Chapter 2

THE p-ADIC, g-ADIC, AND g*-ADIC SERIES

Historically, K. Hensel was led to his p-adic and g-adic numbers by considerations of analogy to function fields.

Let Σ be the complex number field, x an indeterminate, and $K = \Sigma(x)$ a simple transcendental extension of Σ; let further $w(a)$ be any valuation or pseudo-valuation of K with the *property* C, i.e., such that

$$w(c) = w_0(c) \text{ if } c \epsilon \Sigma,$$

where $w_0(a)$ denotes the trivial valuation defined in §1 of Chapter 1. It can be proved that every valuation with the property C must be equivalent to one of the valuations

$$w_0(a), \ ||a||, \ ||a||_{p_r}$$

introduced in § 3 of Chapter 1; however, now every "prime" p has the special form $p=x-c$ where $c \epsilon \Sigma$ because Σ is algebraically closed. One can further show that every pseudo-valuation with the property C either is equivalent to one of these valuations, or it is equivalent to a pseudo-valuation of one of the two forms

$$w_1(a) = \max(||a||_{p_1}, \ldots, ||a||_{p_r}) \quad \text{and} \quad w_2(a) = \max(||a||, ||a||_{p_1}, \ldots, ||a||_{p_r}).$$

Here

$$p_1 = x - c_1, \ldots, p_r = x - c_r, \text{ where } c_h \neq c_k \text{ if } h \neq k,$$

are finitely many distinct "primes", and we have $r \geq 2$ in the case of $w_1(a)$ and $r \geq 1$ in that of $w_2(a)$. The position is thus analogous to that mentioned in § 14 of Chapter 1 for the rational field Γ, with $||a||, ||a||_p, w_1(a), w_2(a)$ corresponding to $|a|, |a|_p, |a|_g, |a|_{g^*}$, respectively, There is, however, the difference that all these valuations and pseudo-valuations of K are *Non-Archimedean.*

It is not difficult to prove that the completion of K with respect to $||a||$ is the field of all *formal* series

$$c_f \left(\frac{1}{x}\right)^f + c_{f+1} \left(\frac{1}{x}\right)^{f+1} + c_{f+2} \left(\frac{1}{x}\right)^{f+2} + \ldots$$

while that of K with respect to $||a||_p$, where $p=x-c$, is the field of all *formal* series

$$c_f(x-c)^f + c_{f+1}(x-c)^{f+1} + c_{f+2}(x-c)^{f+2} + \ldots .$$

In both cases f may be any rational integer, and the coefficients c_m may be arbitrary elements of Σ. The convergence of the series follows from the results in § 17 of Chapter 1 because

$$||\tfrac{1}{x}|| = \theta < 1, \ ||c_m|| \leq 1, \text{ and } ||x-c||_p = \theta < 1, \ ||c_m||_p \leq 1,$$

respectively, and hence

$$\lim_{m\to\infty} ||c_m \left(\frac{1}{x}\right)^m|| = 0, \qquad \lim_{m\to\infty} ||c_m(x-c)^m||_p = 0.$$

In both cases the constant field Σ has the algebraic property of being the residue class field K/x and K/x-c, respectively.

Similar, but slightly more complicated developments hold also for the completions of K with respect to $w_1(a)$ and $w_2(a)$, but there is no need to go into details.

Consider now the valuation $|a|_p$ of Γ and the corresponding p-adic completion P_p of Γ. We have

$$|p|_p = \frac{1}{p} < 1, \text{ and } |c|_p \leq 1 \text{ for all rational integers } c.$$

It follows that every formal series

$$c_f p^f + c_{f+1}p^{f+1} + c_{f+2}p^{f+2} + \ldots$$

where f and all the coefficients c_m are rational integers, converges with respect to $|a|_p$; for the valuation $|a|_p$ is Non-Archimedean, and

$$\lim_{m\to\infty} |c_m p^m|_p = 0.$$

It will be proved in this chapter that every element of P_p can be written in many ways as a series of this kind, but that there is one and only one series in which the coefficients assume only values in the finite set $\{0,1,\ldots, p-1\}$.

When Hensel discovered the p-adic numbers towards the end of last century, there was not yet any general field theory or theory of valuations. He defined his numbers by the series and by the rules for computing with them. In this work he followed the analogy to the Laurent series

$$c_f\left(\frac{1}{x}\right)^f + c_{f+1}\left(\frac{1}{x}\right)^{f+1} + c_{f+2}\left(\frac{1}{x}\right)^{f+2} + \ldots$$

or

$$c_f(x-c)^f + c_{f+1}(x-c)^{f+1} + c_{f+2}(x-2)^{f+2} + \ldots$$

for an analytic function in the neighbourhood of a pole, either at $x=\infty$ or at a finite point x=c. Such series are convergent in the sense of complex analysis rather than with respect to the valuations $||a||$ or $||a||_p$; but even in function theory the latter kind of convergence plays a big role in connection with the orders of poles and zeros.

