THE WADSWORTH MATHEMATICS SERIES

W. Beckner, A. Calderón, R. Fefferman, P. Jones, *Conference on Harmonic Analysis in Honor of Antoni Zygmund*
M. Behzad, G. Chartrand, L. Lesniak-Foster, *Graphs and Digraphs*
J. Cochran, *Applied Mathematics: Principles, Techniques, and Applications*
A. Garsia, *Topics in Almost Everywhere Convergence*
K. Stromberg, *An Introduction to Classical Real Analysis*
R. Salem, *Algebraic Numbers and Fourier Analysis*, and L. Carleson, *Selected Problems on Exceptional Sets*

ALGEBRAIC NUMBERS AND FOURIER ANALYSIS

RAPHAEL SALEM

SELECTED PROBLEMS ON EXCEPTIONAL SETS

LENNART CARLESON
MITTAG-LEFFLER INSTITUT

WADSWORTH INTERNATIONAL GROUP
Belmont, California
A Division of Wadsworth, Inc.

Mathematics Editor: John Kimmel
Production Editor: Diane Sipes

The text of *Algebraic Numbers and Fourier Analysis* has been reproduced from the original with no changes. Minor revisions have been made by the author to the text of *Selected Problems on Exceptional Sets*.

Printed in the United States of America

1 2 3 4 5 6 7 8 9 10—87 86 85 84 83

Library of Congress Cataloging in Publication Data

Salem, Raphaël.
Algebraic numbers and Fourier analysis.

(Wadsworth mathematics series)
Reprint. Originally published: Boston: Heath, 1963.
Reprint. Originally published: Princeton, N.J.: Van Nostrand, c1967.
Includes bibliographies and index.
1. Algebraic number theory. 2. Fourier analysis. 3. Harmonic analysis. 4. Potential, Theory of. I. Carleson, Lennart. Selected problems on exceptional sets. II. Title. III. Series.
QA247.S23 1983 512'.74 82-20053
ISBN 0-534-98049-X

Algebraic Numbers and Fourier Analysis

RAPHAEL SALEM

To the memory of my father —

to the memory of my nephew, Emmanuel Amar,

who died in 1944 in a concentration camp —

to my wife and my children, to whom

I owe so much —

this book is dedicated

PREFACE

THIS SMALL BOOK contains, with but a few developments, the substance of the lectures I gave in the fall of 1960 at Brandeis University at the invitation of its Department of Mathematics.

Although some of the material contained in this book appears in the latest edition of Zygmund's treatise, the subject matter covered here has never until now been presented as a whole, and part of it has, in fact, appeared only in original memoirs. This, together with the presentation of a number of problems which remain unsolved, seems to justify a publication which, I hope, may be of some value to research students. In order to facilitate the reading of the book, I have included in an Appendix the definitions and the results (though elementary) borrowed from algebra and from number theory.

I wish to express my thanks to Dr. Abram L. Sachar, President of Brandeis University, and to the Department of Mathematics of the University for the invitation which allowed me to present this subject before a learned audience, as well as to Professor D. V. Widder, who has kindly suggested that I release my manuscript for publication in the series of *Heath Mathematical Monographs*. I am very grateful to Professor A. Zygmund and Professor J.-P. Kahane for having read carefully the manuscript, and for having made very useful suggestions.

R. Salem
Paris, 1 November 1961

Professor Raphaël Salem died suddenly in Paris on the twentieth of June, 1963, a few days after seeing final proof of his work.

CONTENTS

Chapter I

A REMARKABLE SET OF ALGEBRAIC INTEGERS

1. Introduction

We shall first recall some notation. Given any real number a, we shall denote by $[a]$ its integral part, that is, the integer such that

$$[a] \leq a < [a] + 1.$$

By (a) we shall denote the fractional part of a; that is,

$$[a] + (a) = a.$$

We shall denote by $\| a \|$ the absolute value of the difference between a and the nearest integer. Thus,

$$\| a \| = \min | a - n |, \quad n = 0, \pm 1, \pm 2, \ldots.$$

If m is the integer nearest to a, we shall also write

$$a = m + \{a\}$$

so that $\| a \|$ is the absolute value of $\{a\}$.

Next we consider a sequence of numbers † $u_1, u_2, \ldots, u_n, \ldots$ such that

$$0 \leq u_j < 1.$$

Let Δ be an interval contained in $(0, 1)$, and let $|\Delta|$ be its length. Suppose that among the first N members of the sequence there are $\nu(\Delta, N)$ numbers in the interval Δ. Then if for any fixed Δ we have

$$\lim_{N \to \infty} \frac{\nu(\Delta, N)}{N} = |\Delta|,$$

we say that the sequence $\{u_n\}$ is *uniformly distributed.* This means, roughly speaking, that each subinterval of $(0, 1)$ contains its proper quota of points.

We shall now extend this definition to the case where the numbers u_j do not fall between 0 and 1. For these we consider the fractional parts, (u_j), of u_j, and we say that the sequence $\{u_n\}$ is *uniformly distributed modulo 1* if the sequence of the fractional parts, $(u_1), (u_2), \ldots, (u_n), \ldots$, is uniformly distributed as defined above.

The notion of uniform distribution (which can be extended to several dimensions) is due to H. Weyl, who in a paper [16], ‡ by now classical, has also given a very useful criterion for determining whether a sequence is uniformly distributed modulo 1 (cf. Appendix, 7).

† By "number" we shall mean "real number" unless otherwise stated.

‡ See the Bibliography on page 67.

Without further investigation, we shall recall the following facts (see, for example, [2]).

1. If ξ is an irrational number, the sequence of the fractional parts $(n\xi)$, $n = 1, 2, \ldots$, is uniformly distributed. (This is obviously untrue for ξ rational.)
2. Let $P(x) = a_k x^k + \cdots + a_0$ be a polynomial where at least one coefficient a_j, with $j > 0$, is irrational. Then the sequence $P(n)$, $n = 1, 2, \ldots$, is uniformly distributed modulo 1.

The preceding results give us some information about the uniform distribution modulo 1 of numbers $f(n)$, $n = 1, 2, \ldots$, when $f(x)$ increases to ∞ with x not faster than a polynomial.

We also have some information on the behavior — from the viewpoint of uniform distribution — of functions $f(n)$ which increase to ∞ slower than n. We know, for instance, that the sequence an^α $(a > 0, 0 < \alpha < 1)$ is uniformly distributed modulo 1. The same is true for the sequence $a \log^\alpha n$ if $\alpha > 1$, but untrue if $\alpha < 1$.

However, almost nothing is known when the growth of $f(n)$ is exponential. Koksma [7] has proved that ω^n is uniformly distributed modulo 1 for *almost all* (in the Lebesgue sense) numbers $\omega > 1$, but nothing is known for particular values of ω. Thus, we do not know whether sequences as simple as e^n or $(\frac{3}{2})^n$ are or are not uniformly distributed modulo 1. We do not even know whether they are everywhere dense (modulo 1) on the interval (0, 1).

It is natural, then, to turn in the other direction and try to study the numbers $\omega > 1$ such that ω^n is "badly" distributed. Besides the case where ω is a rational integer (in which case for all n, ω^n is obviously congruent to 0 modulo 1), there are less trivial examples of distributions which are as far as possible from being uniform. Take, for example, the quadratic algebraic integer †

$$\omega = \tfrac{1}{2}(1 + \sqrt{5}) \text{ with conjugate } \tfrac{1}{2}(1 - \sqrt{5}) = \omega'.$$

Here $\omega^n + \omega'^n$ is a rational integer; that is,

$$\omega^n + \omega'^n \equiv 0 \pmod 1.$$

But $|\omega'| < 1$, and so $\omega'^n \to 0$ as $n \to \infty$, which means that $\omega^n \to 0$ (modulo 1). In other words, the sequence ω^n has (modulo 1) a single limit point, which is 0. This is a property shared by some other algebraic integers, as we shall see.

2. The algebraic integers of the class S

DEFINITION. *Let θ be an algebraic integer such that all its conjugates (not θ itself) have moduli strictly less than* 1. *Then we shall say that θ* belongs to the class S.‡

† For the convenience of the reader, some classical notions on algebraic integers are given in the Appendix.

‡ We shall always suppose (without loss of generality) that $\theta > 0$. θ is necessarily real. Although every natural integer belongs properly to S, it is convenient, to simplify many statements, to exclude the number 1 from S. Thus, in the definition we can always assume $\theta > 1$.

Then we have the following.

THEOREM 1. *If θ belongs to the class S, then θ^n tends to* 0 *(modulo* 1) *as $n \to \infty$.*

PROOF. Suppose that θ is of degree k and let $\alpha_1, \alpha_2, \ldots, \alpha_{k-1}$ be its conjugates. The number $\theta^n + \alpha_1^n + \cdots + \alpha_{k-1}^n$ is a rational integer. Since $|\alpha_j| < 1$ for all j, we have, denoting by ρ the greatest of the $|\alpha_j|$, $j = 1, 2, \ldots, k-1$,

$$|\alpha_1|^n + \cdots + |\alpha_{k-1}|^n < (k-1)\rho^n, \quad \rho < 1,$$

and thus, since $\quad \theta^n + \alpha_1^n + \cdots + \alpha_{k-1}^n \equiv 0 \pmod 1,$

we see that (modulo 1) $\theta^n \to 0$, and even that it tends to zero in the same way as the general term of a convergent geometric progression.

With the notation of section 1, we write $\|\theta^n\| \to 0$.

Remark. The preceding result can be extended in the following way. Let λ be any algebraic integer of the field of θ, and let $\mu_1, \mu_2, \ldots, \mu_{k-1}$ be its conjugates. Then

$$\lambda\theta^n + \mu_1\alpha_1^n + \cdots + \mu_{k-1}\alpha_{k-1}^n$$

is again a rational integer, and thus $\|\lambda\theta^n\|$ also tends to zero as $n \to \infty$, as can be shown by an argument identical to the preceding one. Further generalizations are possible to other numbers λ.

Up to now, we have not constructed any number of the class S except the quadratic number $\frac{1}{2}(1 + \sqrt{5})$. (Of course, all rational integers belong trivially to S.) It will be of interest, therefore, to prove the following result [10].

THEOREM 2. *In every real algebraic field, there exist numbers of the class S.*†

PROOF. Denote by $\omega_1, \omega_2, \ldots, \omega_k$ a basis ‡ for the integers of the field, and let $\omega_1^{(i)}, \omega_2^{(i)}, \ldots, \omega_k^{(i)}$ for $i = 1, 2, \ldots, k-1$ be the numbers conjugate to $\omega_1, \omega_2, \ldots, \omega_k$. By Minkowski's theorem on linear forms [5] (cf. Appendix, 9), we can determine rational integers $x_1, x_2, \ldots, x_k$, not all zero, such that

$$|x_1\omega_1 + \cdots + x_k\omega_k| \le A$$

$$|x_1\omega_1^{(i)} + \cdots + x_k\omega_k^{(i)}| \le \rho < 1 \quad (i = 1, 2, \ldots, k-1)$$

provided $\quad A\rho^{k-1} \ge \sqrt{|D|},$

D being the discriminant of the field. For A large enough, this is always possible, and thus the integer of the field

$$\theta = x_1\omega_1 + \cdots + x_k\omega_k$$

belongs to the class S.

† We shall prove, more exactly, that there exist numbers of S having the degree of the field.

‡ The notion of "basis" of the integers of the field is not absolutely necessary for this proof, since we can take instead of $\omega_1, \ldots, \omega_k$ the numbers $1, \alpha, \ldots, \alpha^{k-1}$, where α is any integer of the field having the degree of the field.

3. Characterization of the numbers of the class S

The fundamental property of the numbers of the class S raises the following question.

Suppose that $\theta > 1$ is a number such that $\|\theta^n\| \to 0$ as $n \to \infty$ (or, more generally, that θ is such that there exists a real number λ such that $\|\lambda\theta^n\| \to 0$ as $n \to \infty$). Can we assert that θ is an algebraic integer belonging to the class S?

This important problem is still unsolved. But it can be answered positively if one of the two following conditions is satisfied in addition:

1. The sequence $\|\lambda\theta^n\|$ tends to zero rapidly enough to make the series $\sum \|\lambda\theta^n\|^2$ convergent.
2. We know beforehand that θ is algebraic.

In other words, we have the two following theorems.

THEOREM A. *If $\theta > 1$ is such that there exists a λ with*

$$\sum \|\lambda\theta^n\|^2 < \infty,$$

then θ is an algebraic integer of the class S, and λ is an algebraic number of the field of θ.

THEOREM B. *If $\theta > 1$ is an* algebraic number *such that there exists a real number λ with the property $\|\lambda\theta^n\| \to 0$ as $n \to \infty$, then θ is an algebraic integer of the class S, and λ is algebraic and belongs to the field of θ.*

The proof of Theorem A is based on several lemmas.

LEMMA I. *A necessary and sufficient condition for the power series*

$$f(z) = \sum_0^\infty c_n z^n \tag{1}$$

to represent a rational function,

$$\frac{P(z)}{Q(z)}$$

(P and Q polynomials), is that its coefficients satisfy a recurrence relation,

$$\alpha_0 c_m + \alpha_1 c_{m+1} + \cdots + \alpha_p c_{m+p} = 0,$$

valid for all $m \geq m_0$, the integer p and the coefficients $\alpha_0, \alpha_1, \ldots, \alpha_p$ being independent of m.

LEMMA II (Fatou's lemma). *If in the series* (1) *the coefficients c_n are rational integers and if the series represents a rational function, then*

$$f(z) = \frac{P(z)}{Q(z)},$$

where P/Q is irreducible, P and Q are polynomials with rational integral coefficients, and $Q(0) = 1$.

LEMMA III (Kronecker). *The series* (1) *represents a rational function if and only if the determinants*

$$\Delta_m = \begin{vmatrix} c_0 & c_1 & \ldots & c_m \\ c_1 & c_2 & \ldots & c_{m+1} \\ \ldots & \ldots & \ldots & \ldots \\ c_m & c_{m+1} & \ldots & c_{2m} \end{vmatrix}$$

are all zero for $m \geq m_1$.

LEMMA IV (Hadamard). *Let the determinant*

$$D = \begin{vmatrix} a_1 & b_1 & \ldots & l_1 \\ a_2 & b_2 & \ldots & l_2 \\ \ldots & \ldots & \ldots & \ldots \\ a_n & b_n & \ldots & l_n \end{vmatrix}$$

have real or complex elements. Then

$$|D^2| \leq \left(\sum_1^n |a_j|^2\right)\left(\sum_1^n |b_j|^2\right)\cdots\left(\sum_1^n |l_j|^2\right).$$

We shall not prove here Lemma I, the proof of which is classical and almost immediate [3], nor Lemma IV, which can be found in all treatises on calculus [4]. We shall use Lemma IV only in the case where the elements of D are real; the proof in that case is much easier. For the convenience of the reader, we shall give the proofs of Lemma II and Lemma III.

PROOF of Lemma II. We start with a definition: A formal power series

$$\sum_0^\infty a_n z^n$$

with rational integral coefficients will be said to be *primitive* if no rational integer $d > 1$ exists which divides *all* coefficients.

Let us now show that if two series,

$$\sum_0^\infty a_n z^n \quad \text{and} \quad \sum_0^\infty b_n z^n,$$

are both primitive, their formal product,

$$\sum_0^\infty c_n z^n, \quad c_n = \sum_{\nu=0}^n a_\nu b_{n-\nu},$$

is also primitive. Suppose that the prime rational integer p divides *all* the c_n. Since p cannot divide all the a_n, suppose that

$$\left.\begin{array}{l} a_0 \equiv 0 \\ a_1 \equiv 0 \\ \ldots\ldots \\ a_{k-1} \equiv 0 \end{array}\right\} \pmod p, \quad a_k \not\equiv 0 \pmod p.$$

We should then have

$$\begin{aligned} c_k &\equiv a_k b_0 \pmod p, \text{ whence } b_0 \equiv 0 \pmod p, \\ c_{k+1} &\equiv a_k b_1 \pmod p, \text{ whence } b_1 \equiv 0 \pmod p, \\ c_{k+2} &\equiv a_k b_2 \pmod p, \text{ whence } b_2 \equiv 0 \pmod p, \end{aligned}$$

and so on, and thus

$$\sum_0^\infty b_n z^n$$

would not be primitive.

We now proceed to prove our lemma. Suppose that the coefficients c_n are rational integers, and that the series

$$\sum_0^\infty c_n z^n$$

represents a rational function

$$f(z) = \frac{P(z)}{Q(z)} = \frac{p_0 + p_1 z + \cdots + p_m z^m}{q_0 + q_1 z + \cdots + q_n z^n},$$

which we assume to be irreducible. As the polynomial $Q(z)$ is wholly determined (except for a constant factor), the equations

$$q_0 c_s + q_1 c_{s-1} + \cdots + q_n c_{s-n} = 0 \quad (s > m)$$

determine completely the coefficients q_j (except for a constant factor). Since the c_s are rational, there is a solution with all q_j rational integers, and it follows that the p_i are also rational integers.

We shall now prove that $q_0 = \pm 1$. One can assume that no integer $d > 1$ divides all p_i and all q_j. (Without loss of generality, we may suppose that there is no common divisor to all coefficients c_n; i.e., $\sum c_n z^n$ is primitive.) The polynomial Q is primitive, for otherwise if d divided q_j for all j, we should have

$$f\frac{Q}{d} = \frac{P}{d}$$

and d would divide all p_j, contrary to our hypothesis.

Now let U and V be polynomials with integral rational coefficients such that

$$PU + QV = m \neq 0,$$

m being an integer. Then

$$m = Q(Uf + V).$$

Since Q is primitive, $Uf + V$ cannot be primitive, for m is not primitive unless $|m| = 1$. Hence, the coefficients of $Uf + V$ are divisible by m. If γ_0 is the constant term of $Uf + V$, we have

$$m = q_0 \gamma_0,$$

and, thus, since m divides γ_0, one has $q_0 = \pm 1$, which proves Lemma II.

PROOF of Lemma III. The recurrence relation of Lemma I,

$$\alpha_0 c_m + \alpha_1 c_{m+1} + \cdots + \alpha_p c_{m+p} = 0, \tag{2}$$

for all $m \geq m_0$, the integer p and the coefficients $\alpha_0, \ldots, \alpha_p$ being independent of m, shows that in the determinant

$$\Delta_m = \begin{vmatrix} c_0 & c_1 & \cdots & c_m \\ c_1 & c_2 & \cdots & c_{m+1} \\ \cdots & \cdots & \cdots & \cdots \\ c_m & c_{m+1} & \cdots & c_{2m} \end{vmatrix},$$

where $m \geq m_0 + p$, the columns of order $m_0, m_0 + 1, \ldots, m_0 + p$ are dependent; hence, $\Delta_m = 0$.

