Chapter 9

APPLICATIONS

1. The theorems of Roth and Ridout.

The two Approximation Theorems proved in Chapters 7 and 8 contain as special cases the theorems of Roth and of Ridout. These results were already mentioned in the introduction to Part 2, and we then gave the references to the literature.

Roth's theorem may be considered as either the special case $d=1$, $\lambda=1$, $\mu=1$ of Theorem (1,I) or as the special case $r=r'=r''=0$ of Theorem (2,I). It states:

If ξ is a real algebraic number; if ρ and c_1 are positive constants; and if there exist infinitely many distinct simplified fractions $\frac{P^{(k)}}{Q^{(k)}}$ such that

$$\left|\frac{P^{(k)}}{Q^{(k)}} - \xi\right| \leqslant c_1 |Q^{(k)}|^{-\rho},$$

then $\rho \leqslant 2$.

This theorem is obvious if ξ is rational; thus, e.g. the case when $\xi = 0$ may be excluded. Now $\frac{P^{(k)}}{Q^{(k)}}$ tends to ξ as k tends to infinity. Hence, by $\xi \neq 0$, the integers $P^{(k)}$, $Q^{(k)}$, and $H^{(k)}$ have the same order of magnitude. It follows that, for all k,

$$c_1 |Q^{(k)}|^{-\rho} \leqslant c_1' H^{(k)-\rho}$$

where c_1' is a further positive constant. Hence the assertion is an immediate consequence of either Approximation Theorem.

We next show that Ridout's theorems may be deduced from Theorem (2,I).

His first theorem is as follows. Let again $\xi \neq 0$ be a real algebraic number; let ρ, c_1, c_3, and c_4 be positive constants; and let λ and μ be constants such that

$$0 \leqslant \lambda \leqslant 1, \quad 0 \leqslant \mu \leqslant 1.$$

Assume that there exist infinitely many simplified fractions $\frac{P^{(k)}}{Q^{(k)}}$ with the following properties:

(i): $$\left|\frac{P^{(k)}}{Q^{(k)}} - \xi\right| \leqslant c_1 |Q^{(k)}|^{-\rho} .$$

(ii): *The numerators $P^{(k)}$ and the denominators $Q^{(k)}$ are distinct from zero* *and can be written in the form*

$$P^{(k)} = P^{(k)*}\prod_{j=1}^{r'} p_j^{e_j}, \qquad Q^{(k)} = Q^{(k)*}\prod_{j=r'+1}^{r'+r''} p_j^{e_j}$$

where $p_1,\dots,p_{r'}, p_{r'+1},\dots,p_{r'+r''}$ *are finitely many distinct primes,* $e_1,\dots,e_{r'}, e_{r'+1},\dots,e_{r'+r''}$ *are non-negative integers, and* $P^{(k)*}$, $Q^{(k)*}$ *are integers such that*

$$0 < |P^{(k)*}| \leqslant c_3|P^{(k)}|^{\lambda}, \quad 0 < |Q^{(k)*}| \leqslant c_4|Q^{(k)}|^{\mu}.$$

Then

$$\rho \leqslant \lambda + \mu .$$

For the three integers $P^{(k)}$, $Q^{(k)}$, and $H^{(k)}$ have again the same order of magnitude. It follows that there exist three positive constants c_1', c_3', and c_4' such that, for all k,

$$c_1|Q^{(k)}|^{-\rho} \leqslant c_1'\, H^{(k)-\rho}$$

and

$$\prod_{j=1}^{r'} |P^{(k)}|_{p_j} \leqslant c_3' H^{(k)\lambda-1}, \qquad \prod_{j=r'+1}^{r'+r''} |Q^{(k)}|_{p_j} \leqslant c_4' H^{(k)\mu-1} .$$

The latter inequalities hold because, e.g.

$$\prod_{j=1}^{r'} p_j^{e_j} = \left|\frac{P^{(k)}}{P^{(k)*}}\right| \geqslant \frac{1}{c_3}\,|P^{(k)}|^{1-\lambda} \geqslant \frac{1}{c_3'}\,H^{(k)1-\lambda} .$$

Therefore, from the hypothesis,

$$\left|\frac{P^{(k)}}{Q^{(k)}} - \xi\right| \prod_{j=1}^{r'} |P^{(k)}|_{p_j} \prod_{j=r'+1}^{r'+r''} |Q^{(k)}|_{p_j} \leqslant c_1'c_3'c_4'\, H^{(k)\lambda+\mu-\rho-2},$$

and so the assertion is contained in the special case r=0 of Theorem (2,I).

Ridout's second theorem generalises that of Roth in a different direction. It is essentially equivalent to the case r'=r''=0 of Theorem (2,I), and it may be stated as follows.

Let ξ, ξ_1,,, ξ_r *be a real, a* p_1*-adic,..., a* p_r*-adic algebraic number, respectively. Let* τ *and* c *be positive constants. Assume there exist infinitely many distinct simplified fractions such that*

$$\left|\frac{P^{(k)}}{Q^{(k)}} - \xi\right| {\prod_{j=1}^{r}}^{*} |P^{(k)} - \xi_j Q^{(k)}|_{p_j}^{*} \leqslant c\, H^{(k)-\tau} .$$

Then $\tau \leqslant 2$.