The investigations of this chapter are concerned only with the p-adic, g-adic, and g*-adic numbers. However, the method is much more general, and it can in particular be used to prove the earlier assertions about the completions of K with respect to $||a||$ and $||a||_p$.

1. Notation.

In this and the later chapters the notation will be essentially the same as before. Always $p_1,\ldots, p_r$ denote finitely many distinct primes, and $g \geq 2$ denotes an integer with the factorisation

$$g = p_1^{e_1} \dots p_r^{e_r}$$

where $e_1, \dots, e_r$ are positive integers. The valuations $|a|$ and $|a|_p$, and the pseudo-valuations $|a|_g$ and $|a|_{g^*}$, are defined as in Chapter 1, and P, P_p, P_g, and P_{g^*} denote the corresponding completions of the rational field Γ; thus are the fields of the real and the p-adic numbers, and the rings of the g-adic and the g*-adic numbers, respectively. We shall in general use Latin letters for rational numbers, small Greek letters for real and p-adic numbers, and capital Greek letters for g-adic and g*-adic numbers.

If $A \leftrightarrow (\alpha_1, \dots, \alpha_r)$ is a g-adic number with the p_j-adic components α_j for j=1, 2,..., r, the g-adic value of A is equal to

$$|A|_g = \max\left(|\alpha_1|_{p_1}^{\frac{\log g}{e_1 \log p_1}}, \dots, |\alpha_r|_{p_r}^{\frac{\log g}{e_r \log p_r}} \right).$$

Similarly, if $A^* \leftrightarrow (\alpha, \alpha_1, \dots, \alpha_r)$ is a g*-adic number with the real component α and the α_j-adic components α_j for j=1, 2,..., r, the g*-adic value of A^* is given by

$$|A^*|_{g^*} = \max\left(|\alpha|, |\alpha_1|_{p_1}^{\frac{\log g}{e_1 \log p_1}}, \dots, |\alpha_r|_{p_r}^{\frac{\log g}{e_r \log p_r}} \right).$$

It will suffice to prove the first formula as the second formula may be obtained in the same way.

There exists a fundamental sequence $\{a_m\}$ in Γ satisfying

$$\lim_{m \to \infty} a_m = A \quad (|a|_g)$$

and hence also satisfying

$$\lim_{m \to \infty} a_m = \alpha_j (|a|_{p_j}) \qquad (j = 1,2,\dots,r).$$

These two limit formulae imply that

$$\lim_{m \to \infty} |a_m|_g = |A|_g \quad \text{and} \quad \lim_{m \to \infty} |a_m|_{p_j} = |\alpha_j|_{p_j} \quad (j = 1,2,\dots,r).$$

Now, by definition,

$$|a_m|_g = \max\left(|a_m|_{p_1}^{\frac{\log g}{e_1 \log p_1}}, \dots, |a_m|_{p_r}^{\frac{\log g}{e_r \log p_r}} \right),$$

and so the assertion follows immediately.

We note that

(I): $$|A^n|_g = (|A|_g)^n, \qquad |A^{*n}|_{g^*} = (|A^*|_{g^*})^n$$

for all $A \in P_g$ and $A^* \in P_{g^*}$ and all positive integers n; and that further

(II): $$|Ag^n|_g = |A|_g (|g|_g)^n = g^{-n} |A|_g$$

for all $A \in P_g$ and all rational integers n. These properties follow easily from the explicit expressions for $|A|_g$ and $|A^*|_{g^*}$, and from

$$|g|_g = g^{-1}, \ |g|_{p_1} = p_1^{-e_1}, \dots, \ |g|_{p_r} = p_r^{-e_r}.$$

They are special cases of the properties (I) and (II) in § 4 of Chapter 1.

Here and later, we have continuously to deal with limits

$$\lim_{m\to\infty} \ldots (w)$$

where w(a) stands for one of

$$|a|,\ |a|_p,\ |a|_g,\ \text{or}\ |a|_{g^*}.$$

In order to shorten the formulae, we shall always omit the sign $|a|$ of the absolute value and write

$$\lim_{m\to\infty} \ldots$$

when dealing with real limits. We further shall replace

$$\lim_{m\to\infty} \ldots (|a|_p) \quad \text{by} \quad \lim_{m\to\infty} \ldots (p),$$

$$\lim_{m\to\infty} \ldots (|a|_g) \quad \text{by} \quad \lim_{m\to\infty} \ldots (g),$$

and

$$\lim_{m\to\infty} \ldots (|a|_{g^*}) \quad \text{by} \quad \lim_{m\to\infty} \ldots (g^*),$$

respectively. This agrees with Hensel's own notation.