We must now show that if $\Delta_m = 0$ for $m \geq m_1$, then the c_n satisfy a recurrence relation of the type (2); if this is so, Lemma III follows from Lemma I. Let p be the first value of m for which $\Delta_m = 0$. Then the last column of Δ_p is a linear combination of the first p columns; that is:

$$L_{j+p} = \alpha_0 c_j + \alpha_1 c_{j+1} + \cdots + \alpha_{p-1} c_{j+p-1} + c_{j+p} = 0, \quad j = 0, 1, \ldots, p.$$

We shall now show that $L_{j+p} = 0$ for all values of j. Suppose that

$$L_{j+p} = 0, \quad j = 0, 1, 2, \ldots, m - 1, \quad (m > p).$$

If we can prove that $L_{m+p} = 0$, we shall have proved our assertion by recurrence. Now let us write

$$\Delta_m = \left|\begin{array}{c|ccc} \Delta_{p-1} & c_p & \cdots & c_m \\ & \vdots & & \vdots \\ \hline c_p & & & c_{p+m} \\ \vdots & & & \vdots \\ c_m & c_{p+m} & \cdots & c_{2m} \end{array}\right|,$$

and let us add to every column of order $\geq p$ a linear combination with coefficients $\alpha_0, \alpha_1, \ldots, \alpha_{p-1}$ of the p preceding columns. Hence,

$$\Delta_m = \left|\begin{array}{c|ccc} \Delta_{p-1} & L_p & \cdots & L_m \\ & \vdots & & \vdots \\ \hline c_p & & & L_{p+m} \\ \vdots & & & \vdots \\ c_m & L_{p+m} & \cdots & L_{2m} \end{array}\right|,$$

and since the terms above the diagonal are all zero, we have

$$\Delta_m = (-1)^{p+m} \Delta_{p-1} (L_{p+m})^{m-p+1}.$$

Since $\Delta_m = 0$, we have $L_{m+p} = 0$, which we wanted to show, and Lemma III follows.

We can now prove Theorem A.

PROOF of Theorem A [10]. We write

$$\lambda\theta^n = a_n + \epsilon_n,$$

where a_n is a rational integer and $|\epsilon_n| \le \frac{1}{2}$; thus $|\epsilon_n| = \|\lambda\theta^n\|$. Our hypothesis is, therefore, that the series $\sum \epsilon_n^2$ converges.

The first step will be to prove by application of Lemma III that the series

$$\sum_0^\infty a_n z^n$$

represents a rational function. Considering the determinant

$$\Delta_n = \begin{vmatrix} a_0 & a_1 & \cdots & a_n \\ a_1 & a_2 & \cdots & a_{n+1} \\ \cdots & \cdots & \cdots & \cdots \\ a_n & a_{n+1} & \cdots & a_{2n} \end{vmatrix},$$

we shall prove that $\Delta_n = 0$ for all n large enough. Writing

$$\eta_m = a_m - \theta a_{m-1} = \theta\epsilon_{m-1} - \epsilon_m,$$

we have

$$\eta_m^2 < (\theta^2 + 1)(\epsilon_{m-1}^2 + \epsilon_m^2).$$

Transforming the columns of Δ_n, beginning with the last one, we have

$$\Delta_n = \begin{vmatrix} a_0 & \eta_1 & \cdots & \eta_n \\ a_1 & \eta_2 & \cdots & \eta_{n+1} \\ \cdots & \cdots & \cdots & \cdots \\ a_n & \eta_{n+1} & \cdots & \eta_{2n} \end{vmatrix}$$

and, by Lemma IV,

$$\Delta_n^2 \le \left(\sum_0^n a_m^2\right)\left(\sum_1^{n+1} \eta_m^2\right)\cdots\left(\sum_n^{2n} \eta_m^2\right)$$

$$\le \left(\sum_0^n a_m^2\right) R_1 R_2 \cdots R_n$$

where R_h denotes the remainder of the convergent series

$$\sum_h^\infty \eta_m^2.$$

But, by the definition of a_m,

$$\sum_0^n a_m^2 < C\theta^{2n},$$

where $C = C(\lambda, \theta)$ depends on λ and θ only.

Hence,

$$\Delta_n^2 \le C \prod_{h=1}^n (\theta^2 R_h),$$

and since $R_h \to 0$ for $h \to \infty$, $\Delta_n \to 0$ as $n \to \infty$, which proves, since Δ_n is a rational integer, that Δ_n is zero when n is larger than a certain integer.

Hence

$$\sum_0^\infty a_n z^n = \frac{P(z)}{Q(z)}, \quad \text{(irreducible)}$$

where, by Lemma III, P and Q are polynomials with rational integral coefficients and $Q(0) = 1$. Writing

$$Q(z) = 1 + q_1 z + \cdots + q_k z^k,$$

we have

$$\begin{aligned} f(z) &= \sum_0^\infty \epsilon_n z^n \\ &= \sum_0^\infty \lambda\theta^n z^n - \sum_0^\infty a_n z^n \\ &= \frac{\lambda}{1 - \theta z} - \frac{P(z)}{1 + q_1 z + \cdots + q_k z^k}. \end{aligned}$$

Since the radius of convergence of

$$\sum_0^\infty \epsilon_n z^n$$

is at least 1, we see that

$$Q(z) = 1 + q_1 z + \cdots + q_k z^k$$

has only one zero inside the unit circle, that is to say, $1/\theta$. Besides, since $\sum \epsilon_n^2 < \infty$, $f(z)$ has no pole of modulus 1;† hence, $Q(z)$ has one root, $1/\theta$, of modulus less than 1, all other roots being of modulus strictly larger than 1. The reciprocal polynomial,

$$z^k + q_1 z^{k-1} + \cdots + q_k,$$

has one root θ with modulus larger than 1, all other roots being strictly interior to the unit circle $|z| < 1$. Thus θ is, as stated, a number of the class S.

Since

$$-\frac{\lambda}{\theta} = \frac{P(1/\theta)}{Q'(1/\theta)},$$

λ is an algebraic number belonging to the field of θ.

† See footnote on page 10.

PROOF of Theorem B. In this theorem, we again write

$$\lambda\theta^n = a_n + \epsilon_n,$$

a_n being a rational integer and $|\epsilon_n| = \|\lambda\theta^n\| \leq \frac{1}{2}$. The assumption here is merely that $\epsilon_n \to 0$ as $n \to \infty$, without any hypothesis about the rapidity with which ϵ_n tends to zero. But here, we assume from the start that θ is algebraic, and we wish to prove that θ belongs to the class S.

Again, the first step will be to prove that the series

$$\sum_0^\infty a_n z^n$$

represents a rational function. But we shall not need here to make use of Lemma III. Let

$$A_0 + A_1\theta + \cdots + A_k\theta^k = 0$$

be the equation with rational integral coefficients which is satisfied by the algebraic number θ. We have, N being a positive integer,

$$\lambda\theta^N(A_0 + A_1\theta + \cdots + A_k\theta^k) = 0,$$

and, since

$$\lambda\theta^{N+p} = a_{N+p} + \epsilon_{N+p},$$

we have

$$A_0a_N + A_1a_{N+1} + \cdots + A_ka_{N+k} = -(A_0\epsilon_N + A_1\epsilon_{N+1} + \cdots + A_k\epsilon_{N+k}).$$

Since the A_j are fixed numbers, the second member tends to zero as $N \to \infty$, and since the first member is a rational integer, it follows that

$$A_0a_N + A_1a_{N+1} + \cdots + A_ka_{N+k} = 0$$

for all $N \geq N_0$. This is a recurrence relation satisfied by the coefficients a_n, and thus, by Lemma I, the series

$$\sum_0^\infty a_n z^n$$

represents a rational function.

From this point on, the proof follows identically the proof of Theorem A. (In order to show that $f(z)$ has no pole of modulus 1, the hypothesis $\epsilon_n \to 0$ is sufficient.†) Thus, the statement that θ belongs to the class S is proved.

† A power series $f(z) = \sum_0^\infty c_n z^n$ with $c_n = o(1)$ cannot have a pole *on* the unit circle. Suppose in fact, without loss of generality, that this pole is at the point $z = 1$. And let $z = r$ tend to $1 - 0$ along the real axis. Then $|f(z)| \leq \sum_0^\infty |c_n| r^n = o(1-r)^{-1}$, which is impossible if $z = 1$ is a pole.

4. An unsolved problem

As we pointed out before stating Theorems A and B, if we know only that $\theta > 1$ is such that there exists a real λ with the condition $\|\lambda\theta^n\| \to 0$ as $n \to \infty$, we are unable to conclude that θ belongs to the class S. We are only able to draw this conclusion either if we know that $\sum \|\lambda\theta^n\|^2 < \infty$ or if we know that θ is algebraic. In other words, the problem that is open is the existence of *transcendental* numbers θ with the property $\|\lambda\theta^n\| \to 0$ as $n \to \infty$.

We shall prove here the only theorem known to us about the numbers θ such that there exists a λ with $\|\lambda\theta^n\| \to 0$ as $n \to \infty$ (without any further assumption).

THEOREM. *The set of all numbers θ having the preceding property is denumerable.*

PROOF. We again write

$$\lambda\theta^n = a_n + \epsilon_n$$

where a_n is an integer and $|\epsilon_n| = \|\lambda\theta^n\|$. We have

$$a_{n+2} - \frac{a_{n+1}^2}{a_n} = \frac{a_na_{n+2} - a_{n+1}^2}{a_n}$$
$$= \frac{(\lambda\theta^n - \epsilon_n)(\lambda\theta^{n+2} - \epsilon_{n+2}) - (\lambda\theta^{n+1} - \epsilon_{n+1})^2}{\lambda\theta^n - \epsilon_n},$$

and an easy calculation shows that, since $\epsilon_n \to 0$, the last expression tends to zero as $n \to \infty$. Hence, for $n \geq n_0$, $n_0 = n_0(\lambda, \theta)$, we have

$$\left| a_{n+2} - \frac{a_{n+1}^2}{a_n} \right| < \frac{1}{2};$$

this shows that the integer a_{n+2} is uniquely determined by the two preceding integers, a_n, a_{n+1}. Hence, the infinite sequence of integers $\{a_n\}$ is determined uniquely by the first $n_0 + 1$ terms of the sequence.

This shows that the set of all possible sequences $\{a_n\}$ is denumerable, and, since

$$\theta = \lim \frac{a_{n+1}}{a_n},$$

that the set of all possible numbers θ is denumerable. The theorem is thus proved.

We can finally observe that since

$$\lambda = \lim \frac{a_n}{\theta^n},$$

the set of all values of λ is also denumerable.

EXERCISES

1. Let K be a real algebraic field of degree n. Let θ and θ' be two numbers of the class S, both of degree n and belonging to K. Then $\theta\theta'$ is a number of the class S. In particular, if q is any positive natural integer, θ^q belongs to S if θ does.

2. The result of Theorem A of this chapter can be improved in the sense that the hypothesis

$$\sum \| \lambda\theta^n \|^2 < \infty$$

can be replaced by the weaker one

$$\sum_{j=1}^{n} j \| \lambda\theta^j \|^2 = o(n).$$

It suffices, in the proof of Theorem A, and with the notations used in this proof, to remark that

$$(R_1 \cdots R_n)^{\frac{1}{n}} \leq \frac{R_1 + \cdots + R_n}{n}$$

and to show, by an easy calculation, that under the new hypothesis, the second member tends to zero for $n \to \infty$.

Chapter II

A PROPERTY OF THE SET OF NUMBERS OF THE CLASS S

1. The closure of the set of numbers belonging to S

THEOREM. *The set of numbers of the class S is a closed set.*

The proof of this theorem [12] is based on the following lemma.

LEMMA. *To every number θ of the class S there corresponds a real number λ such that $1 \leq \lambda < \theta$ and such that the series*

$$\sum_{0}^{\infty} \| \lambda\theta^n \|^2$$

converges with a sum less than an absolute constant (i.e., independent of θ and λ).

PROOF. Let $P(z)$ be the irreducible polynomial with rational integral coefficients having θ as one of its roots (all other roots being thus strictly interior to the unit circle $|z| < 1$), and write

$$P(z) = z^k + q_1 z^{k-1} + \cdots + q_k.$$

Let $Q(z)$ be the reciprocal polynomial

$$Q(z) = z^k P\left(\frac{1}{z}\right) = 1 + q_1 z + \cdots + q_k z^k.$$

We suppose first that P and Q are not identical, which amounts to supposing that θ is not a quadratic unit. (We shall revert later to this particular case.)

The power series

$$\frac{P(z)}{Q(z)} = c_0 + c_1 z + \cdots + c_n z^n + \cdots$$

has rational integral coefficients (since $Q(0) = 1$) and its radius of convergence is θ^{-1}. Let us determine μ such that

$$g(z) = \frac{\mu}{1 - \theta z} - \frac{P(z)}{Q(z)} \tag{1}$$

will be regular in the unit circle. If we set

$$P(z) = (z - \theta)P_1(z),$$
$$Q(z) = (1 - \theta z)Q_1(z),$$

then P_1 and Q_1 are reciprocal polynomials, and we have

$$\mu = \left(\frac{1}{\theta} - \theta\right) \frac{P_1(1/\theta)}{Q_1(1/\theta)}.$$

Since $\left|\dfrac{P_1(z)}{Q_1(z)}\right| = 1$ for $|z| = 1$, and since $\dfrac{P_1}{Q_1}$ is regular for $|z| \leq 1$, we have

$$\left|\frac{P_1(\theta^{-1})}{Q_1(\theta^{-1})}\right| < 1,$$

and, thus,

$$|\mu| < \theta - \frac{1}{\theta} < \theta. \tag{2}$$

Finally,

$$\begin{aligned} g(z) &= \sum_0^\infty \mu\theta^n z^n - \sum_0^\infty c_n z^n \\ &= \sum_0^\infty (\mu\theta^n - c_n) z^n \end{aligned}$$

has a radius of convergence *larger* than 1, since the roots of $Q(z)$ different from θ^{-1} are all *exterior* to the unit circle. Hence,

$$\sum_0^\infty (\mu\theta^n - c_n)^2 = \frac{1}{2\pi}\int_0^{2\pi} |g(e^{i\varphi})|^2 \, d\varphi.$$

But, by (1) and (2), we have for $|z| = 1$

$$|g(z)| < \frac{|\mu|}{\theta - 1} + \left|\frac{P}{Q}\right| < \frac{\theta^2 - 1}{\theta(\theta - 1)} + 1 = 2 + \frac{1}{\theta} < 3.$$

Hence,

$$\sum_0^\infty (\mu\theta^n - c_n)^2 < 9$$

which, of course, gives

$$\sum_0^\infty \| \mu\theta^n \|^2 < 9. \tag{3}$$

Now, by (2) $|\mu| < \theta$ and one can assume, by changing, if necessary, the sign of $\dfrac{P}{Q}$, that $\mu > 0$. (The case $\mu = 0$, which would imply $P\left(\dfrac{1}{\theta}\right) = 0$, is excluded for the moment, since we have assumed that θ is not a quadratic unit.) We can, therefore, write $0 < \mu < \theta$.

To finish the proof of the lemma, we suppose $\mu < 1$. (Otherwise we can take $\lambda = \mu$ and there is nothing to prove.) There exists an integer s such that

$$\frac{1}{\theta^s} \leq \mu < \frac{1}{\theta^{s-1}}$$

or

$$1 \leq \theta^s\mu < \theta,$$

We take $\lambda = \theta^s\mu$ and have by (3)

$$\begin{aligned} \sum_0^\infty \| \lambda\theta^n \|^2 &= \sum_0^\infty \| \mu\theta^{n+s} \|^2 \\ &= \sum_s^\infty \| \mu\theta^m \|^2 \\ &< \sum_0^\infty \| \mu\theta^m \|^2 < 9. \end{aligned}$$

Since $1 \leq \lambda < \theta$, this last inequality proves the lemma when θ is not a quadratic unit.

It remains to consider the case when θ is a quadratic unit. (This particular case is not necessary for the proof of the theorem, but we give it for the sake of completeness.) In this case

$$\theta^n + \theta^{-n}$$

is a rational integer, and

$$\| \theta^n \| \leq \frac{1}{\theta^n}.$$

Thus,

$$\sum_0^\infty \| \theta^n \|^2 < \sum_0^\infty \frac{1}{\theta^{2n}} = \frac{\theta^2}{\theta^2 - 1}$$

and since $\theta + \dfrac{1}{\theta}$ is at least equal to 3, we have $\theta \geq 2$ and

$$\frac{\theta^2}{\theta^2 - 1} < \frac{4}{3}.$$

Thus, since $\sum \| \theta^n \|^2 < \frac{4}{3}$, the lemma remains true, with $\lambda = 1$.

Remark. Instead of considering in the lemma the convergence of

$$\sum_0^\infty \| \lambda\theta^n \|^2$$

we can consider the convergence (obviously equivalent) of

$$\sum_0^\infty \sin^2 \pi\lambda\theta^n.$$

In this case we have

$$\sum_0^\infty \sin^2 \pi\lambda\theta^n \leq 9\pi^2.$$

PROOF of the theorem. Consider a sequence of numbers of the class S, $\theta_1, \theta_2, \ldots, \theta_p, \ldots$ tending to a number ω. We have to prove that ω belongs to S also.

Let us associate to every θ_p the corresponding λ_p of the lemma such that

$$1 \leq \lambda_p < \theta_p, \quad \sum_0^\infty \sin^2 \pi\lambda_p\theta_p{}^n < 9\pi^2. \tag{4}$$

Considering, if necessary, a subsequence only of the θ_p, we can assume that the λ_p which are included, for p large enough, between 1 and, say, 2ω, tend to a limit μ. Then (4) gives immediately

$$\sum_0^\infty \sin^2 \pi\mu\omega^n \leq 9\pi^2$$

which, by Theorem A of Chapter I, proves that ω belongs to the class S. Hence, the set of all numbers of S is closed.

It follows that 1 is not a limit point of S. In fact it is immediate that $\theta \in S$ implies, for all integers $q > 0$, that $\theta^q \in S$. Hence, if $1 + \epsilon_m \in S$, with $\epsilon_m \to 0$, one would have

$$(1 + \epsilon_m)^{\left[\frac{\alpha}{\epsilon_m}\right]} \in S,$$

α being any real positive number and $\left[\dfrac{\alpha}{\epsilon_m}\right]$ denoting the integral part of $\dfrac{\alpha}{\epsilon_m}$. But, as $m \to \infty$, $\epsilon_m \to 0$ and

$$(1 + \epsilon_m)^{\left[\frac{\alpha}{\epsilon_m}\right]} \to e^\alpha.$$

It would follow that the numbers of S would be everywhere dense, which is contrary to our theorem.

2. Another proof of the closure of the set of numbers belonging to the class S

This proof, [13], [11], is interesting because it may be applicable to different problems.

Let us first recall a classical definition: If $f(z)$ is analytic and regular in the unit circle $|z| < 1$, we say that it *belongs to the class* H^p $(p > 0)$ if the integral

$$\int_0^{2\pi} |f(re^{i\varphi})|^p \, d\varphi \quad (r < 1)$$

is bounded for $r < 1$. (See, e.g., [17].)

This definition can be extended in the following way. Suppose that $f(z)$ is meromorphic for $|z| < 1$, and that it has only a finite number of poles there (nothing is assumed for $|z| = 1$). Let $z_1, \ldots, z_m$, be the poles and denote by $P_j(z)$ the principal part of $f(z)$ in the neighborhood of z_j. Then the function

$$g(z) = f(z) - \sum_{j=1}^m P_j(z)$$

is regular for $|z| < 1$, and if $g(z) \in H^p$ (in the classical sense), we shall say that $f(z) \in H^p$ (in the extended sense).