As we see, this theorem does not require that

$$\xi \neq 0,\ \xi_1 \neq 0, \ldots, \xi_r \neq 0,$$

a restriction imposed by both Approximation Theorems. However, this presents no difficulty. For choose a rational integer $n > 0$ such that the $r+1$ algebraic numbers

$$\xi' = \xi + n, \quad \xi_1' = \xi_1 + n, \ldots, \xi_r' = \xi_r + n$$

are all distinct from zero, and put

$$P^{(k)'} = P^{(k)} + nQ^{(k)}.$$

Then

$$H^{(k)'} \leqslant H^{(k)}.\,(n+1), \qquad \text{where} \qquad H^{(k)'} = \max(|P^{(k)'}|, |Q^{(k)}|),$$

and it is evident that

$$\left|\frac{P^{(k)'}}{Q^{(k)}} - \xi'\right|^* = \left|\frac{P^{(k)}}{Q^{(k)}} - \xi\right|^*$$

and

$$|P^{(k)'} - \xi_j' Q^{(k)}|^*_{p_j} = |P^{(k)} - \xi_j Q^{(k)}|^*_{p_j} \qquad (j = 1,2,\ldots,r).$$

Further

$$\left|\frac{P^{(k)'}}{Q^{(k)}} - \xi_j'\right|_{p_j} = |Q^{(k)}|^{-1}_{p_j}\, |P^{(k)'} - \xi_j' Q^{(k)}|_{p_j}$$

and hence

$$\left|\frac{P^{(k)'}}{Q^{(k)}} - \xi_j'\right|^*_{p_j} \leqslant |Q^{(k)}|^{-1}_{p_j}\, |P^{(k)} - \xi_j Q^{(k)}|^*_{p_j},$$

because

$$|Q^{(k)}|_{p_j} \leqslant 1 .$$

The hypothesis implies therefore that

$$\left|\frac{P^{(k)'}}{Q^{(k)}} - \xi'\right|^* \prod_{j=1}^{r} \left|\frac{P^{(k)'}}{Q^{(k)}} - \xi_j'\right|^*_{p_j} \leqslant K_1 H^{(k)'-\tau},$$

where K_1 denotes the constant

$$K_1 = c(n+1)^{\tau} \sup_{k} \prod_{j=1}^{r} |Q^{(k)}|^{-1}_{p_j}$$

where the supremum exists because

$$(P^{(k)}, Q^{(k)}) = 1 \text{ and } \xi_j' \neq 0.$$

On applying now Theorem (2,I) to this inequality, with $r'=r''=0$ and with $\xi', \xi_1', \ldots, \xi_r'$ as the algebraic numbers, the assertion $\tau \leqslant 2$ follows at once. For $P^{(k)'}$ can be zero for only finitely many k.

2. The continued fraction of a real algebraic number.

One simple application of Ridout's first theorem is of interest in itself.

Let ξ be a real irrational algebraic number. Then ξ can be written as an infinite continued fraction

$$\xi = [a_0, a_1, a_2, \ldots]$$

where the incomplete denominators $a_0, a_1, a_2, \ldots$ are integers, all but perhaps a_0 being positive. Denote by $\frac{P_n}{Q_n}$ the n-th convergent of this continued fraction. As was proved in Chapter 4,

$$\left|\frac{P_n}{Q_n} - \xi\right| < Q_n^{-2} .$$

We can now show the following result.

Both the greatest prime factor of P_n *and that of* Q_n *tend to infinity with* n.

For assume, say, that there exists an infinite sequence of suffixes,

$$N = \{n_1, n_2, n_3, \ldots\}, \quad \text{where} \quad n_1 < n_2 < n_3 < \ldots,$$

such that, for $n \in N$, P_n allows only the finitely many prime factors $p_1, \ldots, p_{r'}$. We can then apply the first theorem of Ridout with

$$\rho = 2, \lambda = 0, \mu = 1,$$

and evidently obtain a contradiction. The assertion for Q_n is proved in the same manner.

3. The powers of a rational number.

The case $\lambda = \mu = 0$ of Ridout's first theorem implies the following result.

Let $\xi \neq 0$ *be a real algebraic number; let* $p_1, \ldots, p_s$ *be finitely many distinct primes; and let* ϵ *be an arbitrarily small positive constant. There exist at most finitely many systems of* s *integers,*

$$\{e\} = \{e_1, e_2, \ldots, e_s\},$$

such that

$$|p_1^{e_1} \ldots p_s^{e_s} - \xi| < e^{-\epsilon E}$$

where

$$E = \max_{j=1,2,\ldots,s} |e_j| .$$

For put

$$p_1^{e_1} \dots p_s^{e_s} = \frac{P}{Q}$$

where P and Q are positive integers which are relatively prime. To each system $\{e\}$ there belongs then such a fraction $\frac{P}{Q}$ such that

$$\left|\frac{P}{Q} - \xi\right| < e^{-\epsilon E}.$$

It is obvious that

$$Q \leqslant p_0^{sE}$$

where p_0 denotes the largest of the primes $p_1, \dots, p_s$. Hence

$$\left|\frac{P}{Q} - \xi\right| < Q^{-\rho}, \qquad \text{where} \qquad \rho = \frac{\epsilon}{s \log p_0} > 0 .$$

The prime factors of both P and Q are bounded. Therefore the first theorem of Ridout may be applied with

$$\rho > 0, \;\; \lambda = \mu = 0, \qquad \text{so that} \qquad \rho > \lambda + \mu ,$$

and it follows that the number of solutions $\frac{P}{Q}$, or, what is the same, that of systems $\{e\}$, is finite.

