux à deux.

6. Au lieu de l'équation (6) nous considérons l'équation plus générale à cinq nombres inconnus

$$x^5 - y^5 = E \cdot \lambda^{5+\mu} z^5, \tag{7}$$

où nous avons posé $\lambda = \sqrt{5}$.

Nous allons montrer que cette équation est impossible quand les inconnus x, y, z, E et μ satisfont aux conditions suivantes : μ est un nombre entier rationnel $\geqslant 0$; E est une unité dans $\mathbf{K}$; x, y et z sont des nombres entiers dans $\mathbf{K}$ tels que $xyz \neq 0$.

Supposons au contraire que l'équation (7) soit résoluble et désignons une solution par $[x, y, z, E, \mu]$. Nous supposons que $(x, y) = (x, z) = (y, z) = (x, \lambda) = (y, \lambda) = 1$.

Le terme à gauche dans (7), $x^5 - y^5$, est le produit des trois facteurs

$$x - y, \quad \lambda xy + \tfrac{1}{2}(\lambda + 1)(x - y)^2, \quad \lambda xy + \tfrac{1}{2}(\lambda - 1)(x - y)^2.$$

Le plus grand commun diviseur de deux quelconques de ces nombres est évidemment égal à λ. Par conséquent on conclut de (7) qu'on doit avoir

$$x - y = E_0 \cdot \lambda^{3+\mu} z_1^5, \tag{8}$$

$$\left.\begin{aligned} xy + \frac{\lambda + 1}{2\lambda}(x - y)^2 &= E_1 x_1^5, \\ xy + \frac{\lambda - 1}{2\lambda}(x - y)^2 &= E_2 y_1^5, \end{aligned}\right\} \tag{9}$$

où x_1, y_1, z_1 sont des nombres entiers dans $\mathbf{K}$ tels que

$$(x_1, y_1) = (x_1, z_1) = (y_1, z_1) = (x_1, \lambda) = (y_1, \lambda) = 1.$$

E_0, E_1 et E_2 sont des unités dans $\mathbf{K}$. En éliminant x et y des équations (8) et (9) on aura

$$E_1 x_1^5 - E_2 y_1^5 = \frac{1}{\lambda}(x - y)^2 = E_0^2 \cdot \lambda^{5+2\mu} z_1^{10},$$

d'où

$$x_1^5 - E_3 y_1^5 = E_4 \lambda^{5+2\mu} z_1^{10}, \tag{10}$$

où E_3 et E_4 sont des unités dans $\mathbf{K}$. En appliquant le Lemme 4 à l'équation (10) nous aurons

$$E_3 \equiv \pm 1 \quad \text{ou} \quad \equiv \pm 2 \pmod{\lambda^2}.$$

D'après le Lemme 1 l'unité E_3 est donc une cinquième puissance d'une unité dans $\mathbf{K}$. Si nous posons $E_3 = E_5^5$, $x_1 = u$, $E_5 y_1 = v$ et $z_1^2 = w$, l'équation (10) peut s'écrire

$$u^5 - v^5 = E_4 \lambda^{5+2\mu} w^5. \tag{11}$$

Ainsi, d'une solution $[x, y, z, E, \mu]$ de l'équation (7) nous avons obtenu une autre solution $[u, v, w, E_4, 2\mu]$. Ces solutions sont liées par la relation

$$z = u\,v\,\sqrt{w}\,E_5^{-1}. \tag{12}$$

En procédant de la même manière avec l'équation (11) nous aurons une troisième équation

$$u_1^5 - v_1^5 = E_6\,\lambda^{5+4\mu}\,w_1^5, \tag{13}$$

où u_1, v_1, w_1 sont des nombres entiers dans $\mathbf{K}$ tels que

$$(u_1, v_1) = (u_1, w_1) = (v_1, w_1) = (u_1, \lambda) = (v_1, \lambda) = 1.$$

E_6 est une unité dans $\mathbf{K}$.

Nous avons ainsi obtenu une troisième solution $[u_1, v_1, w_1, E_6, 4\mu]$ de l'équation (7). Entre les solutions subsiste la relation

$$w = u_1\,v_1\,\sqrt{w_1}\,E_7, \tag{14}$$

où E_7 est une unité.

Parmi toutes les solutions $[x, y, z, E, \mu]$ de l'équation (7) il y a au moins une avec la propriété suivante : Le nombre des facteurs premiers non-associés du nombre z est minimum, eventuellement $= 0$. Supposons maintenant que notre solution initiale $[x, y, z, E, \mu]$ satisfait à cette condition minimale. Alors il résulte de (12) et de (14) que les nombres u, v et u_1, v_1 sont des unités.

Entre les nombres u, v, u_1 et v_1 subsistent les relations suivantes, analogues aux relations (8) et (9) :

$$u - v = E_8 \cdot \lambda^{3+2\mu}\,z_2^5, \tag{15}$$

$$\left.\begin{aligned} u\,v + \frac{\lambda+1}{2\lambda}(u-v)^2 &= E_9\,u_1^5, \\ u\,v + \frac{\lambda-1}{2\lambda}(u-v)^2 &= E_{10}\,v_1^5, \end{aligned}\right\} \tag{16}$$

où E_8, E_9 et E_{10} sont des unités dans $\mathbf{K}$. En multipliant les deux relations (16) on aura

$$\frac{u^5 - v^5}{5\,(u-v)} = E_9\,E_{10}\,(u_1\,v_1)^5.$$

Ici le terme à droite est une unité. Si nous posons $E = u/v$, le nombre E est une unité $\neq 1$. D'après (15) on a $E \equiv 1 \pmod 5$. Il en résulte que le nombre

$$H = \frac{E^5 - 1}{5\,(E-1)}$$

doit être une unité. Or d'après le Lemme 3 c'est impossible quand $E \equiv 1 \pmod 5$ et $E \neq 1$.

Notre théorème sur l'équation (7) se trouve ainsi demontré.

Tryckt den 14 november 1958

Uppsala 1958. Almqvist & Wiksells Boktryckeri AB