We can now state Theorem A of Chapter I in the following equivalent form.

THEOREM A′. *Let $f(z)$ be analytic, regular in the neighborhood of the origin, and such that its expansion there*

$$\sum_0^\infty a_n z^n$$

has rational integral coefficients. Suppose that $f(z)$ is regular for $|z| < 1$, except for a simple pole $1/\theta$ $(\theta > 1)$. Then, if $f(z) \in H^2$, it is a rational function and θ belongs to the class S.

The reader will see at once that the two forms of Theorem A are equivalent.

Now, before giving the new proof of the theorem of the closure of S, we shall prove a lemma.

LEMMA. *Let $P(z)$ be the irreducible polynomial having rational integral coefficients and having a number $\theta \in S$ for one of its roots. Let*

$$Q(z) = z^k P\left(\frac{1}{z}\right)$$

be the reciprocal polynomial (k *being the degree of* P). *Let λ be such that*

$$\frac{\lambda}{1 - \theta z} - \frac{P(z)}{Q(z)}$$

is regular in the neighborhood of $1/\theta$ and, hence, for all $|z| < 1$. [We have already seen that $|\lambda| < \theta - \dfrac{1}{\theta}$ (and that thus, changing if necessary the sign of Q, we can take $0 < \lambda < \theta - \dfrac{1}{\theta}$).] *Then, in the opposite direction* [11],

$$\lambda > \frac{1}{2(\theta + 1)},$$

provided θ is not quadratic, and thus $P \neq Q$.

PROOF. We have already seen that

$$\frac{P(z)}{Q(z)} = \sum_0^\infty c_n z^n,$$

the coefficients c_n being rational integers. We now write

$$g(z) = \frac{\lambda}{1 - \theta z} - \frac{P(z)}{Q(z)} = \sum_0^\infty (\lambda\theta^n - c_n) z^n = \sum_0^\infty \epsilon_n z^n.$$

We have

$$I = \frac{1}{2\pi} \int_0^{2\pi} |g(e^{i\varphi})|^2 \, d\varphi = \sum_0^\infty \epsilon_n{}^2, \tag{5}$$

as already stated.

On the other hand, the integral can be written

$$I = \frac{1}{2\pi i}\int_C \left\{\frac{\lambda}{1-\theta z} - \frac{P}{Q}(z)\right\}\left\{\frac{\lambda}{1-\frac{\theta}{z}} - \frac{P}{Q}\left(\frac{1}{z}\right)\right\}\frac{dz}{z},$$

where the integral is taken along the unit circle, or

$$I = \frac{1}{2\pi i}\int_C \left\{\frac{\lambda}{1-\theta z} - \frac{P}{Q}\right\}\left\{\frac{\lambda}{z-\theta} - \frac{Q}{zP}\right\} dz.$$

But changing z into $1/z$, we have

$$\int_C \frac{\lambda}{1-\theta z}\frac{Q}{zP}\,dz = -\int_C \frac{\lambda}{1-\frac{\theta}{z}}\frac{P}{Q}\frac{dz}{z} = \int_C \frac{\lambda}{z-\theta}\frac{P}{Q}\,dz$$

$$= \frac{\lambda}{\frac{1}{\theta}-\theta}\lim\left\{\left(z-\frac{1}{\theta}\right)\frac{P}{Q}\right\}_{z=\frac{1}{\theta}} = \frac{\lambda}{\frac{1}{\theta}-\theta}\left(-\frac{\lambda}{\theta}\right) = \frac{\lambda^2}{\theta^2-1}.$$

Therefore,

$$I = \frac{1}{2\pi i}\int_C \frac{dz}{z} - \frac{2\lambda^2}{\theta^2-1} + \frac{1}{2\pi i}\int_C \frac{\lambda^2}{(1-\theta z)(z-\theta)}\,dz$$

$$= 1 - \frac{2\lambda^2}{\theta^2-1} + \frac{\lambda^2}{\frac{1}{\theta}-\theta}\left[\frac{z-\frac{1}{\theta}}{1-\theta z}\right]_{z=\frac{1}{\theta}}$$

$$= 1 - \frac{2\lambda^2}{\theta^2-1} + \frac{\lambda^2}{\theta^2-1} = 1 - \frac{\lambda^2}{\theta^2-1}$$

and thus (5) gives

$$1 - \frac{\lambda^2}{\theta^2-1} = \sum_0^\infty \epsilon_n^2. \tag{6}$$

This leads to

$$|\lambda| < \sqrt{\theta^2-1}$$

or changing, if necessary, the sign of Q, to $\lambda < \sqrt{\theta^2-1}$ (an inequality weaker than $\lambda < \theta - \frac{1}{\theta}$ already obtained in (2)).

On the other hand, since $\lambda - c_0 = \epsilon_0$, we have

$$|\lambda - c_0| = |\epsilon_0| < 1.$$

But

$$c_0 = \frac{P(0)}{Q(0)} = \frac{q_k}{\pm 1} \geq 1.$$

Hence $\lambda > 0$ and $c_0 < \lambda + 1$.

We shall now prove that

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

In fact, suppose that

$$\lambda \leq \frac{1}{2(\theta+1)};$$

then $\lambda < \frac{1}{4}$ and necessarily $c_0 = 1$. But, since

$$\frac{P}{Q}(1-\theta z) = c_0 + \sum_1^\infty (c_n - \theta c_{n-1})z^n,$$

we have, if $z = e^{i\varphi}$,

$$\frac{1}{2\pi}\int_0^{2\pi}\left|\frac{P}{Q}(1-\theta z)\right|^2 d\varphi = c_0^2 + \sum_1^\infty (c_n - \theta c_{n-1})^2,$$

and since $\left|\frac{P}{Q}\right| = 1$ for $|z| = 1$ and the integral is

$$1 + \theta^2,$$

the equality $c_0 = 1$ implies

$$|c_1 - \theta| < \theta.$$

Hence, since c_1 is an integer, $c_1 \geq 1$.

And thus, since by (6)

$$\frac{\lambda^2}{\theta^2-1} + \epsilon_0^2 + \epsilon_1^2 < 1,$$

we have, with $c_0 = 1$, $c_1 \geq 1$, $\lambda\theta \leq \frac{1}{2}$,

$$\frac{\lambda^2}{\theta^2-1} + (\lambda-1)^2 + (\lambda\theta-1)^2 < \frac{\lambda^2}{\theta^2-1} + (\lambda-c_0)^2 + (\lambda\theta-c_1)^2 < 1,$$

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

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

This contradicts

$$\lambda \leq \frac{1}{2(\theta+1)}.$$

Thus, as stated,

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

We can now give the new proof of the theorem stating the closure of S.

Proof. Let ω be a limit point of the set S, and suppose first $\omega > 1$. Let $\{\theta_s\}$ be an infinite sequence of numbers of S, tending to ω as $s \to \infty$. Denote by $P_s(z)$ the irreducible polynomial with rational integral coefficients and having the root θ_s and let K_s be its degree (the coefficient of z^{K_s} being 1). Let

$$Q_s(z) = z^{K_s} P_s\left(\frac{1}{z}\right)$$

be the reciprocal polynomial. The rational function P_s/Q_s is regular for $|z| \le 1$ except for a single pole at $z = \theta_s^{-1}$, and its expansion around the origin

$$\frac{P_s}{Q_s} = \sum_{n=0}^{\infty} a_n^{(s)} z^n$$

has rational integral coefficients.

Determine now λ_s such that

$$g_s(z) = \frac{\lambda_s}{1 - \theta_s z} - \frac{P_s(z)}{Q_s(z)} \tag{7}$$

will be regular for $|z| \le 1$. (We can discard in the sequence $\{\theta_s\}$ the quadratic units, for since $\theta_s \to \omega$, K_s is necessarily unbounded.)† By the lemma, and changing, if necessary, the sign of Q_s, we have

$$\frac{1}{2(\theta_s + 1)} < \lambda_s < \theta_s.$$

Therefore, we can extract from the sequence $\{\lambda_s\}$ a subsequence tending to a limit different from 0. (We avoid complicating the notations by assuming that this subsequence is the original sequence itself.)

On the other hand, if $|z| = 1$,

$$|g_s(z)| < \frac{|\lambda_s|}{\theta_s - 1} + 1 < A,$$

A being a constant independent of s. Since $g_s(z)$ is regular, this inequality holds for $|z| \le 1$.

We can then extract from the sequence $\{g_s(z)\}$, which forms a normal family, a subsequence tending to a limit $g^*(z)$. (And again we suppose, as we may, that this subsequence is the original sequence itself.) Then (7) gives

$$g^*(z) = \frac{\mu}{1 - \omega z} - \lim \frac{P_s}{Q_s}.$$

Since the coefficients $a_n^{(s)}$ of the expansion of P_s/Q_s are rational integers, their limits can only be rational integers. Thus the limit of P_s/Q_s satisfies all requirements of Theorem A'. (The fact that $g^*(z) \in H^2$ is a trivial consequence of its

† See Appendix, 5.

boundedness, since $|g^*(z)| \le A$.) Therefore ω is a number of the class S, since $1/\omega$ is actually a pole for

$$\lim \frac{P_s}{Q_s},$$

because $\mu \ne 0$. (This is essential, and is the reason for proving a lemma to the effect that the λ_s are bounded *below*.)

Exercise

Let a be a natural positive integer ≥ 2. Then a is a limit point for the numbers of the class S. (Considering the equation

$$z^n(z - a) - 1 = 0,$$

the result for $a > 2$ is a straightforward application of Rouché's theorem. With a little care, the argument can be extended to $a = 2$.)

Chapter III

APPLICATIONS TO THE THEORY OF POWER SERIES; ANOTHER CLASS OF ALGEBRAIC INTEGERS

1. A generalization of the preceding results

Theorem A′ of Chapter II can be extended, and thus restated in the following way.

THEOREM A″. *Let $f(z)$ be analytic, regular in the neighborhood of the origin, and such that the coefficients of its expansion in this neighborhood,*

$$\sum_0^\infty a_n z^n$$

are either rational integers or integers of an imaginary quadratic field. Suppose that $f(z)$ is regular for $|z| < 1$ except for a finite number of poles $1/\theta_i$ ($|\theta_i| > 1$, $i = 1, 2, \ldots, k$). Then if $f(z)$ belongs to the class H^2 (in the extended sense), $f(z)$ is a rational function, and the θ_i are algebraic integers.

The new features of this theorem, when compared with Theorem A′, are:

1. We can have several (although a *finite* number of) poles.
2. The coefficients a_n need not be rational integers, but can be integers of an imaginary quadratic field.

Nevertheless, the proof, like that for Theorem A′, follows exactly the pattern of the proof of Theorem A (see [10]). Everything depends on showing that a certain Kronecker determinant is zero when its order is large enough. The transformation of the determinant is based on the same idea, and the fact that it is zero is proved by showing that it tends to zero. For this purpose, one uses the well-known fact [9] that the integers of imaginary quadratic fields share with the rational integers the property of not having zero as a limit point.

Theorem A″ shows, in particular, that if

$$f(z) = \sum_0^\infty a_n z^n,$$

where the a_n are rational integers, is regular in the neighborhood of $z = 0$, has only a finite number of poles in $|z| < 1$, and is uniformly bounded in the neighborhood of the circumference $|z| = 1$, then $f(z)$ is a rational function.

This result suggests the following extension.

THEOREM I. *Let*

$$f(z) = \sum_0^\infty a_n z^n,$$

where the a_n are rational integers, be regular in the neighborhood of $z = 0$, and

suppose that $f(z)$ is regular for $|z| < 1$ except for a finite number of poles. Let α be any imaginary or real number. If there exist two positive numbers, δ, η ($\eta < 1$) such that $|f(z) - \alpha| > \delta$ for $1 - \eta \leq |z| < 1$, then $f(z)$ is a rational function.

PROOF. For the sake of simplicity, we shall assume that there is only *one* pole, the proof in this case being typical. We shall also suppose, to begin with, that $\alpha = 0$, and we shall revert later to the general case.

Let ϵ be any positive number such that $\epsilon < \eta$. If ϵ is small enough, there is *one* pole of $f(z)$ for $|z| < 1 - \epsilon$, and, say N zeros, N being independent of ϵ. Consider

$$g(z) = \frac{1}{1 + mz\,f(z)},$$

m being a positive integer, and consider the variation of the argument of $mz\,f(z)$ along the circumference $|z| = 1 - \epsilon$. We have, denoting this circumference by Γ,

$$\Delta_\Gamma \operatorname{Arg}[mz\,f(z)] = 2\pi[N + 1 - 1] = 2\pi N.$$

If now we choose m such that $m(1 - \eta)\delta > 2$, we have for $|z| = 1 - \epsilon$,

$$|mz\,f(z)| > m(1 - \eta)\delta > 2,$$

and thus we have also

$$\Delta_\Gamma \operatorname{Arg}[1 + mz\,f(z)] = 2\pi N.$$

But $mz\,f(z) + 1$ has one pole in $|z| < 1 - \epsilon$; hence it has $N + 1$ zeros. Since ϵ can be taken arbitrarily small, it follows that $g(z)$ has $N + 1$ poles for $|z| < 1$. But the expansion of $g(z)$ in the neighborhood of the origin,

$$\sum_0^\infty c_n z^n,$$

has rational integral coefficients. And, in the neighborhood of the circumference $|z| = 1$, $g(z)$ is bounded, since

$$|1 + mzf| > |mzf| - 1 > m(1 - \eta)\delta - 1 > 1.$$

Hence, by Theorem A″ g is a rational function, and so is $f(z)$.

If now $\alpha \neq 0$, let $\alpha = \lambda + \mu i$; we can obviously suppose λ and μ rational, and thus

$$\alpha = \frac{p + qi}{r},$$

p, q, and r being rational integers. Then

$$|rf - (p + qi)| \geq r\delta,$$

and we consider $f^* = rf - (p + qi)$. Then we apply Theorem A″ in the case of Gaussian integers (integers of $K(i)$).

Extensions. The theorem can be extended [13] (1) to the case of the a_n being integers of an imaginary quadratic field, (2) to the case where the number of poles in $|z| < 1$ is infinite (with limit points on $|z| = 1$), (3) to the case of the a_n being integers after only a certain rank $n \geq n_0$, (4) to the case when $z = 0$ is itself a pole. The proof with these extensions does not bring any new difficulties or significant changes into the arguments.

A particular case of the theorem can be stated in the following simple way.

Let

$$f(z) = \sum_0^\infty a_n z^n$$

be a power series with rational integral coefficients, converging for $|z| < 1$. *Let S be the set of values taken by* $f(z)$ *when* $|z| < 1$. *If the derived set* S' *is not the whole plane,* $f(z)$ *is a rational function.*

In other words if $f(z)$ is not a rational function, it takes in the unit circle values arbitrarily close to any given number α.

It is interesting to observe that the result would become false if we replace the *whole* unit circle by a circular sector. We shall, in fact, construct a power series with integral coefficients, converging for $|z| < 1$, which is not a rational function, and which is bounded in a certain circular sector of $|z| < 1$. Consider the series

$$f(z) = \sum_{p=0}^\infty \frac{z^{p^2}}{(1-z)^p}.$$

It converges uniformly for $|z| < r$ if r is any number less than 1. In fact

$$\left|\frac{z^{p^2}}{(1-z)^p}\right| \leq \frac{r^{p^2}}{(1-r)^p},$$

which is the general term of a positive convergent series. Hence, $f(z)$ is analytic and regular for $|z| < 1$. It is obvious that its expansion in the unit circle has integral rational coefficients. The function $f(z)$ cannot be rational, for $z = 1$ cannot be a pole of $f(z)$, since $(1-z)^k f(z)$ increases infinitely as $z \to 1 - 0$ on the real axis, no matter how large the integer k. Finally, $f(z)$ is bounded, say, in the half circle

$$|z| < 1, \quad \Re(z) \leq 0.$$

For, if $\frac{3}{4} < |z| < 1$, say, then

$$|1 - z| > (1 + \tfrac{9}{16})^{\frac{1}{2}} = \tfrac{5}{4},$$

and thus

$$|f(z)| < \sum_0^\infty (\tfrac{4}{5})^p.$$

The function $f(z)$ is even continuous on the arc $|z| = 1$, $\Re(z) \leq 0$.

2. Schlicht power series with integral coefficients [13]

THEOREM II. *Let* $f(z)$ *be analytic and schlicht (simple) inside the unit circle* $|z| < 1$. *Let its expansion in the neighborhood of the origin be*

$$f(z) = a_{-1}z^{-1} + \sum_0^\infty a_n z^n.$$

If an integer p exists such that for all $n \geq p$ *the coefficients* a_n *are rational integers (or integers of an imaginary quadratic field), then* $f(z)$ *is a rational function.*

PROOF. Suppose first that $a_{-1} \neq 0$. Then the origin is a pole, and since there can be no other pole for $|z| < 1$, the expansion written above is valid in all the open disc $|z| < 1$. Moreover, the point at infinity being an interior point for the transformed domain, $f(z)$ is bounded for, say, $\frac{1}{2} < |z| < 1$. Hence the power series

$$\sum_0^\infty a_n z^n$$

is bounded in the unit circle, and the nature of its coefficients shows that it is a polynomial, which proves the theorem in this case.

Suppose now that $a_{-1} = 0$. Then $f(z)$ may or may not have a pole inside the unit circle. The point $f(0) = a_0$ is an interior point for the transformed domain. Let $u = f(z)$. To the circle C, $|u - a_0| < \delta$, in the u-plane there corresponds, for δ small enough, a domain D in the z-plane, including the origin, and completely interior, say, to the circle $|z| < \frac{1}{2}$. Now, by Theorem I, if $f(z)$ is not rational, there exists in the ring $\frac{2}{3} < |z| < 1$ a point z_1 such that $|f(z_1) - a_0| < \delta/2$. Then $u_1 = f(z_1)$ belongs to the circle C and consequently there exists in the domain D a point z_2, necessarily distinct from z_1, such that $f(z_2) = u_1 = f(z_1)$. This contradicts the hypothesis that $f(z)$ is schlicht. Hence, $f(z)$ is a rational function.

3. A class of power series with integral coefficients [13]; **the class** T **of algebraic integers and their characterization**

Let $f(z)$ be a power series with rational integral coefficients, converging for $|z| < 1$ and admitting at least *one* "exceptional value" in the sense of Theorem I; i.e., we assume that $|f(z) - \alpha| > \delta > 0$ uniformly as $|z| \to 1$. Then $f(z)$ is rational and it is easy to find its form. For

$$f(z) = \frac{P(z)}{Q(z)},$$

P and Q being polynomials with rational integral coefficients, and by Fatou's lemma (see Chapter I) $Q(0) = 1$. The polynomial $Q(z)$ must have no zeros inside the unit circle (P/Q being irreducible) and, since $Q(0) = 1$, it means that all zeros are *on* the unit circle. By a well-known theorem of Kronecker [9] these zeros are all roots of unity unless $Q(z)$ is the constant 1.

