PART 2

RATIONAL APPROXIMATIONS OF ALGEBRAIC NUMBERS

The problem and its history.

Let α be a real algebraic number of degree $n \geqslant 2$; thus α is irrational. One of the results obtained in the proof of Theorem 1 of Chapter 3 was as follows. Let

$$F(x) = A_0 x^m + A_1 x^{m-1} + \ldots + A_m \neq 0$$

be any polynomial with integral coefficients, of degree at most m, and of height

$$A = \lceil F(x) \rceil = \max(|A_0|, |A_1|, \ldots, |A_m|) \geqslant 1.$$

Then

$$\text{either } F(\alpha) = 0 \quad \text{or} \quad |F(\alpha)| \geqslant c_1(m) A^{-(m-1)},$$

where $c_1(m) > 0$ depends on α and on m, but not on A.

Let now $m=1$ and $F(x)=Qx-P$ where $Q > 0$ and P are integers; then $A=\max(|P|, Q)$, and on putting $c_1 = c_1(1)$, the last result implies that

$$|Q\alpha - P| \geqslant c_1 \max(|P|, Q)^{-(n-1)},$$

because $Q\alpha - P \neq 0$. This inequality is equivalent to

(1):
$$\left|\alpha - \frac{P}{Q}\right| \geqslant cQ^{-n}$$

where $c > 0$ is another constant depending only on α. For either

$$\left|\frac{P}{Q}\right| > |\alpha| + 1 \quad \text{and then} \quad \left|\alpha - \frac{P}{Q}\right| > 1 \geqslant Q^{-n},$$

or

$$\left|\frac{P}{Q}\right| \leqslant |\alpha| + 1, \text{ hence } \max(|P|, Q) \leqslant (|\alpha| + 1)Q, \text{ and then}$$

$$\left|\alpha - \frac{P}{Q}\right| \geqslant \frac{c_1}{Q} \{(|\alpha| + 1)Q\}^{-(n-1)} = \frac{c_1}{(|\alpha|+1)^{n-1}} Q^{-n}.$$

The inequality (1) is due to J. Liouville[1] who used it in his construction of real transcendental numbers. Apart from the value of the constant c, it is best possible for quadratic irrationals ($n=2$). For, as was proved in two different ways in Chapters 3 and 4, if α is any irrational number (not necessarily algebraic), then there are infinitely many distinct rational numbers $\frac{P}{Q}$ such that

[1] C. R. Acad. Sci. (Paris), 18 (1844), 883-885, 910-911.

(2): $$\left|\alpha - \frac{P}{Q}\right| < \frac{1}{Q^2} .$$

Let, however, α be a real algebraic number of degree $n \geqslant 3$. Then the inequality (1) can be improved. Denote by $M(\alpha)$ the least upper bound of all positive numbers ρ for which the inequality

(3): $$\left|\alpha - \frac{P}{Q}\right| < \frac{1}{Q^\rho}$$

has infinitely many distinct rational solutions $\frac{P}{Q}$. From the inequalities (1) and (2) it is evident that

$$2 \leqslant M(\alpha) \leqslant n.$$

The first improvement of the upper bound for $M(\alpha)$ was obtained by A. Thue[2] who showed that

$$M(\alpha) \leqslant \frac{n}{2} + 1.$$

Not only was his work of great importance by its implications for the theory of Diophantine equations, but, in addition, *the method introduced by him formed the basis for all later work on the subject.*

Next, C. L. Siegel[3] proved that

$$M(\alpha) \leqslant \min_{s=1,2,\dots,n-1} \left(\frac{n}{s+1} + s\right) < 2\sqrt{n},$$

an inequality which is of great importance in the theory of Diophantine equations. A further improvement was given by F. J. Dyson[4] who found that

$$M(\alpha) \leqslant \sqrt{2n} ,$$

a result also obtained by A. Gelfond.

Finally, K. F. Roth[5] has settled the problem by proving that

$$M(\alpha) = 2.$$

This result may be stated in several equivalent forms. It implies that for $\rho > 2$ the inequality (3) has at most finitely many rational solutions and hence that there is then a constant $\gamma(\alpha,\rho) > 0$ such that

$$\left|\alpha - \frac{P}{Q}\right| \geqslant \gamma(\alpha,\rho) Q^{-\rho} \quad \text{for all rational numbers } \frac{P}{Q} .$$

However, no method is known for actually finding such a constant $\gamma(\alpha,\rho)$, a disadvantage shared by the methods of Thue, Siegel, Dyson, and Roth, and also by the work in this second part.