This result may now be generalised, as follows.

Theorem 1: *Let* $\xi \neq 0$ *be a real algebraic number; let* $p_1, \dots, p_s$ *be finitely many distinct primes; and let* ϵ *be an arbitrarily small positive constant. There exist at most finitely many systems of* $s+1$ *integers*

$$\{e\} = \{e_0, e_1, \dots, e_s\}$$

with $e_0 \neq 0$ *such that*

$$0 < |p_1^{e_1} \dots p_s^{e_s} - e_0 \xi| < e^{-\epsilon E}$$

where

$$E = \max_{j=1,2,\dots,s} |e_j| .$$

Proof: We assume that the assertion is false, hence that there are infinitely many different solutions

$$\{e^{(k)}\} = \{e_0^{(k)}, e_1^{(k)}, \dots, e_s^{(k)}\} \qquad (k = 1,2,3,\dots)$$

of the inequality

$$(1): \qquad 0 < |p_1^{e_1^{(k)}} \dots p_s^{e_s^{(k)}} - e_0^{(k)} \xi| < e^{-\epsilon E^{(k)}}$$

where

$$E^{(k)} = \max_{j=1,2,\dots,s} |e_j^{(k)}| .$$

For each solution $\{e^{(k)}\}$ put

$$p_1^{e_1^{(k)}} \cdots p_s^{e_s^{(k)}} = \frac{P^{(k)}}{Q^{(k)}}$$

with positive integers $P^{(k)}$ and $Q^{(k)}$ which are relatively prime.

We divide now the solutions into equivalence classes by putting two solutions $\{e^{(k)}\}$ and $\{e^{(1)}\}$ into the same class, in symbols

$$\{e^{(k)}\} \sim \{e^{(1)}\},$$

whenever

$$\frac{P^{(k)}}{e_0^{(k)}Q^{(k)}} = \frac{P^{(l)}}{e_0^{(l)}Q^{(l)}} .$$

Each such class evidently contains a unique element, $\{e^{(m)}\}$ say, for which the positive integer $|e_0^{(m)}|$ is a minimum. This solution $\{e^{(m)}\}$ is said to be the *minimum solution* of its class.

Consider now an arbitrary solution $\{e^{(k)}\}$ for which the greatest common divisor

$$(e_0^{(k)}, P^{(k)}), = d^{(k)} \text{ say,}$$

is greater than 1, and put

(2): $$P^{(k)*} = \frac{P^{(k)}}{d^{(k)}}, \quad e_0^{(k)*} = \frac{e^{(k)}}{d^{(k)}},$$

so that

$$(e_0^{(k)*}, P^{(k)*}) = 1.$$

Then

$$\frac{P^{(k)*}}{Q^{(k)}} = p_1^{e_1^{(k)*}} \cdots p_s^{e_s^{(k)*}}$$

with new integers $e_1^{(k)*}, \ldots, e_s^{(k)*}$. From the construction, it is clear that, for $j = 1,2,\ldots, s$,

$$0 \leqslant e_j^{(k)*} \leqslant e_j^{(k)} \text{ if } e_j^{(k)} \geqslant 0, \quad e_j^{(k)*} = e_j^{(k)} \text{ if } e_j^{(k)} < 0 .$$

Therefore

$$E^{(k)*} = \max_{j=1,2,\ldots,s} |e_j^{(k)*}|$$

satisfies the inequality

$$0 \leq E^{(k)*} \leq E^{(k)} .$$

It follows then from (1) and (2) that

$$0 < \left| p_1^{e_1^{(k)*}} \dots p_s^{e_s^{(k)*}} - e_0^{(k)*} \xi \right| < \frac{e^{-\epsilon E^{(k)}}}{|d^{(k)}|} < e^{-\epsilon E^{(k)*}} ,$$

and hence $\{e^{(k)*}\}$ is likewise a solution. Evidently

$$\{e^{(k)*}\} \sim \{e^{(k)}\} \qquad \text{and} \qquad |e_0^{(k)*}| < |e_0^{(k)}| .$$

We have thus proved that *every minimum solution* $\{e^{(m)}\}$ *satisfies the equation*

(3): $$(e_0^{(m)}, P^{(m)}) = 1.$$

Next consider any solution $\{e^{(k)}\}$ which is in the same class as the minimum solution $\{e^{(m)}\}$; i.e.,

$$\frac{P^{(k)}}{e_0^{(k)} Q^{(k)}} = \frac{P^{(m)}}{e_0^{(m)} Q^{(m)}} .$$

Then, by (1),

$$0 < \left| \frac{P^{(m)}}{e_0^{(m)} Q^{(m)}} - \xi \right| = \left| \frac{P^{(k)}}{e_0^{(k)} Q^{(k)}} - \xi \right| < \frac{e^{-\epsilon E^{(k)}}}{|e_0^{(k)}|} .$$

Hence *there can only be finitely many solutions* $\{e^{(k)}\} \sim \{e^{(m)}\}$ because otherwise the right-hand side would tend to zero.