Now, suppose that the expansion

$$\sum_{0}^{\infty} a_n z^n,$$

with rational integral coefficients, of $f(z)$ is valid only in the neighborhood of the origin, but that $f(z)$ has a simple pole $1/\tau$ ($|\tau| > 1$) and no other singularity for $|z| < 1$.

Suppose again that there exists at least one exceptional value α such that $|f(z) - \alpha| > \delta > 0$ uniformly as $|z| \to 1$. Then $f(z)$ is rational; i.e.,

$$f(z) = \frac{P}{Q},$$

P, Q being polynomials with rational integral coefficients, P/Q irreducible, and $Q(0) = 1$. The point $1/\tau$ is a simple zero for $Q(z)$ and there are no other zeros of modulus less than 1. If $f(z)$ is bounded on the circumference $|z| = 1$, $Q(z)$ has no zeros of modulus 1, all the conjugates of $1/\tau$ lie outside the unit circle, and τ belongs to the class S.

If, on the contrary, $f(z)$ is unbounded on $|z| = 1$, $Q(z)$ has zeros of modulus 1. If all these zeros are roots of unity, $Q(z)$ is divisible by a cyclotomic polynomial, and again τ belongs to the class S. If not, τ is an algebraic integer whose conjugates lie all *inside or on* the unit circle.

We propose to discuss certain properties of this new class of algebraic integers.

DEFINITION. *A number* τ belongs to the class T *if it is an algebraic integer whose conjugates all lie inside or on the unit circle, assuming that some conjugates lie actually on the unit circle (for otherwise τ would belong to the class S).*

Let $P(z) = 0$ be the irreducible equation determining τ. Since there must be at least one root of modulus 1, and since this root is not ± 1, there must be *two* roots, imaginary conjugates, α and $1/\alpha$ on the unit circle. Since $P(\alpha) = 0$ and $P(1/\alpha) = 0$ and P is irreducible, P is a reciprocal polynomial; τ is its only root outside, and $1/\tau$ its only root inside, the unit circle; τ is real (we may always suppose $\tau > 0$; hence $\tau > 1$). There is an even number of imaginary roots of modulus 1, and the degree of P is even, at least equal to 4. Finally, τ is a unit. If $P(z)$ is of degree $2k$ and if we write

$$y = z + \frac{1}{z},$$

the equation $P(z) = 0$ is transformed into an equation of degree k, $R(y) = 0$, whose roots are algebraic integers, all real. One of these, namely $\tau + \tau^{-1}$, is larger than 2, and all others lie between -2 and $+2$.

We know that the characteristic property of the numbers θ of the class S is that to each $\theta \in S$ we can associate a real $\lambda \neq 0$ such that $\sum \| \lambda\theta^n \|^2 < \infty$; i.e., the series $\sum \| \lambda\theta^n \| z^n$ belongs to the class H^2.†

† Of course, if $\theta \in S$, the series is even *bounded* in $|z| < 1$. But it is *enough* that it should belong to H^2 in order that θ should belong to S.

The corresponding theorem for the class T is the following one.

THEOREM III. *Let τ be a real number > 1. A necessary and sufficient condition for the existence of a real $\mu \neq 0$ such that the power series* †

$$\sum_{0}^{\infty} \{\mu\tau^n\} z^n$$

should have its real part bounded above (without belonging to the class H^2) for $|z| < 1$ is that τ should belong to the class T. Then μ is algebraic and belongs to the field of τ.

PROOF. *The condition is necessary.* Let a_n be the integer nearest to $\mu\tau^n$, so that $\mu\tau^n = a_n + \{\mu\tau^n\}$. We have

$$\frac{\mu}{1 - \tau z} = \sum_{0}^{\infty} a_n z^n + \sum_{0}^{\infty} \{\mu\tau^n\} z^n.$$

Now if

$$\frac{\tau + 1}{2\tau} < |z| < 1$$

we have

$$|1 - \tau z| > \tfrac{1}{2}(\tau - 1).$$

Hence,

$$\left| \sum_{0}^{\infty} a_n z^n + \sum_{0}^{\infty} \{\mu\tau^n\} z^n \right| \leq \frac{2|\mu|}{\tau - 1}.$$

Therefore, the real part of

$$f(z) = \sum_{0}^{\infty} a_n z^n$$

is bounded below in the ring

$$\frac{\tau + 1}{2\tau} < |z| < 1.$$

Since this power series has rational integral coefficients and is regular in $|z| < 1$ except for the pole $1/\tau$, it follows, by Theorem I, that it represents a rational function and, hence, that τ is a number, either of the class S or of the class T. Since $f(z)$ is not in H^2, τ is not in S, and thus belongs to T. The calculation of residues shows that μ is algebraic and belongs to the field of τ.

The condition is sufficient. Let τ be a number of the class T and let $2k$ be its degree. Let

$$\tau^{-1}, \alpha_j, \alpha_j^* \quad (j = 1, 2, \ldots, k - 1;\ \alpha_j\alpha_j^* = 1)$$

be its conjugates. Let

$$\sigma = \tau + \tau^{-1}, \quad \rho_j = \alpha_j + \alpha_j^*,$$

so that $\sigma, \rho_1, \rho_2, \ldots, \rho_{k-1}$ are conjugate algebraic integers of degree k.

† See the Introduction (page 1) for the notation $\{a\}$. We recall that $\|a\| = |\{a\}|$.

The determinant

$$\Delta = \begin{vmatrix} 1 & \sigma & \cdots & \sigma^{k-1} \\ 1 & \rho_1 & \cdots & \rho_1^{k-1} \\ \cdots & \cdots & \cdots & \cdots \\ 1 & \rho_{k-1} & \cdots & \rho_{k-1}^{k-1} \end{vmatrix}$$

being not zero, we can, by Minkowski's theorem (as given at the beginning of Chapter VI and Appendix, 9), find rational integers $A_1, \ldots, A_k$, such that the number

$$\theta = A_1\sigma^{k-1} + \cdots + A_{k-1}\sigma + A_k$$

has its conjugates $\beta_1, \ldots, \beta_{k-1}$ all less than 1 in absolute value. In other words, θ is a number of the class S belonging to the field of σ. Its conjugates are all real. Take now

$$\mu = \theta^{2h} \quad \text{and} \quad \gamma_j = \beta_j^{2h},$$

h being a positive integer such that

$$\gamma_1 + \gamma_2 + \cdots + \gamma_{k-1} < \tfrac{1}{8}.$$

Since $\sigma = \tau + \tau^{-1}$ and τ is a unit, μ is an algebraic integer of the field of τ, $K(\tau)$, and the numbers

$$\mu \text{ itself}, \gamma_1, \gamma_1, \gamma_2, \gamma_2, \ldots, \gamma_{k-1}, \gamma_{k-1}$$

correspond to μ in the conjugate fields

$$K(\tau^{-1}), K(\alpha_1), K(\alpha_1^*), \ldots, K(\alpha_{k-1}), K(\alpha_{k-1}^*)$$

respectively. It follows that the function

$$f(z) = \frac{\mu}{1 - \tau z} + \frac{\mu}{1 - \tau^{-1}z} + \sum_1^{k-1} \frac{\gamma_j}{1 - \alpha_j z} + \sum_1^{k-1} \frac{\gamma_j}{1 - \alpha_j^* z}$$

has, in the neighborhood of the origin, an expansion

$$\sum_0^\infty a_n z^n$$

with rational integral coefficients. The only singularity of $f(z)$ for $|z| < 1$ is the pole $1/\tau$. We have

$$\sum_0^\infty (a_n - \mu\tau^n)z^n = \sum_0^\infty a_n z^n - \frac{\mu}{1 - \tau z} = \frac{\mu}{1 - \tau^{-1}z} + \sum_1^{k-1} \frac{\gamma_j}{1 - \alpha_j z} + \sum_1^{k-1} \frac{\gamma_j}{1 - \alpha_j^* z}.$$

By well-known properties of linear functions we have for $|\alpha| = 1$ and $|z| < 1$

$$\Re\left(\frac{1}{1 - \alpha z}\right) \geq \frac{1}{2}$$

and

$$\Re\left(\frac{1}{1 - \tau^{-1}z}\right) \geq \frac{\tau}{\tau + 1}.$$

Therefore, since $\gamma_j > 0$, we have for $|z| < 1$

$$\Re\left\{\sum_0^\infty (a_n - \mu\tau^n)z^n\right\} \geq \frac{\mu\tau}{\tau + 1} + \sum_1^{k-1} \gamma_j > \frac{\mu\tau}{\tau + 1}.$$

On the other hand,

$$a_n = \mu\tau^n + \mu\tau^{-n} + \sum_1^{k-1} \gamma_j(\alpha_j^n + \alpha_j^{*n})$$

and, since $|\alpha_j^n + \alpha_j^{*n}| < 2$,

$$\left|\sum_1^{k-1} \gamma_j(\alpha_j^n + \alpha_j^{*n})\right| < 2\sum_1^{k-1} \gamma_j < \tfrac{1}{4}.$$

Take now for m the smallest integer such that

$$\frac{\mu}{\tau^m} < \frac{1}{4}; \quad \text{i.e., } m = \left[\frac{\log 4\mu}{\log \tau}\right] + 1.$$

Then, for $n \geq m$

$$|a_n - \mu\tau^n| < \tfrac{1}{2}; \quad \text{i.e., } a_n - \mu\tau^n = -\{\mu\tau^n\}.$$

Therefore, we can write

$$\Re\left\{\sum_0^{m-1} (a_n - \mu\tau^n)z^n - \sum_m^\infty \{\mu\tau^n\} z^n\right\} > \frac{\mu\tau}{\tau + 1}.$$

On the other hand, since for all n

$$|a_n - \mu\tau^n| < \frac{\mu}{\tau^n} + \frac{1}{4},$$

we have for $|z| < 1$

$$\left|\sum_0^{m-1} (a_n - \mu\tau^n)z^n\right| < \frac{m}{4} + \mu\sum_0^{m-1} \frac{1}{\tau^n} < \frac{m}{4} + \frac{\mu\tau}{\tau - 1},$$

whence, finally,

$$\Re\left\{\sum_m^\infty \{\mu\tau^n\} z^n\right\} < \frac{m}{4} + \frac{\mu\tau}{\tau - 1} - \frac{\mu\tau}{\tau + 1} = \frac{m}{4} + \frac{2\mu\tau}{\tau^2 - 1}.$$

Thus

$$\Re\left\{\sum_0^\infty \{\mu\tau^n\} z^n\right\} < \frac{3m}{4} + \frac{2\mu\tau}{\tau^2 - 1} = A(\mu, \tau),$$

where A is a function of μ and τ only, which proves the second part of our theorem.

4. Properties of the numbers of the class T

THEOREM IV. *Every number of the class S*† *is a limit point of numbers of the class T on both sides* [13].

PROOF. Let θ be a number of the class S, root of the irreducible polynomial

$$P(z) = z^p + c_1 z^{p-1} + \cdots + c_p$$

with rational integral coefficients. Let $Q(z)$ be the reciprocal polynomial.

We suppose first that θ is not a quadratic unit, so that Q and P will not be identical.

We denote by m a positive integer, and let

$$R_m(z) = z^m P(z) + Q(z).$$

Then $R_m(z)$ is a reciprocal polynomial whose zeros are algebraic integers.

We denote by ϵ a positive number and consider the equation

$$(1 + \epsilon) z^m P + Q = 0.$$

Since for $|z| = 1$ we have $|P| = |Q|$, it follows by Rouché's theorem that *in* the circle $|z| = 1$ the number of roots of the last equation is equal to the number of roots of $z^m P$, that is to say, $m + p - 1$. As $\epsilon \to 0$, these roots vary continuously. Hence, for $\epsilon = 0$ we have $m + p - 1$ roots with modulus ≤ 1 and, hence, at most one root *outside* the unit circle.‡

It is easy to show now that the root of $R_m(z)$ with modulus *larger* than 1 actually exists. In fact, we have first

$$R_m(\theta) = Q(\theta) \neq 0,$$

since θ is not quadratic. On the other hand, it is easily seen that $P'(\theta) > 0$. We fix $\sigma > 0$ small enough for $P'(z)$ to have no zeros on the real axis in the interval

$$\theta - \sigma \leq z \leq \theta + \sigma.$$

We suppose that in this interval $P'(z) > \mu$, μ being a positive number fixed as soon as σ is fixed.

If we take δ real and $|\delta| < \sigma$, $P(\theta + \delta)$ has the sign of δ and is in absolute value not less than $|\delta| \mu$. Hence, taking e.g.,

$$|\delta| = \frac{1}{\sqrt{m}},$$

† We recall that we do not consider the number 1 as belonging to the class S (see Chapter I).

‡ This proof, much shorter and simpler than the original one, has been communicated to me by Prof. Hirschman, during one of my lectures at the Sorbonne.

we see that for m large enough

$$R_m(\theta + \delta) = (\theta + \delta)^m P(\theta + \delta) + Q(\theta + \delta)$$

has the sign of δ. Taking $\delta Q(\theta) < 0$, we see that $R_m(\theta)$ and $R_m(\theta + \delta)$ are, for m large enough, of opposite sign, so that $R_m(z)$ has a root τ_m

$$\text{between } \theta \text{ and } \theta + m^{-\frac{1}{2}} \text{ if } Q(\theta) < 0,$$

and

$$\text{between } \theta - m^{-\frac{1}{2}} \text{ and } \theta \text{ if } Q(\theta) > 0.$$

Hence, $\tau_m \to \theta$ as $m \to \infty$.

This proves, incidentally, since we can have a sequence of τ_m all different tending to θ, that there exist numbers of the class T of arbitrarily large degree. It proves also that τ_m has, actually, conjugates of modulus 1, for m large enough, for evidently τ_m cannot be constantly quadratic (see Appendix, 5).

To complete the proof for θ not quadratic, we consider, instead of $z^m P + Q$, the polynomial

$$\frac{z^m P - Q}{z - 1},$$

which is also reciprocal, and we find a sequence of numbers of the class T approaching θ from the other side.

Suppose now that θ is a quadratic unit. Thus θ is a quadratic integer > 1, with conjugate $\frac{1}{\theta}$. Then $\theta + \theta^{-1}$ is a rational integer $r \geq 3$. Denote by $T_m(x)$ the first Tchebycheff polynomial of degree m (i.e., $T_m(x) = 2 \cos m\varphi$ for $x = 2 \cos \varphi$). T_m has m distinct real zeros between -2 and $+2$. The equation

$$(x - r) T_m(x) - 1 = 0$$

has then $m - 1$ real roots (algebraic integers) between -2 and $+2$, and one real root between r and $r + \epsilon_m$ ($\epsilon_m > 0$, $\epsilon_m \to 0$ as $m \to \infty$). Putting

$$x = y + \frac{1}{y},$$

we get an equation in y which gives us a number of the class T approaching θ from the right as $m \to \infty$.

We get numbers of T approaching θ from the left if we start from the equation

$$(x - r) T_m(x) + 1 = 0.$$

This completes the proof of the theorem.

We do not know whether numbers of T have limit points other than numbers of S.

5. Arithmetical properties of the numbers of the class T

We have seen at the beginning of Chapter I that, far from being uniformly distributed, the powers θ^n of a number θ of the class S tend to zero modulo 1.

On the contrary, the powers τ^m of a number τ of the class T are, modulo 1, everywhere dense in the interval (0, 1). In order to prove this, let us consider a number $\tau > 1$ of the class T, root of an irreducible equation of degree $2k$. We denote the roots of this equation by

$$\tau, \quad \frac{1}{\tau}, \quad \alpha_1, \quad \alpha_2, \quad \ldots, \quad \alpha_{k-1}, \qquad \bar{\alpha}_1, \quad \bar{\alpha}_2, \quad \ldots, \quad \bar{\alpha}_{k-1},$$

where $|\alpha_j| = 1$ and $\bar{\alpha}_j = \alpha_j^{-1}$ is the imaginary conjugate of α_j. We write

$$\alpha_j = e^{2\pi i\omega_j}.$$

Our first step will be to show that the ω_j $(j = 1, 2, \ldots, k-1)$ and 1 are linearly independent.† For suppose, on the contrary, the existence of a relation

$$A_0 + A_1\omega_1 + \cdots + A_{k-1}\omega_{k-1} = 0,$$

the A_j being rational integers. Then

$$e^{2\pi i(A_0 + \cdots + A_{k-1}\omega_{k-1})} = 1$$

or

$$\alpha_1^{A_1}\alpha_2^{A_2}\cdots\alpha_{k-1}^{A_{k-1}} = 1. \tag{1}$$

Since the equation considered is irreducible, it is known ([1] and Appendix, 6) that its Galois group is transitive; i.e., there exists an automorphism σ of the Galois group sending, e.g., the root α_1 into the root τ. This automorphism can not send any α_j into $1/\tau$; for. since $\sigma(\alpha_1) = \tau$,

$$\sigma\left(\frac{1}{\alpha_1}\right) = \frac{1}{\tau},$$

and thus this would imply

$$\alpha_j = \frac{1}{\alpha_1},$$

which is not the case. Thus the automorphism applied to (1) gives

$$\tau^{A_1}\alpha_2'^{A_2}\cdots\alpha_{k-1}'^{A_{k-1}} = 1$$

if $\sigma(\alpha_j) = \alpha_j'$ $(j \neq 1)$. This is clearly impossible since $\tau > 1$ and $|\alpha_s'| = 1$. Hence, we have proved the linear independence of the ω_j and 1.

Now, we have, modulo 1,

$$\tau^m + \frac{1}{\tau^m} + \sum_{j=1}^{k-1}(e^{2\pi im\omega_j} + e^{-2\pi im\omega_j}) \equiv 0$$

† This argument is due to Pisot.

or

$$\tau^m + 2\sum_{j=1}^{k-1}\cos 2\pi m\omega_j \to 0 \pmod 1$$

as $m \to \infty$. But by the well-known theorem of Kronecker on linearly independent numbers ([2] and Appendix, 8) we can determine the integer m, arbitrarily large, such that

$$2\sum_{j=1}^{k-1}\cos 2\pi m\omega_j$$

will be arbitrarily close to any number given in advance (mod 1). It is enough to take m, according to Kronecker, such that

$$|m\omega_1 - \delta| < \epsilon \pmod 1$$

$$|m\omega_j - \tfrac{1}{4}| < \epsilon \pmod 1 \quad (j = 2, 3, \ldots, k-1).$$

We have thus proved that the $\{\tau^m\}$ (mod 1) are everywhere dense.

The same argument applied to $\lambda\tau^m$, λ being an integer of the field of τ, shows that $\lambda\tau^m$ (mod 1) is everywhere dense in a certain interval.

THEOREM V. *Although the powers τ^m of a number τ of the class T are, modulo* 1, *everywhere dense, they are not uniformly distributed in* (0, 1).

In order to grasp better the argument, we shall first consider a number τ of the class T of the 4th degree. In this case the roots of the equation giving τ are

$$\tau, \quad \frac{1}{\tau}, \quad \alpha, \quad \bar{\alpha} = \frac{1}{\alpha} \quad (|\alpha| = 1),$$

and we have, m being a positive integer,

$$\tau^m + \frac{1}{\tau^m} + \alpha^m + \bar{\alpha}^m \equiv 0 \pmod 1.$$

Writing $\alpha = e^{2\pi i\omega}$, we have

$$\tau^m + \frac{1}{\tau^m} + 2\cos 2\pi m\omega \equiv 0 \pmod 1.$$

The number ω is irrational. This is a particular case of the above result, where we prove linear independence of $\omega_1, \omega_2, \ldots, \omega_{k-1}$, and 1. One can also argue in the following way. If ω were rational, α would be a root of 1, and the equation giving τ would not be irreducible.