[2] Skrifter udgivne af Videnskabs-Selskabet i Christiania, 1908, and J. reine angew. Math. 135 (1909), 284-305.

[3] Math. Z. 10 (1921), 173-213.

[4] Acta math. 79 (1947), 225-240.

[5] Mathematika 2 (1955), 1-20 and 168.

Before Roth, Th. Schneider[6] had already proved a weaker theorem. Assume there exists an infinite sequence of rational numbers

$$\frac{P_1}{Q_1}, \frac{P_2}{Q_2}, \frac{P_3}{Q_3}, \ldots, \quad \text{where} \quad 1 \leqslant Q_1 < Q_2 < Q_3 < \ldots,$$

such that

$$(4): \qquad \left|\alpha - \frac{P_k}{Q_k}\right| \leqslant Q_k^{-\rho} \qquad (k = 1,2,3,\ldots)$$

for some $\rho > 2$. Then

$$(5): \qquad \limsup_{k \to \infty} \frac{\log Q_{k+1}}{\log Q_k} = \infty .$$

This theorem by Schneider is nearly as powerful as Roth's theorem for certain applications to proofs of transcendency.

Generalisations of these results by Siegel and Schneider have been known for many years. Already Siegel himself[3] extended his result to the approximations of α by the numbers of an arbitrary algebraic number field of finite degree. The corresponding analogue of Roth's theorem has recently been established by W.J. LeVeque[7]. As these lectures do not deal with the $\mathfrak{p}$-adic completions of algebraic number fields, such generalisations will not be discussed. But it would have much interest to carry out a similar extension of the later Approximation Theorems. See, however, Appendix C.

In another kind of generalisation, the numerator P or the denominator Q of the rational approximation $\frac{P}{Q}$ is restricted by some arithmetic condition. For instance, it may be demanded that Q is a power of a given positive integer or that, more generally, the greatest prime factor of Q is bounded. Such theorems were given by Schneider[6] and myself[8], but asserted only a result of the form (5). However, now that Roth's method is known, D. Ridout[9] has obtained an extension of this kind for Roth's theorem which is free of this defect.

A third kind of generalisation will seem natural to the reader of the first part. Instead of studying the rational approximations of a real algebraic number, one considers those of a p-adic, g-adic, or g*-adic algebraic number $\mathfrak{a}$. In the notation of Chapter 3, it is then especially the behaviour of the function

$$\Omega\left(\mathfrak{a} - \frac{P}{Q}\right)$$

which is of interest. Some 25 years ago, I[10] studied exactly this kind of problem by means of Siegel's methods. Again Ridout[11] has obtained the analogous extension of Roth's theorem.

[6] J. reine angew. Math. 175 (1936), 182-192.

[7] Topics in number theory, vol. 2, chapter 4 (Reading, Mass. 1956).

[8] Proc. Kon. Akad. Amsterdam 39 (1936), 633-644, 729-737; Acta Arithmetica 3 (1938), 89-93.

[9] Mathematika 4 (1957), 125-131.

[10] Math. Ann. 107 (1933), 691-730; 108 (1933, 37-55). My results have been extended to the approximations of $\mathfrak{p}$-adic algebraic numbers by C. J. Parry, Acta math. 83 (1950), 1-100.

[11] Mathematika 5 (1958), 40-48.

The aim of the following chapters may now be stated as follows. We shall combine the method of Roth with the idea of Schneider on arithmetic restrictions for P and Q and that of mine on the use of p-adic algebraic numbers. By deliberately applying g-adic numbers and the g-adic pseudo-valuation, it will be possible to simplify many of the proofs, as compared with my old paper[10].

Although the following proofs will make essential use of both real and g-adic numbers, at least one form of the final results will be completely free of these numbers and state a property of rational numbers only. Thus real and g-adic numbers will serve as tools, but not as an end in themselves. This seems to me highly satisfactory. For the theory of numbers still has its main interest in what it can tell us about the rational numbers and the rational integers. But if we want to find properties of the rational numbers, nothing must stop us in the choice of methods used for this purpose.