It follows that *it may be assumed, without loss of generality, that all solutions* $\{e^{(k)}\}$ *are, in fact, minimum solutions;* for we may, if necessary, omit all solutions which are not.

Next, we are allowed to renumber the primes $p_1, \dots, p_s$, and to replace the infinite sequence of minimum solutions $\{e^{(k)}\}$ by any infinite subsequence. There is then no restriction of generality in imposing the following further assumption. *There are two non-negative integers* r' *and* r'' *with* $r'+r'' > 0$ *such that, for every solution* $\{e^{(k)}\}$,

$$e_j^{(k)} \geq 0 \text{ if } j = 1, 2, \dots, r'; \quad e_j^{(k)} \leq 0 \text{ if } j = r'+1, r'+2, \dots, r'+r'' .$$

This implies that, for every k, $P^{(k)}$ cannot have prime factors distinct from $p_1, \dots, p_{r'}$, and $Q^{(k)}$ cannot have prime factors distinct from $p_{r'+1}, \dots, p_{r'+r''}$.

Finally put

$$Q^{(k)*} = e_0^{(k)} Q^{(k)}, \qquad H^{(k)} = \max(P^{(k)}, |Q^{(k)*}|).$$

It is clear that $H^{(k)}$ tends to infinity with k, and that

$$(4): \qquad 0 < \left| \frac{P^{(k)}}{Q^{(k)*}} - \xi \right|^{*} < \frac{e^{-\epsilon E^{(k)}}}{|e_0^{(k)}|} \leqslant 1.$$

By the construction, $P^{(k)}$ and $Q^{(k)}$ are relatively prime; it follows then from (3) that also

$$(5): \qquad (P^{(k)}, Q^{(k)*}) = 1.$$

By what has just been said about the prime factors of $P^{(k)}$ and $Q^{(k)}$,

$$|P^{(k)}| \prod_{j=1}^{r'} |P^{(k)}|_{p_j} = 1, \qquad |Q^{(k)}| \prod_{j=r'+1}^{r'+r''} |Q^{(k)}|_{p_j} = 1.$$

It is further obvious that

$$0 < \prod_{j=r'+1}^{r'+r''} |e_0^{(k)}|_{p_j} \leqslant 1 .$$

Therefore

$$0 < |Q^{(k)}| \prod_{j=r'+1}^{r'+r''} |Q^{(k)*}|_{p_j} \leqslant 1 ,$$

whence

$$(6): \; 0 < \left| \frac{P^{(k)}}{Q^{(k)*}} - \xi \right|^{*} \cdot \prod_{j=1}^{r'} |P^{(k)}|_{p_j} \cdot \prod_{j=r'+1}^{r'+r''} |Q^{(k)*}|_{p_j} < \frac{e^{-\epsilon E^{(k)}}}{|e_0^{(k)} P^{(k)} Q^{(k)}|} = \frac{e^{-\epsilon E^{(k)}}}{|P^{(k)} Q^{(k)*}|}$$

Now $\xi \neq 0$, and it follows from (4) that the fractions $\frac{P^{(k)}}{Q^{(k)*}}$ tend to ξ. Therefore $P^{(k)}$ and $Q^{(k)*}$ have the same order of magnitude as $H^{(k)}$. There exists then a positive constant c such that, for all k,

$$|P^{(k)} Q^{(k)*}| \geqslant c H^{(k)2}.$$

On the other hand, the definitions of $P^{(k)}, Q^{(k)*}$, and $H^{(k)}$ imply that

$$H^{(k)} \leqslant p_0^{sE^{(k)}}$$

where again p_0 denotes the largest of the primes $p_1, \ldots, p_s$. Hence

$$e^{-\epsilon E^{(k)}} \leqslant H^{(k)-\rho}$$

where

$$\rho = \frac{\epsilon}{s \log p_0} ,$$

whence, by (6),

$$0 < \left| \frac{P^{(k)}}{Q^{(k)*}} - \xi \right|^{*} \cdot \prod_{j=1}^{r'} |P^{(k)}|_{p_j} \cdot \prod_{j=r'+1}^{r'+r''} |Q^{(k)}|_{p_j} < K_1 H^{(k)-\tau} .$$

Here, for shortness,

$$K_1 = \frac{1}{c}, \quad \tau = 2+\rho > 2 .$$

On applying now Theorem (2,I) with $r=0$, we obtain a contradiction. This concludes the proof.