Now, in order to prove the nonuniform distribution of τ^m (mod 1), it is enough to prove the nonuniform distribution of $2\cos 2\pi m\omega$. This is a consequence of the more general lemma which follows.

LEMMA. *If the sequence* $\{u_n\}_1^\infty$ *is uniformly distributed modulo* 1, *and if* $\omega(x)$ *is a continuous function, periodic with period* 1, *the sequence* $\omega(u_n) = v_n$ *is uniformly distributed if and only if the distribution function of* $\omega(x)$ (mod 1) *is linear.*†

PROOF of the lemma. Let (a, b) be any subinterval of $(0, 1)$ and let $\chi(x)$ be a periodic function, with period 1, equal for $0 \leq x < 1$ to the characteristic function of (a, b). The uniform distribution modulo 1 of $\{v_n\}$ is equivalent to

$$\lim \frac{\sum_1^N \chi(v_n)}{N} = b - a.$$

But, owing to the uniform distribution of $\{u_n\}$,

$$\lim \frac{1}{N}\sum_1^N \chi(v_n) = \lim \frac{1}{N}\sum_1^N \chi[\omega(u_n)] = \int_0^1 \chi(\omega(x))\, dx.$$

Let $\omega^*(x) \equiv \omega(x)$ (mod 1), $0 \leq \omega^*(x) < 1$. The last integral is

$$\int_0^1 \chi(\omega^*(x))dx = \text{meas } E\,\{a < \omega^*(x) < b\}.$$

Hence,

$$\text{meas } E\,\{a < \omega^*(x) < b\} = b - a, \tag{2}$$

which proves the lemma.

An alternative necessary and sufficient condition for the uniform distribution modulo 1 of $v_n = \omega(u_n)$ is that

$$\int_0^1 e^{2\pi i h\omega(x)}\, dx = 0 \tag{3}$$

for all integers $h \neq 0$.

For the uniform distribution of $\{v_n\}$ is equivalent to

$$\lim \frac{1}{N}\sum_1^N e^{2\pi i h\omega(u_n)} = \lim \frac{1}{N}\sum_1^N e^{2\pi i h v_n} = 0$$

by Weyl's criterion. But

$$\lim \frac{1}{N}\sum_1^N e^{2\pi i h\omega(u_n)} = \int_0^1 e^{2\pi i h\omega(x)}\, dx.$$

Hence, we have the result, and it can be proved directly without difficulty, considering again $\omega^*(x)$, that (3) is equivalent to (2).

In our case $\{u_m\} = \{m\omega\}$ is uniformly distributed modulo 1, and it is enough to remark that the function $2 \cos 2\pi x$ has a distribution function (mod 1) which

† No confusion can arise from the notation $\omega(x)$ for the distribution function and the *number* ω occurring in the proof of the theorem.

is not linear. This can be shown by direct computation or by remarking that

$$\int_0^1 e^{4\pi i h \cos 2\pi x} = J_0(4\pi h)$$

is not zero for all integers $h \neq 0$.

In the general case (τ not quadratic) if $2k$ is the degree of τ, we have, using the preceding notations,

$$\tau^m + \frac{1}{\tau^m} + \sum_{j=1}^{k-1} \alpha_j^m + \sum_{j=1}^{k-1} \alpha_j^{-m} \equiv 0 \pmod 1$$

or

$$\tau^m + \frac{1}{\tau^m} + \sum_{j=1}^{k-1} 2 \cos 2\pi m\omega_j \equiv 0 \pmod 1$$

and we have to prove that the sequence

$$v_m = 2 \cos 2\pi m\omega_1 + \cdots + 2 \cos 2\pi m\omega_{k-1}$$

is not uniformly distributed modulo 1.

We use here a lemma analogous to the preceding one.

LEMMA. *If the p-dimensional vector* $\{u_n^j\}_{n=1}^\infty$ $(j = 1, 2, \ldots p)$ *is uniformly distributed modulo* 1 in R^p, *the sequence*

$$v_n = \omega(u_n^1) + \omega(u_n^2) + \cdots + \omega(u_n^p)$$

where $\omega(x)$ *is continuous with period* 1 *is uniformly distributed if and only if condition* (2) *or the equivalent condition* (3) *is satisfied.*

PROOF of the lemma. It is convenient here to use the second form of the proof. The condition is

$$\frac{1}{N}\sum_1^N e^{2\pi i h v_n} \to 0 \quad (h \text{ is any integer} \neq 0).$$

But

$$\frac{1}{N}\sum_{n=1}^N e^{2\pi i h[\omega(u_n^1) + \cdots + \omega(u_n^p)]} \to \left\{\int_0^1 e^{2\pi i h\omega(x)}\, dx\right\}^p.$$

Hence the lemma.

Theorem V about τ^m follows from the fact that $\{m\omega_1, m\omega_2, \ldots, m\omega_{k-1}\}$ is uniformly distributed in the unit torus of R^{k-1} owing to the fact that $\omega_1, \ldots, \omega_{k-1}$, and 1 are linearly independent. This completes the proof.

EXERCISE

Show that any number τ of the class T is the quotient θ/θ' of two numbers of the class S belonging to the field of τ. (For this and other remarks, see [13].)

Chapter IV

A CLASS OF SINGULAR FUNCTIONS; BEHAVIOR OF THEIR FOURIER-STIELTJES TRANSFORMS AT INFINITY

1. Introduction

By a *singular function* $f(x)$ we shall mean, in what follows, a singular continuous monotonic function (e.g., nondecreasing), bounded, and whose derivative vanishes for almost all (in the Lebesgue sense) values of the real variable x.

A wide class of singular functions is obtained by constructing, say, in $(0, 2\pi)$ a perfect set of measure zero, and by considering a nondecreasing continuous function $f(x)$, constant in every interval contiguous to the set (but not everywhere).

A very interesting and simple example of perfect sets to be considered is the case of symmetrical perfect sets with constant ratio of dissection. Let ξ be a positive number, strictly less than $\frac{1}{2}$, and divide the fundamental interval, say, $(0, 2\pi)$, into three parts of lengths proportional to ξ, $1-2\xi$, and ξ respectively. Remove the central open interval ("black" interval). Two intervals ("white" intervals) are left on which we perform the same operation. At the kth step we are left with 2^k white intervals, each one of length $2\pi\xi^k$. Denote by E_k the set of points belonging to these 2^k closed white intervals. Their left-hand end points are given by the formula

$$(1) \qquad x = 2\pi[\epsilon_1(1-\xi) + \epsilon_2\xi(1-\xi) + \cdots + \epsilon_k\xi^{k-1}(1-\xi)],$$

where the ϵ_i are 0 or 1. The intersection of all E_k is a perfect set E of measure equal to

$$2\pi \lim_{k\to\infty} (\xi^k 2^k) = 0$$

and whose points are given by the infinite series

$$(2) \qquad x = 2\pi[\epsilon_1(1-\xi) + \epsilon_2\xi(1-\xi) + \cdots + \epsilon_k\xi^{k-1}(1-\xi) + \cdots],$$

where the ϵ_i can take the values 0 or 1. The reader will recognize that the classical Cantor's ternary set is obtained by taking $\xi = \frac{1}{3}$.

We define now, when $x \in E$, a function $f(x)$ given by

$$f(x) = \frac{\epsilon_1}{2} + \frac{\epsilon_2}{2^2} + \cdots + \frac{\epsilon_k}{2^k} + \cdots,$$

when x is given by (2). It is easily seen that at the end points of a black interval (e.g., $\epsilon_1 = 0$, $\epsilon_2 = \epsilon_3 = \cdots = 1$ and $\epsilon_1 = 1$, $\epsilon_2 = \epsilon_3 = \cdots = 0$) $f(x)$ takes the same value. We then define $f(x)$ in this interval as a constant equal to this common value. The function $f(x)$ is now defined for $0 \le x \le 2\pi$ ($f(0) = 0$, $f(2\pi) = 1$),

is continuous, nondecreasing, and obviously singular. We shall call it the "Lebesgue function" associated with the set E.

The Fourier-Stieltjes coefficients of df are given by

$$(3) \qquad c_n = (2\pi)^{-1} \int_0^{2\pi} e^{nix}\, df(x),$$

and, likewise, the Fourier-Stieltjes transform of df is defined by

$$\gamma(u) = (2\pi)^{-1} \int_{-\infty}^{\infty} e^{uix}\, df(x)$$

$$= (2\pi)^{-1} \int_0^{2\pi} e^{uix}\, df(x)$$

for the continuous parameter u, f being defined to be equal to 0 in $(-\infty, 0)$ and to 1 in $(2\pi, \infty)$.

One can easily calculate the Riemann-Stieltjes integral in (3) by remarking that in each "white" interval of the kth step of the dissection f increases by $1/2^k$. The origins of the intervals are given by (1), or, for the sake of brevity, by

$$x = 2\pi[\epsilon_1 r_1 + \cdots + \epsilon_k r_k],$$

with $r_k = \xi^{k-1}(1-\xi)$. Hence an approximate expression of the integral

$$\int_0^{2\pi} e^{nix}\, df$$

is

$$\frac{1}{2^k} \sum e^{2\pi ni(\epsilon_1 r_1 + \cdots + \epsilon_k r_k)},$$

the summation being extended to the 2^k combinations of $\epsilon_j = 0, 1$. This sum equals

$$\frac{1}{2^k} \prod_{s=1}^{k} (1 + e^{2\pi nir_s}) = e^{\pi ni \sum_1^k r_s} \prod_{s=1}^{k} \cos \pi nr_s.$$

Since $\sum_1^\infty r_s = 1$, we have

$$(4) \qquad e^{-\pi ni}\, 2\pi c_n = \prod_{k=1}^{\infty} \cos \pi nr_k = \prod_{k=1}^{\infty} \cos \pi n\xi^{k-1}(1-\xi)$$

and likewise

$$(5) \qquad e^{-\pi ui}\, 2\pi\gamma(u) = \prod_{k=1}^{\infty} \cos \pi u\xi^{k-1}(1-\xi).$$

2. The problem of the behavior at infinity

It is well known in the elementary theory of trigonometric series that if f is absolutely continuous, the Fourier-Stieltjes transform

$$\gamma(u) = (2\pi)^{-1} \int_0^{2\pi} e^{uix}\, df$$

tends to zero as $|u| \to \infty$, because in this case $\gamma(u)$ is nothing but the ordinary Fourier transform of a function of the class L. The situation is quite different if f is continuous, but singular. In this case $\gamma(u)$ need not tend to zero, although there do exist singular functions for which $\gamma(u) \to 0$ ([17], and other examples in this chapter). The same remarks apply to the Fourier-Stieltjes coefficients c_n.

The problem which we shall solve here is the following one. Given a symmetrical perfect set with constant ratio of dissection ξ, which we shall denote by $E(\xi)$, we construct the Lebesgue function f connected with it, and we try to determine for what values of ξ the Fourier-Stieltjes transform (5) (or the Fourier-Stieltjes coefficient (4)) tends or does not tend to zero as $|u|$ (or $|n|$) increases infinitely.

We shall prove first the following general theorem.

THEOREM I. *For any function of bounded variation f the Riemann-Stieltjes integrals*

$$2\pi c_n = \int_0^{2\pi} e^{nix}\, df \quad \textit{and} \quad 2\pi\gamma(u) = \int_0^{2\pi} e^{vix}\, df$$

tend or do not tend to zero together when $|n|$ or $|u|$ tends to ∞.

Since it is obvious that $\gamma(u) = o(1)$ implies $c_n = o(1)$, we have only to prove the converse proposition. We shall base this proof on the following lemma, interesting in itself.

LEMMA. *Let $f(x)$ be a function of bounded variation such that, as $|n| \to \infty$,*

$$\int_0^{2\pi} e^{nix}\, df \to 0. \tag{6}$$

Let $B(x)$ be any function such that the Lebesgue-Stieltjes integral

$$\int_0^{2\pi} B(x)df(x)$$

has a meaning. Then the integral

$$\int_0^{2\pi} e^{nix} B(x) df$$

tends also to zero for $|n| = \infty$.

PROOF of the lemma. We observe first that by the properties of the Lebesgue-Stieltjes integral, there exists a step function $T(x)$ such that

$$\int_0^{2\pi} |B(x) - T(x)|\, df < \epsilon, \tag{7}$$

ϵ being arbitrarily small. Secondly, by a well-known theorem of Wiener [17], the condition (6) implies that f is continuous. Hence, in (7) we can replace $T(x)$ by a trigonometric polynomial $P(x)$. But (6) implies

$$\int_0^{2\pi} e^{nix} P(x) df \to 0.$$

Hence, ϵ being arbitrarily small in (7), we have

$$\int_0^{2\pi} B(x) e^{nix}\, df \to 0$$

as stated in the lemma.

PROOF of Theorem I. Suppose that

$$c_n \to 0 \text{ as } |n| \to \infty.$$

If $\gamma(u)$ does not tend to zero as $|u| \to \infty$, we can find a sequence

$$\{u_k\}_{k=1}^{\infty} \text{ with } |u_k| \to \infty$$

such that

$$\left| \int_0^{2\pi} e^{u_k ix}\, df \right| \geq \delta > 0.$$

Let

$$u_k = n_k + \alpha_k,$$

n_k being an integer and $0 \leq \alpha_k < 1$. By extracting, if necessary, a subsequence from $\{u_k\}$, we can suppose that α_k tends to a limit α. We would then have

$$\left| \int_0^{2\pi} e^{n_k ix} e^{\alpha ix}\, df \right| \geq \frac{\delta}{2} > 0,$$

which is contrary to the lemma, since $c_n \to 0$ and $e^{\alpha ix}$ is continuous.

It follows now that in order to study the behavior of c_n or $\gamma(u)$, it is enough to study

$$\Gamma(u) = \prod_{k=1}^{\infty} \cos \pi u \xi^k \tag{8}$$

when $u \to \infty$.

THEOREM II. *The infinite product $\Gamma(u)$ tends to zero as $u \to \infty$ if and only if $1/\xi$ is not a number of the class S (as defined in Chapter I). We suppose here $\xi \neq \frac{1}{2}$.*

Remark. We have seen that the expressions (4) and (5) represent respectively the Fourier-Stieltjes coefficient and the Fourier-Stieltjes transform of the Lebesgue function constructed on the set $E(\xi)$ if $0 < \xi < \frac{1}{2}$. Nevertheless, it is easy to see that in order that the infinite products (4), (5), (8) have a meaning, it is enough to suppose that $0 < \xi < 1$. For example, $\Gamma(u)$ still represents a Fourier-Stieltjes transform if only $0 < \xi < 1$, namely the transform of the monotonic function which is the convolution of an infinity of discontinuous measures (mass $\frac{1}{2}$ at each of the two points $\pi\xi^k, -\pi\xi^k$).

Our theorem being true in the general case $0 < \xi < 1$, we shall only assume this condition to prove it.

PROOF of Theorem II. If $\Gamma(u) \neq o(1)$ for $u = \infty$, we can find an infinite increasing sequence of numbers u_s such that

$$|\Gamma(u_s)| \geq \delta > 0.$$

Writing $1/\xi = \theta \quad (\theta > 1)$, we can write

$$u_s = \lambda_s \theta^{m_s},$$

where the m_s are natural integers increasing to ∞, and $1 \leq \lambda_s < \theta$.

By extracting, if necessary, a subsequence from $\{u_s\}$, we can suppose that $\lambda_s \to \lambda$ $(1 \leq \lambda \leq \theta)$. We write

$$|\Gamma(u_s)| \leq \cos \pi\lambda_s \cos \pi\lambda_s\theta \cdots \cos \pi\lambda_s\theta^{m_s},$$

whence

$$\prod_{q=0}^{m_s} [1 - \sin^2 \pi\lambda_s\theta^q] \geq \delta^2,$$

and, since $1 + x < e^x$,

$$e^{-\sum_{q=0}^{m_s} \sin^2 \pi\lambda_s\theta^q} \geq \delta^2;$$

that is to say,

$$\sum_{q=0}^{m_s} \sin^2 \pi\lambda_s\theta^q \leq \log(1/\delta^2).$$

Choosing any $r > s$, we have

$$\sum_{q=0}^{m_s} \sin^2 \pi\lambda_r\theta^q \leq \sum_{q=0}^{m_r} \sin^2 \pi\lambda_r\theta^q \leq \log(1/\delta^2).$$

Keeping now s fixed and letting $r \to \infty$, we have

$$\sum_{q=0}^{m_s} \sin^2 \pi\lambda\theta^q \leq \log(1/\delta^2),$$

and, since s is arbitrarily large,

$$\sum_{q=0}^{\infty} \sin^2 \pi\lambda\theta^q \leq \log(1/\delta^2),$$

which, according to the results of Chapter I, shows that $\theta = \xi^{-1}$ belongs to the class S.

We have thus shown that $\Gamma(u) \neq o(1)$ implies that $\theta \in S$.

Conversely, if $\theta \in S$ and $\theta \neq 2$, then $\Gamma(u)$ does not tend to zero. (Remark that if $\xi = \frac{1}{2}$, the Fourier-Stieltjes coefficient c_n of (4) is zero for all $n \neq 0$ and then $f(x) = x$ $(0 \leq x \leq 2\pi)$.)

Supposing now $\theta = \xi^{-1} \neq 2$, we have

$$\Gamma(\theta^k) = |\cos \pi\theta \cos \pi\theta^2 \cdots \cos \pi\theta^k| \cdot \left|\cos \frac{\pi}{\theta} \cos \frac{\pi}{\theta^2} \cdots \cos \frac{\pi}{\theta^k} \cdots\right|.$$

Since $\theta \in S$, we have $\sum \sin^2 \pi\theta^n < \infty$. Hence, the infinite product

$$\prod_{m=1}^{\infty} \cos^2 \pi\theta^m$$

converges to a number $A \neq 0$ (except if $\theta^q = h + \frac{1}{2}$, h being a natural integer, but this is incompatible with the fact that $\theta \in S$). Hence,

$$|\Gamma(\theta^k)| \geq \sqrt{A} \left|\cos \frac{\pi}{\theta} \cos \frac{\pi}{\theta^2} \cdots\right|$$

and the last product converges to a number $B > 0$, since $\theta \neq 2$ ($\theta^q = 2$ is impossible for $q > 1$ if $\theta \in S$). Hence,

$$|\Gamma(\theta^k)| \geq B\sqrt{A},$$

which completes the proof of Theorem II.

Chapter V

THE UNIQUENESS OF THE EXPANSION IN TRIGONOMETRIC SERIES; GENERAL PRINCIPLES

1. Fundamental definitions and results

Let us consider a trigonometric series

$$(S)\qquad \sum_{0}^{\infty} (a_n \cos nx + b_n \sin nx),$$

where the variable x is real. The classical theory of Cantor shows [17] that if this series converges everywhere to zero, it vanishes identically.