2. The ring I_g and the ideal $\mathfrak{g}$.

Denote by I_g and $\mathfrak{g}$ the two sets of all rational numbers satisfying

$$|a|_g \leqslant 1$$

and

$$|a|_g \leqslant \frac{1}{g},$$

respectively; thus $\mathfrak{g}$ is a subset of I_g, and I_g is a subset of Γ.

The set I_g *is a ring.* For $|a|_g$ is a Non-Archimedean pseudo-valuation. It follows that if a and b are in I_g and hence

$$|a|_g \leqslant 1,\ |b|_g \leqslant 1,$$

then

$$|a\mp b|_g \leqslant \max(|a|_g, |b|_g) \leqslant 1,\ |ab|_g \leqslant |a|_g|b|_g \leqslant 1,$$

and so a+b, a-b, and ab likewise belong to I_g.

The set $\mathfrak{g}$ *is an ideal of* I_g. For let a and b be in $\mathfrak{g}$, and let c be any element of I_g, so that

$$|a|_g \leqslant \frac{1}{g},\ \ |b|_g \leqslant \frac{1}{g},\ \ |c|_g \leqslant 1.$$

Then

$$|a\mp b|_g \leqslant \max(|a|_g,\ |b|_g) \leqslant \frac{1}{g},\ |ac|_g \leqslant |a|_g|c|_g \leqslant \frac{1}{g},$$

and hence a+b, a-b, and ac are likewise in $\mathfrak{g}$.

By the identity (II),

$$\left|\frac{a}{g}\right|_g = g|a|_g.$$

Hence it follows that

$$a \textit{ belongs to } \mathfrak{g} \textit{ if and only if } \frac{a}{g} \textit{ belongs to } I_g.$$

Thus $\mathfrak{g}$ consists of all multiples a=a'g where $a' \in I_g$. In the language of ideal theory, $\mathfrak{g}$ is the principal ideal $\mathfrak{g}=(g)$ of I_g.

The elements of I_g and $\mathfrak{g}$ may also be characterised as follows. Write the rational number a as a quotient $a = \frac{P}{Q}$ of two rational integers P and $Q \neq 0$ that are relatively prime. Then

$$a \textit{ belongs to } I_g \textit{ if and only if } (g, Q) = 1, \text{ and}$$

$$a \textit{ belongs to } \mathfrak{g} \textit{ if and only if } g|P, (g, Q) = 1.$$

The proof follows easily from the definition of $|a|_g$.

3. The residue class ring $I_g/\mathfrak{g}$.

If a and b are two elements of I_g such that a-b lies in $\mathfrak{g}$, we write

$$a \equiv b(\mathfrak{g}).$$

From the ideal property of $\mathfrak{g}$ one deduces easily that this is an *equivalence relation:*

$$a \equiv a(\mathfrak{g});$$

$$\text{if } a \equiv b(\mathfrak{g}), \text{ then } b \equiv a(\mathfrak{g});$$

$$\text{if } a \equiv b(\mathfrak{g}) \text{ and } b \equiv c(\mathfrak{g}), \text{ then } a \equiv c(\mathfrak{g}).$$

One can then subdivide I_g into classes $\mathfrak{g}+a$ where $\mathfrak{g}+a$ consists of all elements a' of I_g such that $a' \equiv a(\mathfrak{g})$. Two such classes are either *disjoint,* or they are *identical.*

Denote by $I_g/\mathfrak{g}$ the set of all these classes. It is again easily proved that $I_g/\mathfrak{g}$ becomes a ring if the sum and the product of any two classes $\mathfrak{g}+a$ and $\mathfrak{g}+b$ are defined by

$$(\mathfrak{g}+a) + (\mathfrak{g}+b) = \mathfrak{g} + (a+b), \quad (\mathfrak{g}+a) \cdot (\mathfrak{g}+b) = \mathfrak{g} + ab.$$

The proof may be omitted, as this is a particular case of a well-known theorem and since similar examples have already occurred.