By way of example, let $\xi \neq 0$ be a real algebraic number; let u and v be two integers such that

$$u > v \geq 2, \quad (u,v) = 1,$$

and let $\epsilon > 0$ be an arbitrarily small positive constant. From Theorem 1 it follows immediately that there can be at most finitely many pairs of integers $\{e_0, e_1\}$ with $e_0 \neq 0$, $e_1 \geq 1$ such that

$$0 < \left| \left(\frac{u}{v}\right)^{e_1} - e_0 \xi \right| < e^{-\epsilon e_1} .$$

The special case $\xi = 1$ means that the fractional parts of the integral powers of $\frac{u}{v}$ cannot be too small. This result is useful in the theory of Waring's problem. For it allows to prove, for all sufficiently large positive integers n, that *every positive integer is the sum of not more than*

$$2^n + \left[\left(\frac{3}{2}\right)^n\right] - 2$$

n-th *powers*

$$0^n, 1^n, 2^n, 3^n, \ldots,$$

where certain positive integers do, in fact, require this number of n-th powers[1].

4. The equation $P^{(k)} + Q^{(k)} + R^{(k)} = 0$.

This section deals with a general theorem on triplets of integers.

Theorem 2: *Let* c *and* ν *be two positive constants, and let*

$$p_1, \ldots, p_r, p_{r+1}, \ldots, p_{r+r'}, p_{r+r'+1}, \ldots, p_{r+r'+r'}$$

be finitely many distinct primes. Denote by Σ *an infinite sequence of distinct triplets*

$$\{P^{(k)}, Q^{(k)}, R^{(k)}\} \qquad (k = 1,2,3,\ldots)$$

where $P^{(k)}, Q^{(k)}$, *and* $R^{(k)}$ *are integers as follows,*

[1] See Hardy and Wright, Theory of Numbers (Oxford 1954, 3rd ed.), 335-337; K. Mahler, Mathematika 4 (1957), 122-124.

$$P^{(k)} \neq 0,\ Q^{(k)} \neq 0,\ R^{(k)} \neq 0,\ P^{(k)} + Q^{(k)} + R^{(k)} = 0,$$

$$(P^{(k)}, Q^{(k)}) = (P^{(k)}, R^{(k)}) = (Q^{(k)}, R^{(k)}) = 1.$$

Put

$$H^{(k)} = \max(P^{(k)}|, |Q^{(k)}|, |R^{(k)}|),$$

and write $P^{(k)}$, $Q^{(k)}$, *and* $R^{(k)}$ *as products of integers,*

$$P^{(k)} = P_1^{(k)}P_2^{(k)}, \qquad Q^{(k)} = Q_1^{(k)}Q_2^{(k)}, \qquad R^{(k)} = R_1^{(k)}R_2^{(k)},$$

where $P_1^{(k)}$ *has no prime factors distinct from* $p_{r+1},\ldots,p_{r+r'}$, $Q_1^{(k)}$ *has no prime factors distinct from* $p_{r+r'+1},\ldots,p_{r+r'+r''}$, *and* $R_1^{(k)}$ *has no prime factors distinct from* $p_1,\ldots,p_r$. *If*

$$|P_2^{(k)}Q_2^{(k)}R_2^{(k)}| \leqslant c\,H^{(k)\nu} \qquad (k = 1,2,3,\ldots,),$$

then $\nu \geqslant 1$.

Proof: For each k, either

$$(7):\qquad |P^{(k)}| \geqslant |Q^{(k)}| \geqslant |R^{(k)}|,$$

or one of the five inequalities obtained from (7) by permuting $P^{(k)}$, $Q^{(k)}$, $R^{(k)}$ is satisfied. Since we may replace Σ by any infinite subsequence, and since we are allowed to rename these three letters and, at the same time, the corresponding sets of primes, there is no loss of generality in assuming that, in fact, *the inequality* (7) *holds for all elements of* Σ.

Put now

$$\kappa^{(k)} = \frac{P^{(k)}}{Q^{(k)}} \qquad \text{and} \qquad \xi = \xi_1 = \ldots = \xi_r = -1.$$

and, just as in the last chapter, write

$$\Phi(\kappa^{(k)}) = |\kappa^{(k)} - \xi|^{*} \cdot \prod_{j=1}^{r} |\kappa^{(k)} - \xi_j|_{p_j}^{*} \cdot \prod_{j=r+1}^{r+r'} |P^{(k)}|_{p_j} \cdot \prod_{j=r+r'+1}^{r+r'+r''} |Q^{(k)}|_{p_j}.$$

Then, by (7),

$$|\kappa^{(k)} - \xi|^{*} = \left|\frac{R^{(k)}}{Q^{(k)}}\right|^{*} = \left|\frac{R^{(k)}}{Q^{(k)}}\right|.$$

Further also

$$|\kappa^{(k)} - \xi_j|_{p_j}^{*} = \left|\frac{R^{(k)}}{Q^{(k)}}\right|_{p_j}^{*} = |R^{(k)}|_{p_j} \qquad (j = 1,2,\ldots,r).$$

For either p_j is a divisor of $Q^{(k)}$, and then it is prime to $R^{(k)}$ and so

$$\left|\frac{R^{(k)}}{Q^{(k)}}\right|_{p_j} > 1, \quad \left|\frac{R^{(k)}}{Q^{(k)}}\right|^*_{p_j} = |R^{(k)}|_{p_j} = 1;$$

or p_j is prime to $Q^{(k)}$, and then

$$\left|\frac{R^{(k)}}{Q^{(k)}}\right|^*_{p_j} = |R^{(k)}|^*_{p_j} = |R^{(k)}|_{p_j} .$$