Cantor himself has generalized this result by proving that if (S) converges to zero for all values of x except for an exceptional set E containing a *finite* number of points x, then the conclusion is the same one, i.e.,

$$a_n = 0,\ b_n = 0 \text{ for all } n.$$

Cantor proved also that the conclusion is still valid if E is infinite, provided that the derived set E' is finite, or even provided that any one of the derived sets of E (of *finite* or *transfinite* order) is empty, in other words if E is a denumerable set which is *reducible* [17].

The results of Cantor go back to the year 1870. Not until 1908 was it proved by W. H. Young that the result of Cantor can be extended to the case where E is *any denumerable set* (even if it is not reducible).

The preceding results lead to the following definition.

DEFINITION. *Let E be a set of points x in $(0, 2\pi)$. Then E is a* set of uniqueness *(set U) if no trigonometric series exists (except vanishing identically) converging to zero everywhere, except, perhaps, for $x \in E$. Otherwise E will be called* set of multiplicity *(set M).*

We have just seen that any denumerable set is a set U. On the other hand, as we shall easily show (page 44):

If E is of positive measure, E is a set M.

It is, therefore, natural to try to characterize the sets of measure zero by classifying them in "sets U" and "sets M." We shall give a partial solution of this problem in the next two chapters, but we must begin here by recalling certain classical theorems of the theory of trigonometric series of Riemann [17].

DEFINITIONS. (*a*) *Given any function $G(x)$ of the real variable x, we shall write*

$$\frac{1}{h^2}\Delta^2 G(x, h) = \frac{G(x+h) + G(x-h) - 2G(x)}{h^2},$$

and, if this expression tends for a given fixed x to a limit λ, as $h \to 0$, we shall say that $G(x)$ has, at the point x, a second generalized derivative *equal to λ.*

(*b*) *If, at a given point x, the expression*

$$\frac{1}{h}\Delta^2 G(x, h) = \frac{G(x+h) + G(x-h) - 2G(x)}{h}$$

tends to zero as $h \to 0$, we shall say that $G(x)$ is smooth *at the point x.*

THEOREM I (Cantor-Lebesgue). *If the trigonometric series*

$$(1)\qquad \tfrac{1}{2}a_0 + \sum_{1}^{\infty} (a_n \cos nx + b_n \sin nx)$$

converges in a set of positive measure, its coefficients a_n and b_n tend to zero.

DEFINITION. *If we integrate the series* (1) *formally twice, assuming that $a_n \to 0$, $b_n \to 0$, we obtain the continuous function*

$$(2)\qquad F(x) = \frac{1}{4} a_0 x^2 - \sum_{1}^{\infty} \frac{(a_n \cos nx + b_n \sin nx)}{n^2},$$

the last series being uniformly convergent. If, at a given point x, $F(x)$ has a second generalized derivative equal to s, we shall say that the series (1) *is* summable-Riemann (*or* summable-*R*) *and that its* sum is *s*.

THEOREM II. *If the series* (1) $(a_n, b_n \to 0)$ *converges to s at the point x, it is also summable-R to s at this point.*

THEOREM IIA. *If the series* (1) *with coefficients tending to zero is summable-R to zero for all the points of an interval, it converges to zero in this interval (consequence of the principle of "localization").*

THEOREM III. *The function $F(x)$ (always assuming $a_n \to 0$, $b_n \to 0$) is smooth at every point x.*

THEOREM IV. *Let $G(x)$ be continuous in an interval (a, b). If the generalized second derivative exists and is zero in (a, b), $G(x)$ is linear in (a, b).*

THEOREM V. *Theorem* IV *remains valid if one supposes that the generalized second derivative exists and is zero except at the points of a denumerable set E, provided that at these points G is smooth.*

Historically, this last theorem was proved first by Cantor (*a*) when E is finite, (*b*) when E is reducible, i.e., has a derived set of finite or transfinite order which is empty. It was extended much later by Young to the general case where E is supposed only to be denumerable.

From Theorem V we deduce finally:

THEOREM VI. *If the series* (1) *converges to* 0 *at all points of* $(0, 2\pi)$ *except perhaps when* x *belongs to a denumerable set* E, *the series vanishes identically.* In other words every denumerable set is a set U, which is the above stated result.

PROOF. This follows immediately as a consequence of Theorems II, III, and V. For the application of these theorems shows that the function $F(x)$ of (2) is linear. Hence, for all x,

$$\sum_1^{\infty} \frac{a_n \cos nx + b_n \sin nx}{n^2} = \frac{1}{4} a_0 x^2 - Ax - B$$

and the periodicity of the series implies $a_0 = A = 0$; next, the series being uniformly convergent, $B = 0$ and $a_n = b_n = 0$ for all n.

We shall now prove the theorem on page 42:

THEOREM. *Every set of positive measure is a set* M.

PROOF. Let $E \subset (0, 2\pi)$ and $|E| > 0$. It will be enough to prove that there exists a trigonometric series (not vanishing identically) and converging to zero in the complementary set of E, that is, CE.

Let P be perfect such that $P \subset E$, and $|P| > 0$. Let $\chi(x)$ be its characteristic function. In an interval Δ contiguous to P, one has $\chi(x) = 0$; hence the Fourier series of $\chi(x)$,

$$\frac{\alpha_0}{2} + \sum_0^{\infty} (\alpha_n \cos nx + \beta_n \sin nx) \sim \chi(x),$$

converges to zero in Δ. Hence it converges to zero in CP, and also in $CE \subset CP$. But this series does not vanish identically, since

$$\alpha_0 = \frac{1}{\pi} \int_0^{2\pi} \chi(x)dx = \frac{|P|}{\pi} > 0,$$

which proves the theorem.

2. Sets of multiplicity

The problem of the classification of sets of measure zero into sets U and sets M is far from solved. But it is completely solved for certain families of perfect sets, as we shall show in the next two chapters.

We shall need the following theorem.

THEOREM. *A necessary and sufficient condition for a closed set E to be a set of multiplicity is that there should exist a trigonometric series*

$$\sum_{-\infty}^{\infty} c_n e^{inx}$$

(not vanishing identically) with coefficients $c_n = o\left(\frac{1}{n}\right)$† *and representing a constant*‡ *in each interval contiguous to* E.

PROOF. *The condition is necessary.* Let E, closed, be of the type M, and consider a nonvanishing trigonometric series

$$(S) \qquad \sum_{-\infty}^{\infty} \gamma_n e^{nix},$$

converging to zero in every interval contiguous to E.

We show first that we can then construct a series

$$(S') \qquad \sum_{-\infty}^{\infty} \gamma_n e^{nix},$$

but with $\gamma_0 = 0$, having the same property. For (S) has at least one nonvanishing coefficient, say, γ_k. Let $l \neq k$. The series

$$(S') = \gamma_k e^{-ilx}(S) - \gamma_l e^{-ikx}(S)$$

has a vanishing constant term, and converges to zero, like (S), for all x belonging to CE, the complementary set of E. Let E_1 be the set where (S) does not converge to zero. (S') cannot vanish identically, for the only points of E_1 (which is necessarily infinite) where (S') converges to zero are the points (*finite* in number) where

$$\gamma_k e^{-ilx} - \gamma_l e^{-ikx} = 0.$$

Let us then consider the series

$$\sum_{-\infty}^{\infty} \gamma_n e^{nix} \quad (\gamma_0 = 0),$$

converging to zero in CE. The series integrated twice,

$$\sum_{-\infty}^{-1} + \sum_1^{\infty} \frac{\gamma_n}{-n^2} e^{inx},$$

represents by Riemann theorems (II and IV on page 43) a linear function in each interval of CE. But this series is the integral of the Fourier series

$$\sum_{-\infty}^{-1} + \sum_1^{\infty} \frac{\gamma_n}{ni} e^{inx},$$

which must hence represent a constant in each interval of CE, and it is now enough to remark that

$$c_n = \frac{\gamma_n}{ni} = o\left(\frac{1}{n}\right),$$

since necessarily $\gamma_n \to 0$ (Th. I).

† The series is a Fourier series by the Riesz-Fischer theorem.

‡ Hence, by the elementary theory, converging to this constant.

The condition is sufficient. Suppose that the series

$$\sum_{-\infty}^{\infty} c_n e^{inx}$$

(not vanishing identically) with $c_n = o\left(\frac{1}{n}\right)$ represents a constant in each interval of CE. One can write

$$c_n = \frac{\gamma_n}{ni} \text{ with } \gamma_n \to 0.$$

It follows that the integrated series

$$c_0 x - \sum_{|n| \geq 1} \frac{\gamma_n}{n^2} e^{inx}$$

represents a linear function in each interval of CE. Hence, the series

$$\sum \gamma_n e^{inx}$$

is summable-R to zero in each interval of CE, and thus, by Theorem IIA, converges to zero in each interval contiguous to E, the set E being, therefore, a set of multiplicity.

Remark. If the series

$$\sum_{-\infty}^{\infty} c_n e^{inx}$$

of the theorem represents a function of bounded variation, the series

$$\sum \gamma_n e^{inx}$$

converging to zero in CE is a Fourier-Stieltjes series (in the usual terminology, the Fourier-Stieltjes series of a "measure" whose "support" is E). In this case, we say that E is a set of multiplicity in the restricted sense.

To construct a set of multiplicity in the restricted sense, it is enough to construct a perfect set, support of a measure

$$d\mu \sim \sum_{-\infty}^{\infty} \gamma_n e^{inx},$$

whose Fourier-Stieltjes coefficients,

$$\gamma_n = \frac{1}{2\pi} \int_0^{2\pi} e^{-inx}\, d\mu(x),$$

tend to 0 for $|n| \to \infty$.

Consequence. The results of Chapter IV show that every symmetrical perfect set $E(\xi)$ with constant ratio ξ, such that $1/\xi$ is *not* a number of the class S, is a set of multiplicity. In view of the preceding remark, it is enough to take for μ the Lebesgue function constructed on the set.

3. Construction of sets of uniqueness

We have just seen that in order to show that a closed set E is a set of uniqueness, we must prove that there is no series

$$\sum_{-\infty}^{\infty} c_n e^{nix}$$

(not vanishing identically) with coefficients $c_n = o\left(\frac{1}{n}\right)$ representing a constant in each interval of CE.

We were able to prove only that a symmetrical perfect set $E(\xi)$ is a set M if ξ^{-1} does not belong to the class S, but we cannot, at this stage, prove that if $\xi^{-1} \in S$, then $E(\xi)$ is a set U. This is because we only know that if $\xi^{-1} \in S$, the Fourier-Stieltjes coefficients of the Lebesgue measure constructed on the set do not tend to zero. But we do not know (*a*) whether this is true for *every* measure whose support is $E(\xi)$ or (*b*) whether there does not exist a series

$$\sum_{-\infty}^{\infty} c_n e^{nix}$$

with $c_n = o\left(\frac{1}{n}\right)$ representing a constant in each interval of CE, and which is *not* a function of bounded variation (i.e., the derived series $\sum \gamma_n e^{nix}$ is *not* a Fourier-Stieltjes series).

A negative proof of this kind would be rather difficult to establish. In general, to prove that a set E is a set of the type U, one tries to prove that it belongs to a family of sets of which one knows, by certain properties of theirs, that they are U sets.

In this connection, we shall make use of the following theorem.

THEOREM I. *Let E be a closed set such that there exists an infinite sequence of functions $\{\lambda_k(x)\}_1^\infty$ with the following properties:*

1. $\lambda_k(x) = 0$ for all k when $x \in E$.
2. *The Fourier series of each*

$$\lambda_k(x) = \sum_n \gamma_n^{(k)} e^{inx}$$

is absolutely convergent, and we have

$$\sum_n |\gamma_n^{(k)}| < A, \text{ constant independent of } k.$$

3. *We have*

$$\lim_{k\to\infty} \gamma_n^{(k)} = 0 \quad \text{for} \quad n \neq 0,$$

$$\lim_{k\to\infty} \gamma_0^{(k)} = l \neq 0.$$

4. *The derivative $\lambda_k'(x)$ exists for each x and each k, and is bounded (the bound may depend on k).*

Under these conditions, E is a set of uniqueness.

We shall first prove the following lemma.

LEMMA. *Let E be a closed set, $\lambda(x)$ a function vanishing for $x \in E$ and having an absolutely convergent Fourier series $\sum \gamma_n e^{nix}$, and a bounded derivative $\lambda'(x)$. Let $\sum c_n e^{nix}$ be a trigonometric series converging to zero in every interval of the complementary set CE. Under these conditions we have*

$$\sum \bar{\gamma}_n c_n = 0.$$

(The series is obviously convergent, since $\sum |\gamma_n| < \infty$ and $c_n \to 0$.)

PROOF. Let Δ be an interval contiguous to E. The series

$$c_0 \frac{x^2}{2} - \sum \frac{c_n}{n^2} e^{nix}$$

converges to a linear function in Δ. Hence, the Fourier series

$$f \sim \sum{}^* \frac{c_n e^{nix}}{ni},$$

where the star means that there is no constant term, represents in Δ a function $-c_0 x + a$, the constant $a = a(\Delta)$ depending on Δ. Parseval's formula is applicable [17] in our hypothesis to the functions $f(x)$ and

$$\lambda'(x) \sim \sum \gamma_n n i e^{nix}$$

and gives

$$\frac{1}{2\pi} \int_0^{2\pi} \overline{\lambda'(x)} f(x) dx = - \sum_{|n| \geq 1} \bar{\gamma}_n c_n.$$

The integral is equal to

$$(2\pi)^{-1} \sum_\Delta \int_\Delta \overline{\lambda'(x)} \, (-c_0 x + a) dx,$$

since λ and λ' are zero for $x \in E$. (Note that if E is closed, but not perfect, its isolated points are denumerable.) Integrating by parts,

$$\int_\Delta \overline{\lambda'(x)} (-c_0 x + a) dx = [(-c_0 x + a)\bar{\lambda}]_\Delta + c_0 \int_\Delta \overline{\lambda(x)} dx,$$

and comparing the three last relations, we have

$$- \sum_{|n| \geq 1} \bar{\gamma}_n c_n = c_0 (2\pi)^{-1} \sum_\Delta \int \overline{\lambda(x)} dx$$

$$= c_0 (2\pi)^{-1} \int_0^{2\pi} \overline{\lambda(x)} dx = c_0 \bar{\gamma}_0$$

or, as stated,

$$\sum \bar{\gamma}_n c_n = 0.$$

Remark. The hypothesis that $\lambda'(x)$ is bounded could be relaxed (which would lead also to a relaxation of the hypothesis (4) of the theorem), but this is of no interest for our applications. It should be observed, however, that *some* hypothesis on $\lambda(x)$ is necessary. We know, in fact, since the obtention of recent results on spectral synthesis [6], [8], that the lemma would not be true if we assume only that $\lambda(x) = 0$ for $x \in E$, and that its Fourier series is absolutely convergent

PROOF of Theorem I. Suppose that E is not a set of uniqueness. Hence, suppose the existence of

$$\sum c_n e^{nix}$$

(not identically 0) converging to 0 in each interval of CE. The lemma would then give

$$\sum_n \bar{\gamma}_n^{(k)} c_n = 0 \tag{3}$$

for all k.

Since $c_n \to 0$ for $n = \infty$ (by general Theorem I on page 43), the hypothesis (2) gives

$$\Big| \sum_{|n| \geq N} \bar{\gamma}_n^{(k)} c_n \Big| < A \cdot \max_{|n| \geq N} |c_n| < A\epsilon,$$

ϵ being arbitrarily small for N large enough. Having fixed N, we have

$$\Big| \sum_{1 \leq |n| < N} \bar{\gamma}_n^{(k)} c_n \Big| < \epsilon$$

for k large enough, by the hypothesis (3) of the theorem.

Hence the first member of (3) differs from $c_0 \bar{l}$ by a quantity arbitrarily small, for k large enough. This proves that $c_0 = 0$.

Multiplying the series

$$\sum c_n e^{nix}$$

by e^{-kix}, we find its constant term to be c_k. Thus the argument gives that $c_k = 0$ for all k, that the series $\sum c_n e^{nix}$ is identically 0, and that E is a set of the type U.

First application: Sets of the type H. A linear set $E \subset (0, 2\pi)$ is said to be "of the type H" if there exists an interval (α, β) contained in $(0, 2\pi)$ and an infinite sequence of integers $\{n_k\}_1^\infty$ such that, for whatever $x \in E$ none of the points of abscissa $n_k x$ (reduced modulo 2π) belongs to (α, β).

For example, the points of Cantor's ternary set constructed on $(0, 2\pi)$:

$$x = 2\pi \left[\frac{\epsilon_1}{3} + \frac{\epsilon_2}{3^2} + \cdots + \frac{\epsilon_k}{3^k} + \cdots \right]$$

where ϵ_j is 0 or 2, form a set of the type H, since the points $3^k x \pmod{2\pi}$ never belong to the middle third of $(0, 2\pi)$. The situation is the same for every symmetrical perfect set $E(\xi)$ with constant ratio ξ, if $1/\xi$ is a rational integer.

THEOREM II. *Every closed set of the type H (and thus also every set of the type H †) is a set U.*

PROOF. Let us fix an $\epsilon > 0$, arbitrarily small and denote by $\lambda(x)$ a function vanishing in $(0, \alpha)$ and in $(\beta, 2\pi)$, equal to 1 in $(\alpha + \epsilon, \beta - \epsilon)$ and having a bounded derivative $\lambda'(x)$, so that its Fourier series is absolutely convergent. Write

$$\lambda(x) = \sum_m \gamma_m e^{mix}$$

and

$$\lambda_k(x) = \lambda(n_k x) = \sum_m \gamma_m e^{mn_k ix}.$$

The sequence of functions $\{\lambda_k(x)\}$ satisfy the conditions (1), (2), (3), (4) of Theorem I. In particular, $\lambda(n_k x)$ is zero for all $x \in E$ and all k, and since

$$\gamma_n^{(k)} = \gamma_m$$

if and only if $n = mn_k$ and $\gamma_n^{(k)} = 0$ if $n_k \not| n$, we see that the conditions (3) are satisfied, with

$$I = \gamma_0 = \frac{1}{2\pi} \int_0^{2\pi} \lambda(x)dx = (2\pi)^{-1}(\beta - \alpha - 2\epsilon),$$

which is positive if ϵ has been chosen small enough.

Second application. Sets of the type $H^{(n)}$. The sets of the type H have been generalized by Piatecki-Shapiro, who described as follows the sets which he calls "of the type $H^{(n)}$."

DEFINITION. *Consider, in the n-dimensional Euclidean space R^n, an infinite family of vectors $\{V_k\}$ with rational integral coordinates*

$$V_k = \{p_k^{(1)}, p_k^{(2)}, \ldots, p_k^{(n)}\} \quad (k = 1, 2, \ldots).$$

This family will be called normal, *if, given n fixed arbitrary integers $a_1, a_2, \ldots, a_n$ not all zero, we have*

$$| a_1 p_k^{(1)} + a_2 p_k^{(2)} + \cdots + a_n p_k^{(n)} | \to \infty$$

as $k \to \infty$.