Therefore

$$\prod_{j=1}^{r} |\kappa^{(k)} - \xi_j|^*_{p_j} = \prod_{j=1}^{r} |R^{(k)}|_{p_j} ,$$

and it follows that

$$\Phi(\kappa^{(k)}) = \left|\frac{R^{(k)}}{Q^{(k)}}\right| \cdot \prod_{j=1}^{r} |R^{(k)}|_{p_j} . \prod_{j=r+1}^{r+r'} |P^{(k)}|_{p_j} . \prod_{j=r+r'+1}^{r+r'+r''} |Q^{(k)}|_{p_j} .$$

Next, the hypothesis implies that, e.g.

$$\prod_{j=1}^{r} |R^{(k)}|_{p_j} = \prod_{j=1}^{r} (|R_1^{(k)}|_{p_j} . |R_2^{(k)}|_{p_j}) \leqslant \prod_{j=1}^{r} |R_1^{(k)}|_{p_j} = |R_1^{(k)}|^{-1} = \left|\frac{R_2^{(k)}}{R^{(k)}}\right| ,$$

and, in the same way,

$$\prod_{j=r+1}^{r+r'} |P^{(k)}|_{p_j} \leqslant \left|\frac{P_2^{(k)}}{P^{(k)}}\right| , \qquad \prod_{j=r+r'+1}^{r+r'+r''} |Q^{(k)}|_{p_j} \leqslant \left|\frac{Q_2^{(k)}}{Q^{(k)}}\right| .$$

Therefore

$$\Phi(\kappa^{(k)}) \leqslant \left|\frac{R^{(k)}}{Q^{(k)}}\right| . \left|\frac{P_2^{(k)} Q_2^{(k)} R_2^{(k)}}{P^{(k)} Q^{(k)} R^{(k)}}\right| \leqslant \frac{c\, H^{(k)\nu}}{P^{(k)} Q^{(k)2}} .$$

Finally, by (7),

$$H^{(k)} = |P^{(k)}| = |Q^{(k)} + R^{(k)}| \leqslant |Q^{(k)}| + |R^{(k)}| \leqslant 2|Q^{(k)}| ,$$

so that

$$|Q^{(k)}| \geqslant \frac{1}{2} H^{(k)} ,$$

and hence

$$\Phi(\kappa^{(k)}) \leqslant 4c\, H^{(k)\nu-3} .$$

It follows then from Theorem (2,I) that

$$3 - \nu \leqslant 2, \quad \nu \geqslant 1,$$

whence the assertion.

It is again not difficult to construct examples which show that the assertion $\nu \geqslant 1$ of the theorem is best-possible.

The Theorem 2 is a special case of the more general

Theorem 3: *Let*

$$F(x,y) = F_0x^f + F_1x^{f-1}y + \dots + F_fy^f, \quad \text{where } f \geqslant 1,\ F_0 \neq 0,\ F_f \neq 0,$$

be a binary form with integral coefficients which has no multiple factors. Let

$$p_1, \dots, p_r, p_{r+1}, \dots, p_{r+r'}, p_{r+r'+1}, \dots, p_{r+r'+r''}$$

be finitely many distinct primes, and let c and ω *be two positive constants. Finally let* Σ *be an infinite sequence of distinct pairs of integers* $\{P^{(k)}, Q^{(k)}\}$ *such that, for all* k,

$$P^{(k)} \neq 0,\ Q^{(k)} \neq 0,\ (P^{(k)}, Q^{(k)}) = 1,\ H^{(k)} = \max(|P^{(k)}|, |Q^{(k)}|)$$

and

$$|F(P^{(k)},Q^{(k)})| \cdot \prod_{j=1}^{r} |F(P^{(k)},Q^{(k)})|_{p_j} \cdot \prod_{j=r+1}^{r+r'} |P^{(k)}|_{p_j} \cdot \prod_{j=r+r'+1}^{r+r'+r''} |Q^{(k)}|_{p_j} \leqslant c H^{(k)\omega}.$$

Then $\omega \geqslant f-2$.

The reader should have no difficulty in deducing Theorem 2 from the special case $F(x,y) = x+y$ of Theorem 3, and in proving Theorem 3 by means of Theorem (2,II).

5. The approximation by rational integers.

The two Approximation Theorems proved in Chapters 7 and 8 have analogues relating to the approximation of *integral* g-adic numbers by rational *integers*. There are again two such theorems, each one having two equivalent forms. These theorems are as follows.

Theorem (4,I): *Let* $\Xi \leftrightarrow (\xi_1, \dots, \xi_r)$, *where* $\xi_1 \neq 0, \dots, \xi_r \neq 0$, *be an algebraic* g*-adic integer. Let* $g' \geqslant 2$ *be a positive integer, and let* c_2, c_3, σ, *and* λ *be four real constants such that*

$$c_2 > 0,\ c_3 > 0,\ \sigma > 0,\ 0 \leqslant \lambda \leqslant 1.$$

If there exists an infinite sequence $\Sigma = \{p^{(1)}, p^{(2)}, p^{(3)}, \dots\}$ *of distinct positive integers such that, for all* k,

$$|\Xi - p^{(k)}|_g \leqslant c_2 p^{(k)-\sigma}, \quad |p^{(k)}|_{g'} \leqslant c_3 p^{(k)\lambda-1},$$

then $\sigma \leqslant \lambda$.