Let Δ be a domain in the n-dimensional torus

$$0 \leq x_j < 2\pi \quad (j = 1, 2, \ldots, n).$$

A set E will be said to belong to the type $H^{(n)}$ if there exists a domain Δ and a normal family of vectors V_k such that for all $x \in E$ and all k, the point with coordinates

$$p_k^{(1)}x, p_k^{(2)}x, \ldots, p_k^{(n)}x,$$

all reduced modulo 2π, never belongs to Δ.

† If E is of the type H, so is its closure, and a subset of a U-set is also a U-set.

THEOREM III. *Every set E of the type $H^{(n)}$ is a set of uniqueness.*

PROOF. We can again suppose that E is closed, and we shall take $n = 2$, the two-dimensional case being typical. Suppose that the family of vectors

$$V_k = (p_k, q_k)$$

is normal. We can assume that Δ consists of the points (x_1, x_2) such that

$$\alpha_1 < x_1 < \beta_1,$$
$$\alpha_2 < x_2 < \beta_2,$$

the intervals (α_1, β_1) and (α_2, β_2) being contained in $(0, 2\pi)$.

We shall denote by $\lambda(x)$ and $\mu(x)$ respectively two functions constructed with respect to the intervals (α_1, β_1) and (α_2, β_2) as was, in the case of sets H, the function $\lambda(x)$ with respect to (α, β). Under these conditions, the functions

$$\lambda(p_k x)\mu(q_k x) \quad (k = 1, 2, \ldots)$$

are equal to zero for all k and all $x \in E$. This sequence of functions will play the role of the sequence denoted by $\lambda_k(x)$ in Theorem I. Thus, the condition (1) of that theorem is satisfied.

Write

$$\lambda(x) = \sum \gamma_m e^{imx}, \quad \mu(x) = \sum \delta_m e^{imx}.$$

The Fourier series of $\lambda(p_k x)\mu(q_k x)$ is absolutely convergent, and, writing

$$\lambda(p_k x)\mu(q_k x) = \sum c_n^{(k)} e^{inx},$$

we have

$$\sum c_n^{(k)} e^{inx} = \sum \gamma_m \delta_{m'} e^{i(mp_k + m'q_k)x}$$

and

$$\sum | c_n^{(k)} | < (\sum | \gamma_n |)(\sum | \delta_n |) < A.$$

This proves that condition (2) is also satisfied.

Condition (4) is satisfied if we have chosen $\lambda(x)$ and $\mu(x)$ possessing bounded derivatives.

Finally, for condition (3) we note that

$$c_n^{(k)} = \sum_{n = mp_k + m'q_k} \gamma_m \delta_{m'}. \tag{4}$$

Suppose first $n = 0$. Then

$$c_0^{(k)} = \sum_{mp_k + m'q_k = 0} \gamma_m \delta_{m'}$$
$$= \gamma_0 \delta_0 + \sum^*_{mp_k + m'q_k = 0} \gamma_m \delta_{m'} = \gamma_0 \delta_0 + T$$

the star meaning that $| m | + | m' | \neq 0$. We shall prove that T tends to zero for $k \to \infty$. Write $T = T_1 + T_2$, where T_1 is extended to the indices $| m | \leq N$,

$|m'| \leq N$. Since the family of vectors $\{V_k\}$ is normal, if $|m|+|m'| \neq 0$, $mp_k + m'q_k$ cannot be zero if k is large enough, and if m and m' are chosen among the finite number of integers such that $|m| \leq N$, $|m'| \leq N$. On the other hand, in T_2 either $|m| > N_1$ or $|m'| > N$ and thus

$$|T_2| < \Big(\sum_{|m|>N} \gamma_m\Big)\Big(\sum_{-\infty}^{\infty} |\delta_{m'}|\Big) + \Big(\sum_{-\infty}^{\infty} |\gamma_m|\Big)\Big(\sum_{|m'|>N} |\delta_{m'}|\Big)$$

is arbitrarily small for N large enough. Choosing first N, and then k, we see that

$$c_0^{(k)} \to \gamma_0\delta_0$$

as $k \to \infty$, and since $\gamma_0\delta_0 \neq 0$, the second part of condition (3) is satisfied.

If now $n \neq 0$, the second member of (4) does not contain the term where $m = 0$, $m' = 0$. The same argument leads then to

$$c_n^{(k)} \to 0 \quad \text{for} \quad k = \infty, n \neq 0.$$

This concludes the proof that all conditions of the general theorem are satisfied and hence that the set E is a set of uniqueness.

In the following two chapters we shall apply the preceding theorems to special sets: symmetrical perfect sets with constant ratio of dissection, and "homogeneous sets."

Chapter VI

SYMMETRICAL PERFECT SETS WITH CONSTANT RATIO OF DISSECTION; THEIR CLASSIFICATION INTO *M*-SETS AND *U*-SETS

In this chapter and in the following one we shall make use of the fundamental theorem of Minkowski on linear forms. For the proof we refer the reader to the classical literature. (See, e.g., [5].)

MINKOWSKI'S THEOREM. *Consider n linear forms of n variables*

$$\lambda_p(x) = \sum_{q=1}^{n} a_q^p x_q \quad (p = 1, 2, \ldots, n)$$

where we suppose first the coefficients a_q^p *to be real. We assume that the determinant D of the forms is not zero. If the positive numbers* $\delta_1, \delta_2, \ldots, \delta_n$ *are such that*

$$\delta_1\delta_2 \cdots \delta_n \geq |D|,$$

there exists a point x with rational integral coordinates $(x_1, x_2, \ldots, x_n)$ *not all zero such that*

$$|\lambda_p(x)| \leq \delta_p \quad (p = 1, 2, \ldots, n).$$

The theorem remains valid if the coefficients a_q^p are complex numbers provided:

1. the complex forms figure in conjugate pairs
2. the δ_p corresponding to conjugate forms are equal.

THEOREM. *Let* $E(\xi)$ *be a symmetrical perfect set in* $(0, 2\pi)$ *with constant ratio of dissection* ξ. *A necessary and sufficient condition for* $E(\xi)$ *to be a set of uniqueness is that* $1/\xi$ *be a number of the class S* [14].

PROOF. The necessity of the condition follows from what has been said in the preceding chapter. We have only to prove here the sufficiency: If ξ^{-1} belongs to the class S, $E(\xi)$ is a U-set.

We simplify the formulas a little by constructing the set $E(\xi)$ on [0, 1]. We write $\theta = 1/\xi$ and suppose, naturally, that $\theta > 2$. We assume that θ is an algebraic integer of the class S and denote by n its degree. We propose to show that $E(\xi)$ is of the type $H^{(n)}$, and hence a set of uniqueness.

The points of $E(\xi)$ are given by

$$x = \epsilon_1 r_1 + \epsilon_2 r_2 + \cdots + \epsilon_j r_j + \cdots$$

where $r_j = \xi^{j-1}(1-\xi) = \dfrac{1}{\theta^{j-1}}\Big(1 - \dfrac{1}{\theta}\Big) = \dfrac{\theta - 1}{\theta^j}$ and the ϵ_j are 0 or 1.

Thus,

$$x = (\theta - 1)\left[\frac{\epsilon_1}{\theta} + \frac{\epsilon_2}{\theta^2} + \cdots + \frac{\epsilon_j}{\theta^j} + \cdots\right].$$

By λ we denote a positive algebraic integer of the field of θ, which we shall determine later. We denote by $\alpha_1, \alpha_2, \ldots, \alpha_{n-1}$ the conjugates of θ and by $\mu_1, \mu_2, \ldots, \mu_{n-1}$ the conjugates of λ.

We have, x being a fixed point in $E(\xi)$ and m a rational integer ≥ 0,

$$\lambda\theta^m x = \lambda(\theta - 1)\left(\frac{\epsilon_{m+1}}{\theta} + \cdots\right) + R \tag{1}$$

$$R = \lambda(\theta - 1)(\epsilon_1\theta^{m-1} + \epsilon_2\theta^{m-2} + \cdots + \epsilon_m).$$

Observe that, for any natural integer $p \geq 0$,

$$\lambda(\theta - 1)\theta^p + \sum_{i=1}^{n-1} \mu_i(\alpha_i - 1)\alpha_i^p \equiv 0 \pmod 1.$$

That is to say

$$\lambda(\theta - 1)\theta^p \equiv -\sum_{i=1}^{n-1} \mu_i(\alpha_i - 1)\alpha_i^p.$$

Hence, remembering that the $|\alpha_i|$ are < 1,

$$|R| < 2\sum_{i=1}^{n-1} |\mu_i| \sum_{m=0}^{\infty} |\alpha_i|^m = 2\sum_{i=1}^{n-1} \frac{|\mu_i|}{1 - |\alpha_i|} \pmod 1. \tag{2}$$

Let us now write (1), after breaking the sum in parenthesis into two parts, as

$$\lambda\theta^m x = \lambda(\theta - 1)\left(\frac{\epsilon_{m+1}}{\theta} + \cdots + \frac{\epsilon_{m+N}}{\theta^N}\right) + \lambda(\theta - 1)\left(\frac{\epsilon_{m+N+1}}{\theta^{N+1}} + \cdots\right) + R \tag{3}$$

$$= P + Q + R.$$

We have

$$|Q| < \lambda(\theta - 1)\frac{\theta^{-N-1}}{1 - \theta^{-1}} = \frac{\lambda}{\theta^N}. \tag{4}$$

We now choose λ of the form

$$\lambda = x_1 + x_2\theta + \cdots + x_n\theta^{n-1},$$

where the x_j are rational integers. Then, obviously,

$$\mu_i = x_1 + x_2\alpha_i + \cdots + x_n\alpha_i^{n-1} \quad (i = 1, 2, \ldots, n - 1).$$

By Minkowski's theorem, we determine the rational integers, such that

$$\frac{\lambda}{\theta^n} \leq \frac{\sigma}{n2^{N/n}}; \quad \frac{2|\mu_i|}{1 - |\alpha_i|} \leq \frac{\sigma}{n2^{N/n}} \quad (i = 1, 2, \ldots, n - 1), \tag{5}$$

where σ will be determined in a moment. The determinant of the forms

$$\frac{\lambda}{\theta^N} \quad \text{and} \quad \frac{2\mu_i}{1 - |\alpha_i|} \quad (i = 1, 2, \ldots, n = 1)$$

can be written as

$$\frac{\Delta}{\theta^N},$$

where Δ is a nonvanishing determinant depending only on θ (and independent of N), say, $\Delta = \Delta(\theta)$. Minkowski's theorem can be applied, provided

$$\frac{\sigma^n}{n^n 2^N} > \frac{\Delta}{\theta^N},$$

and, after choosing σ, we can always determine N so that this condition be fulfilled, since $\theta/2 > 1$.

By (2), (3), (4), and (5), we shall then obtain for an arbitrary fixed $x \in E(\xi)$ and any arbitrary natural integer $m \geq 0$

$$|\lambda\theta^m x - P| \leq \frac{\sigma}{2^{N/n}} \pmod 1,$$

that is to say

$$\left|\lambda\theta^m x - \lambda(\theta - 1)\left(\frac{\epsilon_{m+1}}{\theta} + \cdots + \frac{\epsilon_{m+N}}{\theta^N}\right)\right| \leq \frac{\sigma}{2^{N/n}} \pmod 1. \tag{6}$$

Denote now by g_m the fractional part of P (depending on m), and denote by O_k, k an arbitrary natural integer, the point having the coordinates $g_{k+1}, g_{k+2}, \ldots, g_{k+n}$.

The *number* of points O_k depends evidently on k, n, and the choice of the ϵ's; but we shall prove that there are at most 2^{N+n-1} distinct points O_k. In fact, observe that g_{k+1} can take 2^N values (according to the choice of the ϵ's). But, once g_{k+1} is fixed, g_{k+2} can only take 2 different values; and, once g_{k+1} and g_{k+2} are fixed, g_{k+3} can take only 2 distinct values. Thus the number of points O_k is at most 2^{N+n-1}.

Let now M_k be the point whose coordinates are

$$(\lambda\theta^{k+1}x), (\lambda\theta^{k+2}x), \ldots, (\lambda\theta^{k+n}x),$$

where (z) denotes, as usual, the fractional part of z. This point considered as belonging to the n-dimensional unit torus is, by (6), interior to a cube of side

$$\frac{2\sigma}{2^{N/n}}$$

and of center O_k. The number of cubes is at most 2^{N+n-1} and their total volume is

$$2^{N+n-1}\frac{(2\sigma)^n}{2^N} = 2^{2n-1}\sigma^n = \frac{1}{2}(4\sigma)^n.$$

If we take $\sigma \leq \frac{1}{4}$, there will remain in the torus $0 \leq x_j < 1$ ($j = 1, 2, \ldots, n$) a "cell" free of points M_k. This will also be true, for every $k > k_0$ large enough, for the point M'_k of coordinates

$$(c_{k+1}x), \ldots, (c_{k+n}x),$$

if we denote generally by c_m the integer nearest to $\lambda\theta^m$, since we know that $\lambda\theta^m = c_m + \delta_m$ with $\delta_m \to 0$ ($m \to \infty$).

To show now that $E(\xi)$ is of the type $H^{(n)}$, we have only to prove that the sequence of vectors

$$V_k = (c_{k+1}, c_{k+2}, \ldots, c_{k+n})$$

in the Euclidean space R^n is normal. Let $a_1, a_2, \ldots, a_n$ be natural integers, not all zero. We have

$$a_1c_{k+1} + \cdots + a_nc_{k+n} = \lambda(a_1\theta^{k+1} + \cdots + a_n\theta^{k+n}) + (a_1\delta_{k+1} + \cdots + a_n\delta_{k+n}).$$

If $k \to \infty$, the last parenthesis tends to zero. On the other hand, the first parenthesis equals

$$\lambda\theta^{k+1}(a_1 + a_2\theta + \cdots + a_n\theta^{n-1}),$$

and its absolute value increases infinitely with k, since, θ being of degree n, we have

$$a_1 + a_2\theta + \cdots + a_n\theta^{n-1} \neq 0.$$

This completes the proof.

Remark. We have just proved that if θ belongs to the class S and has degree n the set $E(\xi)$ is of the type $H^{(n)}$. But it does not follow that E cannot be of a simpler type. Thus, for instance, if θ is quadratic, our theorem shows that E is of the type $H^{(2)}$. But in this particular case, one can prove that E is, more simply, of the type H.†

Stability of sets of uniqueness. We have shown in Chapter II that the set of numbers of the class S is closed. If $E(\xi_0)$ is a set M, ξ_0^{-1} belongs to an open interval contiguous to S. Hence, there exists a neighborhood of ξ_0 such that all numbers of this neighborhood give again sets M. Thus, a symmetrical perfect set of the type M presents a certain *stability* for small variations of ξ. On the contrary, if $E(\xi_0)$ is a U-set, there are in the neighborhood of ξ_0 numbers ξ such that $E(\xi)$ is an M-set. The sets of uniqueness are are "stable" for small variations of ξ.

† See *Trans. Amer. Math. Soc.*, Vol. 63 (1948), p. 597.

Chapter VII

THE CASE OF GENERAL "HOMOGENEOUS" SETS

1. Homogeneous sets

The notion of symmetrical perfect set with constant ratio of dissection can be generalized as follows.

Considering, to fix the ideas, the interval $[0, 1]$ as "fundamental interval," let us mark in this interval the points of abscissas

$$\eta_0 = 0, \quad \eta_1, \eta_2, \ldots, \eta_d \quad (d \geq 1;\ \eta_d = 1 - \xi),$$

and consider each of these points as the origin of an interval ("white" interval) of length ξ, ξ being a positive number such that

$$\xi < \frac{1}{d+1}$$

$$\eta_{j+1} - \eta_j > \xi \quad (\text{for all } j)$$

so that no two white intervals can have any point in common. The intervals between two successive "white" intervals are "black" intervals and are removed. Such a dissection of $[0, 1]$ will be called of the type $(d, \xi;\ \eta_0, \eta_1, \eta_2, \ldots, \eta_d)$.

We operate on each white interval a dissection homothetic to the preceding one. We get thus $(d+1)^2$ white intervals of length ξ^2, and so on indefinitely. By always removing the black intervals, we get, in the limit, a nowhere dense perfect set of measure zero, whose points are given by

$$x = \epsilon_0 + \epsilon_1\xi + \epsilon_2\xi^2 + \cdots, \tag{1}$$

where each ϵ_j can take the values $\eta_0, \eta_1, \ldots, \eta_d$.

The case of the symmetrical perfect set is obtained by taking

$$d = 1, \quad \eta_0 = 0, \eta_1 = 1 - \xi.$$

The set E of points (1) will be called "homogeneous" because, as is readily seen, E can be decomposed in $(d+1)^k$ portions, all homothetic to E in the ratio ξ^k ($k = 1, 2, \ldots$).

2. Necessary conditions for the homogeneous set E to be a U-set

Since each subset of a set of uniqueness is also a set of uniqueness, if we consider the set $E_0 \subset E$ whose points are given by (1) but allowing the ϵ_j to take only the values $\eta_0 = 0$ or $\eta_d = 1 - \xi$, then E_0 is a set U, if E is a set U.

But E_0 is a symmetrical perfect set with constant ratio of dissection ξ. Hence, if the homogeneous set E is a U-set, we have necessarily $\xi = 1/\theta$, where θ is a number of the class S.

Consider further the subset E' of E whose points are given by (1) but with the choice of the ϵ_j restricted as follows:

$$\begin{array}{lll} \epsilon_0 = 0 \text{ or } \eta_1 & \epsilon_d = 0 \text{ or } \eta_1 & \\ \epsilon_1 = 0 \text{ or } \eta_2 & \epsilon_{d+1} = 0 \text{ or } \eta_2 & \text{etc.} \\ \cdots\cdots & \cdots\cdots & \\ \epsilon_{d-1} = 0 \text{ or } \eta_d & \epsilon_{2d-1} = 0 \text{ or } \eta_d & \end{array}$$

The points of this set E' are given by

$$x' = \epsilon_1'\eta_1 + \epsilon_2'\eta_2\xi + \cdots + \epsilon_d'\eta_d\xi^{d-1} + \epsilon_{d+1}'\eta_1\xi^d + \cdots = \sum \epsilon_j' r_j,$$

where the ϵ_j' are either 0 or 1.