Theorem (4,II): *Let* $F(x)$ *be a polynomial with integral coefficients which does not vanish at* $x=0$ *and has no multiple factors. Let* $g \geqslant 2$ *and* $g' \geqslant 2$ *be two positive integers, and let* c_2', c_3, σ, *and* λ *be four real constants* *such that*

$$c_2' > 0,\ c_3 > 0,\ \sigma > 0,\ 0 \leq \lambda \leq 1.$$

If there exists an infinite sequence $\Sigma = \{P^{(1)}, P^{(2)}, P^{(3)}, \ldots\}$ *of distinct positive integers such that, for all* k,

$$|F(P^{(k)})|_g \leq c_2' P^{(k)-\sigma}, \quad |P^{(k)}|_{g'} \leq c_3 P^{(k)\lambda-1},$$

then $\sigma \leq \lambda$.

Theorem (5,I): *Let* $p_1, \ldots, p_r, p_{r+1}, \ldots, p_{r+r'}$ *be finitely many distinct primes, and let* $\xi_1 \neq 0, \ldots, \xi_r \neq 0$ *be an algebraic* p_1*-adic integer, etc., an algebraic* p_r*-adic integer, respectively. Let* K_1 *and* τ *be two positive constants. If there exists an infinite sequence* $\Sigma = \{P^{(1)}, P^{(2)}, P^{(3)}, \ldots\}$ *of distinct positive integers such that, for all* k,

$$\prod_{j=1}^{r} |P^{(k)} - \xi_j|_{p_j} \cdot \prod_{j=r+1}^{r+r'} |P^{(k)}|_{p_j} \leq K_1 P^{(k)-\tau},$$

then $\tau \leq 1$.

Theorem (5,II): *Let* $p_1, \ldots, p_r, p_{r+1}, \ldots, p_{r+r'}$ *be finitely many distinct primes, and let* $F_1(x), \ldots, F_r(x)$ *be* r *polynomials with integral coefficients which do not vanish at* x=0 *and have no multiple factors. Let* K_2 *and* τ *be two positive constants. If there exists an infinite sequence* $\Sigma = \{P^{(1)}, P^{(2)}, P^{(3)}, \ldots\}$ *of distinct positive integers such that, for all* k,

$$\prod_{j=1}^{r} |F_j(P^{(k)})|_{p_j} \cdot \prod_{j=r+1}^{r+r'} |P^{(k)}|_{p_j} \leq K_2 P^{(k)-\tau},$$

then $\tau \leq 1$.

A discussion similar to that in Chapters 7 and 8 allows again to show that these four theorems are equivalent, in the sense that each implies the other three.

It suffices then to prove Theorem (4,I). This is done by essentially repeating those constructions and estimates of §§2-8 of Chapter 7 that led to the case d=2 of the Main Lemma. One assumes that the assertion is false and that, say,

$$\sigma = \lambda + 4\epsilon \quad \text{where} \quad 0 < \epsilon \leq \frac{1}{5}.$$

The proof then procedes with the values

$$\kappa^{(k)} = \frac{P^{(k)}}{1}, \ Q^{(k)} = 1, \ H^{(k)} = P^{(k)}$$

and hence with the values

$$\kappa_h = \frac{P_h}{1}, \ Q_h = 1, \ H_h = P_h \qquad (h = 1,2,\ldots, m).$$

Here the parameters $m, s, t, r_1, \ldots, r_m$ are selected just as in §2 of Chapter

7, and the polynomial $A(x_1,\dots,x_m)$ is defined as in §3. In particular, the inequality (14) of §2 takes the form,

$$P_1^{r_1 \sum_{h=1}^{m} \frac{k_h}{r_h}} \leq P_1^{k_1} \dots P_m^{k_m} \leq P_1^{(1+\epsilon) r_1 \sum_{h=1}^{m} \frac{k_h}{r_h}} .$$

The proof now depends on upper and lower estimates for the integer

$$A_{(l)} = \frac{N(l)}{1} = A_{l_1 \dots l_m}(\kappa_1,\dots,\kappa_m) \neq 0,$$

which has the explicit value

$$A_{(l)} = \sum_{i_1=0}^{r_1} \dots \sum_{i_m=0}^{r_m} a_{i_1 \dots i_m} \binom{i_1}{l_1} \dots \binom{i_m}{l_m} P_1^{i_1-l_1} \dots P_m^{i_m-l_m} .$$

Here, by the upper bound for $a_{i_1 \dots i_m}$,

$$\sum_{i_1=0}^{r_1} \dots \sum_{i_m=0}^{r_m} |a_{i_1 \dots i_m}| \binom{i_1}{l_1} \dots \binom{i_m}{l_m} \leq 5(4c)^{r_1+\dots+r_m} \sum_{i_1=0}^{r_1} \dots \sum_{i_m=0}^{r_m} 2^{i_1+\dots+i_m} \leq$$

$$\leq 5(4c)^{mr_1} (2^{r_1+1}-1) \dots (2^{r_m+1}-1) < 5(4c)^{mr_1} (2^{2r_1})^m = 5(16c)^{mr_1} \leq (80c)^{mr_1} .$$