We can, as in the case of symmetrical perfect sets, define a measure carried by this set and prove that its Fourier-Stieltjes transform is

$$\prod_{k=1}^{\infty} \cos \pi u r_k. \tag{2}$$

If E is a U-set, E' is a U-set and (2) cannot tend to zero if $u \to \infty$. It follows that there exists an infinite sequence of values of u for which each of the infinite products

$$\begin{gathered} \cos \pi u\eta_1 \cdot \cos \pi u\eta_1\xi^d \cdot \cos \pi u\eta_1\xi^{2d} \cdots \\ \cos \pi u\eta_2\xi \cdot \cos \pi u\eta_2\xi^{d+1} \cdot \cos \pi u\eta_2\xi^{2d+1} \cdots \\ \cdots\cdots\cdots \\ \cos \pi u\eta_d\xi^{d-1} \cdot \cos \pi u\eta_d\xi^{2d-1} \cdot \cos \pi u\eta_d\xi^{3d-1} \end{gathered}$$

has absolute value larger than a fixed positive number a. Write $\omega = 1/\xi^d$. We have, for an infinite sequence of values of u:

$$\prod_{k=0}^{\infty} |\cos \pi u\eta_h\xi^{h-1} \cdot \xi^{kd}| > a \quad (h = 1, 2, \ldots, d),$$

and from this we deduce, by the same argument as in Chapter IV, the existence of a real number $\Lambda \neq 0$ such that

$$\sum \sin^2 \pi\Lambda\eta_h\xi^{h-1}\omega^n < \infty \quad (h = 1, 2, \ldots, d).$$

We know that from this condition it follows that (1) $\omega \in S$, a condition which we shall suppose to be fulfilled (since we know that we have the necessary condition $\xi^{-1} \in S$, which implies $\xi^{-d} \in S$), (2) the numbers

$$\Lambda\eta_1, \Lambda\eta_2, \ldots, \Lambda\eta_d$$

all belong to the field of ω (hence to the field of $\theta = \xi^{-1}$). Since $\eta_d = 1 - \xi$, it follows that

$$\eta_1, \eta_2, \ldots, \eta_d$$

Summing up our results we get:

THEOREM. *If the homogeneous set E is a set of uniqueness*, then:

1. $1/\xi$ *is an algebraic integer θ of the class S.*
2. *The abscissas $\eta_1, \ldots, \eta_d$ are algebraic numbers of the field of θ.*

We proceed now to prove that the preceding conditions are *sufficient* in order that E be a U-set.

3. Sufficiency of the conditions

THEOREM. *The homogeneous set E whose points are given by* (1), *where $1/\xi = \theta$ is an algebraic integer of the class S and the numbers $\eta_1, \ldots, \eta_d$ are algebraic belonging to the field of θ, is a set of the type $H^{(n)}$* (n being the degree of θ), *and thus a set of uniqueness.*

PROOF. Let a be a rational positive integer such that $a\eta_1, a\eta_2, \ldots, a\eta_d$ are integers of the field of θ. Denote by

$$\alpha^{(1)}, \ldots, \alpha^{(n-1)}$$

the conjugates of θ and by

$$\omega_j^{(1)}, \ldots, \omega_j^{(n-1)} \quad (j = 1, 2, \ldots, d)$$

the conjugates of η_j. Denote further by λ an algebraic integer of the field of θ, whose conjugates shall be denoted by

$$\mu^{(1)}, \ldots, \mu^{(n-1)}.$$

Writing (1) in the form

$$x = \epsilon_0 + \frac{\epsilon_1}{\theta} + \frac{\epsilon_2}{\theta^2} + \cdots \quad (\epsilon_j = \eta_0, \eta_1, \ldots, \eta_d)$$

we have, if m is a natural integer ≥ 0,

$$\lambda a\theta^m\eta_j + \sum_{i=1}^{n-1} \mu^{(i)}a \cdot \alpha^{(i)m}\omega_j^{(i)} \equiv 0 \pmod 1.$$

Thus, $x \in E$ being fixed, we have always

$$\lambda a\theta^m x = \lambda a\left(\frac{\epsilon_{m+1}}{\theta} + \cdots + \frac{\epsilon_{m+N}}{\theta^N}\right) + \lambda a\left(\frac{\epsilon_{m+N+1}}{\theta^{N+1}} + \cdots\right) + R \pmod 1,$$

where $N > 1$ is a natural integer to be chosen later on, and where, putting

$$M = \max_{i,j} \{|\omega_j^{(i)}|, \eta_j\}$$

we have

$$R < Ma\sum_{i=1}^{n-1} |\mu^{(i)}| \sum_{m=0}^{\infty} |\alpha^{(i)m}| = Ma\sum_{i=1}^{n-1} \frac{|\mu^{(i)}|}{1 - |\alpha^{(i)}|}.$$

Just as in the case considered in Chapter VI, Minkowski's theorem leads to the determination of the positive algebraic integer λ of the field of θ such that

$$\frac{\lambda a M}{\theta^N(\theta - 1)} < \frac{1}{2n(d+1)^{(N/n)+1}},$$

$$Ma \frac{|\mu_i|}{1 - |\alpha^{(i)}|} \leq \frac{1}{2n(d+1)^{(N/n)+1}},$$

provided that

$$[2n(d+1)^{\frac{N}{n}+1}]^{-n} > |\Delta| \theta^{-N}.$$

Here Δ is a certain nonvanishing determinant depending on the set E and on θ, but not on N. This condition can be written

$$\theta^N > \Delta(d+1)^N[2n(d+1)]^n$$

and will certainly be satisfied for a convenient choice of N, since $\theta > d+1$.

The numbers λ and N being now thus determined, we shall have, for all m and all $x \in E$,

$$\left| \lambda a \theta^m x - \lambda a \left(\frac{\epsilon_{m+1}}{\theta} + \cdots + \frac{\epsilon_{m+N}}{\theta^N} \right) \right| < \frac{1}{2(d+1)^{(N/n)+1}} \pmod 1.$$

The argument is now identical with the one of Chapter VI. It is enough to observe that

$$(d+1)^{N+n-1} \left[\frac{1}{(d+1)^{(N/n)+1}} \right]^n = \frac{1}{d+1}$$

in order to see that there exists in the torus $0 \leq x_j < 1$ ($j = 1, 2, \ldots, n$) a "cell" free of points whose coordinates are the fractional parts of

$$\lambda a \theta^{k+1} x, \lambda a \theta^{k+2} x, \ldots, \lambda a \theta^{k+n} x,$$

the natural integer $k > 0$ and the point $x \in E$ being arbitrary.

Since $\theta \in S$, we have $\lambda a \theta^m = c_m + \delta_m$, c_m being a rational integer and $\delta_m \to 0$. The remainder of the proof is as before, and we observe that the vectors

$$V_k(c_{k+1}, c_{k+2}, \ldots, c_{k+n})$$

form a normal family.

Exercise

The notion of symmetric perfect set with constant ratio of dissection (described at the beginning of Chapter IV) can be generalized as follows.

Divide the fundamental interval (say [0, 1]) in three parts of respective lengths ξ_1, $1 - 2\xi_1$, ξ_1 (where $0 < \xi_1 < \frac{1}{2}$). Remove the central part ("black" interval) and divide each of the two "white" intervals left in three parts of lengths proportional to ξ_2, $1 - 2\xi_2$, ξ_2 ($0 < \xi_2 < \frac{1}{2}$). The central parts are removed, and the 4 white intervals left are divided in parts proportional to ξ_3, $1 - 2\xi_3$, ξ_3 ($0 < \xi_3 < \frac{1}{2}$). We proceed like this using an infinite sequence of ratios $\xi_1, \xi_2, \ldots, \xi_n, \ldots$ and we obtain a symmetric perfect set with variable rates of dissection $E(\xi_1, \ldots, \xi_n, \ldots)$.

Suppose now that the sequence $\{\xi_n\}_1^\infty$ is periodic, i.e., that $\xi_{p+j} = \xi_j$ for all j, the period p being a fixed integer. Prove that the set $E(\xi_1, \ldots, \xi_n \ldots)$ can be considered as a "homogeneous set" in the sense of Chapter VII, with a constant rate of dissection

$$X = \xi_1 \cdots \xi_p.$$

Using the results of this chapter, prove that this set is a set of uniqueness if and only if the following hold.

1. X^{-1} belongs to the class S.
2. The numbers $\xi_1, \ldots, \xi_p$ are algebraic and belong to the field of X.

SOME UNSOLVED PROBLEMS

1. The following problem has already been quoted in Chapter I:

Suppose that the real number $\theta > 1$ is such that there exists a real λ with the property that $\| \lambda\theta^n \| \to 0$ as the integer n increases infinitely (without any other hypothesis). Can one conclude that θ belongs to the class S?

Another way to state the same problem is:

Among the numbers $\theta > 1$ such that, for a certain real λ, $\| \lambda\theta^n \| \to 0$ as $n \to \infty$, do there exist numbers θ which are not algebraic?

2. Let us consider the numbers τ of the class T defined in Chapter III. It is known that every number θ of the class S is a limit point of numbers τ (on both sides). Do there exist other limit points of the numbers τ, and, if so, which ones?

3. It has been shown in Chapter IV that the infinite product

$$\Gamma(u) = \prod_{k=0}^{\infty} \cos \pi u \xi^k$$

is, for $0 < \xi < \frac{1}{2}$, the Fourier-Stieltjes transform of a positive measure whose support is a set $E(\xi)$ of the Cantor type and of constant rate of dissection ξ. But this infinite product has a meaning if we suppose only $0 < \xi < 1$, and in the case $\frac{1}{2} < \xi < 1$ it is the Fourier-Stieltjes transform of a positive measure whose support is a whole interval.† We know that $\Gamma(u) = o(1)$ for $u \to \infty$, if and only if ξ^{-1} does not belong to the class S. Let

$$\Gamma_1(u) = \prod_{0}^{\infty} \cos \pi u \xi_1^k,$$

$$\Gamma_2(u) = \prod_{0}^{\infty} \cos \pi u \xi_2^k$$

where ξ_1^{-1} and ξ_2^{-1} both belong to the class S, so that neither $\Gamma_1(u)$ nor $\Gamma_2(u)$ tends to zero for $u = \infty$. What is the behavior of the product

$$\Gamma_1(u) \cdot \Gamma_2(u)$$

as $u \to \infty$? Can this product tend to zero? Example, $\xi_1 = \frac{1}{3}$, $\xi_2 = \frac{1}{4}$.

This may have an application to the problem of sets of multiplicity. In fact, if ξ_1 and ξ_2 are small enough, $\Gamma_1\Gamma_2$ is the Fourier-Stieltjes transform of a measure whose support is a perfect set of measure zero, namely $E(\xi_1) + E(\xi_2)$.† If $\Gamma_1\Gamma_2 \to 0$, this set would be a set of multiplicity.

† See Kahane and Salem, *Colloquium Mathematicum*, Vol. VI (1958), p. 193. By $E(\xi_1) + E(\xi_2)$ we denote the set of all numbers $x_1 + x_2$ such that $x_1 \in E(\xi_1)$ and $x_2 \in E(\xi_2)$.

4. In the case $\frac{1}{2} < \xi < 1$, the measure of which $\Gamma(u)$ is the Fourier-Stieltjes transform can be either absolutely continuous or purely singular.† Determine the values of ξ for which one or the other case arises. (Of course, if $\xi^{-1} \in S$, $\Gamma(u) \neq o(1)$ and the measure is purely singular. The problem is interesting only if ξ^{-1} does not belong to the class S.)

† See Jessen and Wintner, *Trans. Amer. Math. Soc.*, Vol. 38 (1935), p. 48.

APPENDIX

For the convenience of the reader we state here a few definitions and results which are used throughout the book.

We assume that the reader is familiar with the elementary notions of algebraic numbers and algebraic fields. (See, e.g., [5].)

1. An *algebraic integer* is a root of an equation of the form

$$x^k + a_1 x^{k-1} + \cdots + a_k = 0,$$

where the a_j are rational integers, the coefficient of the term of highest degree being 1.

If α is any algebraic number, there exists a natural integer m such that $m\alpha$ be an algebraic integer.

If θ is an algebraic integer of degree n, then the irreducible equation of degree n with rational coefficients, with coefficient of x^n equal to 1, and having θ as one of its roots, has all its coefficients rational integers. The other roots, which are also algebraic integers, are the *conjugates* of θ.

Every symmetric function of θ and its conjugates is a rational integer. This is the case, in particular, for the product of θ and all its conjugates, which proves that it is impossible that θ and all its conjugates have all moduli less than 1.

The algebraic integer θ is a *unit* if $1/\theta$ is an algebraic integer.

2. If (in a given field) $f(x)$ is an irreducible polynomial, and if a root ξ of $f(x)$ is also a root of a polynomial $P(x)$, then $f(x)$ divides $P(x)$ and thus all roots of f are roots of P.

3. If an algebraic integer and all its conjugates have all moduli equal to 1, they are all roots of unity (see [9]).

4. Let R be a ring of real or complex numbers such that 0 is not a limit point of numbers of R. (R is then called a *discontinuous domain of integrity*.) Then the elements of R are rational integers or integers of an imaginary quadratic field (see [9]).

5. There exist only a finite number of algebraic integers of given degree n, which lie with all their conjugates in a bounded domain of the complex plane (see [9]).

6. Let $P(x)$ be a polynomial in a field k. Let K be an extension of k such that, in K, $P(x)$ can be factored into linear factors. If $P(x)$ cannot be so factored in an intermediate field K' (i.e., such that $k \subset K' \subset K$), the field K is said to be a *splitting* field of $P(x)$, and the roots of $P(x)$ generate K.

Let $\alpha_1, \ldots, \alpha_n$ be the roots of $P(x)$ in the splitting field $K = k(\alpha_1, \ldots, \alpha_n)$. Each automorphism of K over k (i.e., each automorphism of K whose restriction

to k is the identity) maps a root of $P(x)$ into a root of $P(x)$, i.e., permutes the roots. The group of automorphisms of K over k is called the (Galois) *group* of the equation $P(x) = 0$. This group is a permutation group acting on the roots $\alpha_1, \ldots, \alpha_n$ of $P(x)$.

If $P(x)$ is irreducible in k, the group thus defined is *transitive*.

See, for all this, [1].

7. Uniform distribution modulo 1 of a sequence of numbers has been defined in Chapter I.

A necessary and sufficient condition for the sequence $\{u_n\}_1^\infty$ to be uniformly distributed modulo 1 is that for every function $f(x)$ periodic with period 1 and Riemann integrable,

$$\lim_{n\to\infty} \frac{f(u_1) + \cdots + f(u_n)}{n} = \int_0^1 f(x)dx.$$

H. Weyl has shown that the sequence $\{u_n\}$ is uniformly distributed modulo 1 if and only if for every integer $h \neq 0$,

$$\lim_{n\to\infty} \frac{e^{2\pi i h u_1} + \cdots + e^{2\pi i h u_n}}{n} = 0.$$

In R^p (p-dimensional Euclidean space) the sequence of vectors

$$V_n = (v_n^1, \ldots, v_n^p)$$

is uniformly distributed modulo 1 in the torus T^p, if for every Riemann integrable function

$$f(x) = f(x^1, \ldots, x^p),$$

periodic with period 1 in each x^j, we have

$$\lim_{n\to\infty} \frac{f(V_1) + \cdots + f(V_n)}{n} = \int_{T^p} f(x)dx,$$

the integral being taken in the p-dimensional unit torus T^p.

H. Weyl's criterion becomes

$$\lim \frac{e^{2\pi i (HV_1)} + \cdots + e^{2\pi i (HV_n)}}{n} = 0$$

where (HV_n) is the scalar product

$$h_1 v_n^1 + \cdots + h_n v_n^p$$

and $h_1, \ldots, h_n$ are rational integers not all 0.

If $\omega_1, \omega_2, \ldots, \omega_p$, and 1 are linearly independent, the vector $(n\omega_1, \ldots, n\omega_p)$ is uniformly distributed modulo 1 (see [2]).

8. *Kronecker's theorem.* See [2]. In the form in which we use it in Chapter III it may be stated as follows:

If

$$\theta_1, \theta_2, \ldots, \theta_k, 1$$

are linearly independent, $\alpha_1, \alpha_2, \ldots, \alpha_k$ *are arbitrary, and N and* ϵ *are positive, there exist integers*

$$n > N, p_1, p_2, \ldots, p_k$$

such that

$$| n\theta_j - p_j - \alpha_j | < \epsilon \quad (j = 1, 2, \ldots, k).$$

(This may be considered as a weak consequence of the preceding result on uniform distribution modulo 1 of the vector $(n\theta_1, \ldots, n\theta_k)$.)

9. We had occasion to cite *Minkowski's theorem* on linear forms in Chapters I, III, and VI. We restate it here as follows.

Let

$$\lambda_p(x) = \sum_{q=1}^{n} a_q{}^p x_q \quad (p = 1, 2, \ldots, n)$$

be n linear forms of the n variables $x_1, \ldots, x_n$ *where the coefficients are real and the determinant D of the forms is not zero. There exists a point x with integral coordinates not all zero,* $x_1, \ldots, x_n$ such that

$$| \lambda_p(x) | \leq \delta_p,$$

provided that $\delta_1 \cdots \delta_p \geq | D |$.

The result holds if the coefficients $a_q{}^p$ are complex, provided that complex forms figure in conjugate pairs, and that the two δ_p's corresponding to a conjugate pair are equal.

The theorem is usually proved by using the following result. If K is a convex region of volume V in the Euclidean space R^n with center of symmetry at the origin and if $V > 2^n$, the region K contains points of integral coordinates other than the origin. An extremely elegant proof of this result has been given by C. L. Siegel, *Acta Mathematica*, Vol. 65 (1935).

BIBLIOGRAPHY

[1] Artin, E., *Galois Theory* (Notre Dame Mathematical Lectures, No. 2), 2d ed., rev. Notre Dame, Indiana; University of Notre Dame Press, 1944. See particularly pp. 30 ff., 46, and 76.

[2] Cassels, J. W. S., *An Introduction to Diophantine Approximation.* Cambridge: Cambridge University Press, 1957. See particularly Chapter IV.

[3] Hardy, G. H., *A Course of Pure Mathematics*, 10th ed. Cambridge: Cambridge University Press, 1952. See particularly Chapter VIII, p. 392.

[4] Hardy, G. H., Littlewood, J. E., and Polya, G., *Inequalities*, 2d ed. Cambridge: Cambridge University Press, 1952. See p. 30.

[5] Hecke, E., *Vorlesungen über die Theorie der Algebraischen Zahlen*, 2. Auflage. Leipzig, 1954. See p. 116.

[6] Kahane, J.-P., *Comptes Rendus,*† Vol. 248 (1959), p. 2943.

[7] Koksma, J. F., *Compositio mathematica*, Vol. 2 (1935), p. 250.

[8] Malliavin, P., *Comptes Rendus,*† Vol. 248 (1959), p. 2155.

[9] Polya, G. and Szegö, G., *Aufgaben und Lehrsätze aus der Analysis*, 2 vols. Berlin: Julius Springer, 1925. See Vol. II, pp. 149–150.

[10] Pisot, C., *Annali di Pisa*, Vol. 7 (1938), pp. 205–248.

[11] Pisot, C., and Dufresnoy, J., *Annales Scientifiques de l'École Normale Supérieure*, Vol. 70 (1953), pp. 105–133.

[12] Salem, R., *Duke Mathematical Journal*, Vol. 11 (1944), pp. 103–108.

[13] Salem, R., *Duke Mathematical Journal*, Vol. 12 (1945), pp. 153–172.

[14] Salem, R., and Zygmund, A., *Comptes Rendus,*† Vol. 240 (1955), pp. 2040–2042. See footnotes.

[15] Salem, R., and Zygmund, A., *Comptes Rendus,*† Vol. 240 (1955), pp. 2281–2285. See footnotes.

[16] Weyl, H., *Mathematische Annalen*, Vol. 77 (1916), pp. 313–352.

[17] Zygmund, A., *Trigonometric Series*, 2d ed., 2 vols. Cambridge: Cambridge University Press, 1959. See particularly Vol. I, Chapter VII and Chapter IX.

† *Comptes Rendus Hebdomadaires des Séances de l'Académie des Sciences.*

INDEX