Hence it follows that, in the notation of Chapter 7,

$$|A_{(l)}| \leq (80c)^{mr_1} \max_{(i)\in I} P_1^{i_1-l_1} \dots P_m^{i_m-l_m} \leq (80c)^{mr_1} \max_{(i)\in I} P_1^{(1+\epsilon) r_1 \sum_{h=1}^{m} \frac{i_h-l_h}{r_h}} ,$$

and therefore

$$|A_{(l)}| \leq (80c)^{mr_1} P_1^{(1+\epsilon) r_1 S_2} .$$

The lower estimate for the case d=2 of $N(l)$, obtained in §7 of Chapter 7, still remains valid; but since $N(l)=A_{(l)}$, it takes the form

$$|A_{(l)}| \geq c_{12}^{-mr_1} P_1^{(1-\lambda+\sigma) r_1 S_1} .$$

On combining these two inequalities, we find that

$$P_1^{E} \leq (80cc_{12})^{m},$$

where we have put

$$E = (1-\lambda+\sigma)S_1 - (1+\epsilon)S_2 .$$

In explicit form,

$$E = (1-\lambda+\sigma)\{\tfrac{1}{2}(m-s) - \Lambda\} - (1+\epsilon)\{\tfrac{1}{2}(m+s) - \Lambda\} =$$

$$= \frac{1}{2}(\sigma-\lambda-\epsilon)m - \frac{1}{2}(\sigma-\lambda+\epsilon+2)s - (\sigma-\lambda-\epsilon)\Lambda$$

Further, just as in Chapter 7,

$$s = \frac{\epsilon m}{6}, \quad 0 \leqslant \Lambda \leqslant \frac{\epsilon m}{6}.$$

It follows then that

$$E = \frac{1}{2}.3\epsilon.m - \frac{1}{2}(5\epsilon+2)s - 3\epsilon.\Lambda \geqslant \frac{3\epsilon m}{2} - \frac{3}{2}\frac{\epsilon m}{6} - \frac{3}{5}\frac{\epsilon m}{6} > \epsilon m .$$

Hence, if P_1 was chosen so large that

$$P_1 \geqslant (80cc_{12})^{\frac{1}{\epsilon}} ,$$

a contradiction arises, proving the assertion.

6. An example.

By way of example, let $p=p_1$ be an odd prime, and let a denote one of the $p-2$ integers $2, 3, \ldots, p-1$. Put

$$P^{(k)} = a^{p^{k-1}} \qquad (k = 1,2,3,\ldots) .$$

It follows from Euler's theorem that

$$a^{\phi(p^k)} = a^{p^k - p^{k-1}} \equiv 1 (\mathrm{mod}\ p^k)$$

and hence

$$P^{(k+1)} \equiv P^{(k)} (\mathrm{mod}\ p^k) ,$$

or, what is the same,

(8): $$|P^{(k+1)} - P^{(k)}|_p \leqslant p^{-k} .$$

In particular,

$$P^{(k)} \equiv P^{(k-1)} \equiv \ldots \equiv P^{(2)} \equiv P^{(1)} = a (\mathrm{mod}\ p)$$

and therefore

(9) $$|P^{(k)} - a|_p \leqslant \frac{1}{p} .$$

By (8), the sequence $\{P^{(1)}, P^{(2)}, P^{(3)}, \ldots\}$ is a p-adic fundamental sequence; let

$$\alpha = \lim_{k\to\infty} P^{(k)} (p)$$

be its limit. Since $P^{(k+1)} = P^{(k)p}$, evidently

$$\alpha = \lim_{k\to\infty} P^{(k+1)} = \left(\lim_{k\to\infty} P^{(k)} \right)^p = \alpha^p (p),$$

so that α is a root of the equation

$$x^p-x = x(x-1)(x^{p-2}+x^{p-3}+\ldots+x+1) = 0.$$

Now a is distinct from 0 and 1, and by (9)

$$|\alpha-a|_p = \lim_{k\to\infty} |P^{(k)}-a|_p \leqslant \frac{1}{p}.$$

Hence $\alpha(\alpha-1)\neq 0$, and so α satisfies the equation

$$x^{p-2}+x^{p-3}+\ldots+x+1 = 0.$$

Thus α is an algebraic p-adic integer distinct from zero. It has the following further property.

If ϵ is an arbitrarily small positive number, then there are at most finitely many positive integers k *such that*

$$(10): \qquad |a^{p^k}-\alpha|_p \leqslant a^{-\epsilon p^k}.$$

For put r=1, $\xi_1=\alpha$, and denote by $p_{r+1},\ldots,p_{r+r'}$ all the distinct prime factors of a. It follows that

$$\prod_{j=r+1}^{r+r'} |P^{(k)}|_{p_j} = P^{(k)-1}.$$

Therefore, by (10),

$$|P^{(k)}-\alpha|_p \prod_{j=r+1}^{r+r'} |P^{(k)}|_{p_j} \leqslant P^{(k)-\tau}, \quad \text{where } \tau = 1+\epsilon > 1,$$

and so the assertion is an immediate consequence of Theorem (5,I).