Consider now an arbitrary element $\mathfrak{g}+c$ of $I_g/\mathfrak{g}$. If c is written as the quotient $c = \frac{R}{S}$ of two integers R and $S \neq 0$ that are relatively prime, then

$$(g, S) = 1$$

since $c \in I_g$. It follows that the elementary congruence

$$R \equiv aS \pmod{g}$$

has integral solutions a. If $a=a_0$ is one of these, the general solution has the form

$$a = a_0 + gk$$

where k is an arbitrary integer. There is then, in particular, a unique integral solution a satisfying

$$0 \leqslant a \leqslant g-1.$$

To this solution a there exists a further integer l such that

$$R - aS = gl$$

and hence that

$$c = \frac{R}{S} = a + g\frac{l}{S}.$$

Evidently

$$\frac{l}{S} \epsilon I_g \quad \text{and} \quad g\frac{l}{S} \epsilon \mathfrak{g}$$

and therefore

$$a \equiv c(\mathfrak{g}).$$

This relation implies further that the class $\mathfrak{g}+a$ is identical with the class $\mathfrak{g}+c$.

We have then the result that *every class in* $I_g/\mathfrak{g}$ *is of the form*

$$\mathfrak{g}+a, \textit{ where } a \textit{ is one of the integers } 0, 1,..., g-1.$$

These g *classes are all distinct.* For if a and a' are integers such that $0 \leqslant a < a' \leqslant g-1$, then a'-a is not devisible by g, hence

$$a \not\equiv a'(\mathfrak{g}).$$

This means that the two classes $\mathfrak{g}+a$ and $\mathfrak{g}+a'$ are distinct.

We have thus proved that *the ring* $I_g/\mathfrak{g}$ *has exactly* g *elements*

$$\mathfrak{g},\ \mathfrak{g}+1,...,\ \mathfrak{g}+(g-1).$$

4. Systems of representatives.

A set

$$M = \{A_0, A_1,..., A_{g-1}\}$$

of g rational numbers is said to be a system of representatives (viz., of the classes $\mathfrak{g}+a$ in $I_g/\mathfrak{g}$) if $A_0, A_1,..., A_{g-1}$ lie in I_g and if

$$A_0 \equiv 0(\mathfrak{g}),\ A_1 \equiv 1(\mathfrak{g}),...,\ A_{g-1} \equiv g-1(\mathfrak{g}).$$

It follows that

$$\mathfrak{g}+A_0,\ \mathfrak{g}+A_1,...,\ \mathfrak{g}+A_{g-1}$$

form again a full set of elements of $I_g/\mathfrak{g}$.

Such systems of representatives have the following property.

If A is any g-adic number satisfying

$$|A|_g \leq 1,$$

and if $M = \{A_0, A_1, \ldots, A_{g-1}\}$ is an arbitrary system of representatives, then there is a unique element A of M such that

$$|A - A|_g \leq \frac{1}{g} \quad .$$

Proof: By the first chapter, Γ lies dense in the g-adic ring $\dot{P}_g$ and so contains a rational number c for which

$$|A-c|_g \leq \frac{1}{g}$$

and hence also

$$|c|_g = |A-(A-c)|_g \leq \max(|A|_g, |A-c|_g) \leq 1.$$

Therefore c lies in I_g and so belongs to a certain class $\mathfrak{g}+A$ where $A \epsilon M$. Further $A-c \epsilon \mathfrak{g}$, so that

$$|A-c|_g \leq \frac{1}{g}.$$

It follows that

$$|A-A|_g = |(A-c) - (A-c)|_g \leq \max(|A-c|_g, |A-c|_g) \leq \frac{1}{g} \quad .$$

If $A' \epsilon M$ also satisfies

$$|A-A'|_g \leq \frac{1}{g},$$

then

$$|A-A'|_g = |A-A') - (A-A)|_g \leq \max(|A-A'|_g, |A-A|_g) \leq \frac{1}{g},$$

so that $A \equiv A' (\mathfrak{g})$, whence $A=A'$.

5. Series for g-adic numbers.

Denote by $h \neq 0$ any fixed integer such that $(g, h) = 1$. It is easily verified that, for all g-adic numbers A and all integers m,

$$|A\left(\frac{g}{h}\right)^m|_g = g^{-m}|A|_g \quad \text{and in particular} \quad |\left(\frac{g}{h}\right)^m|_g = g^{-m}$$

because

$$|h|_g = |h|_{p_1} = \ldots = |h|_{p_r} = 1.$$

Let, for every integer m, a system of representatives

$$M^{(m)} = \{A_0^{(m)}, A_1^{(m)}, \ldots, A_{g-1}^{(m)}\}$$

be given; systems belonging to different m may be equal or distinct.

If A is an arbitrary g-adic number, denote by f any integer satisfying

the inequality

$$g^{-f} \geqslant |A|_g$$

and put

$$A^{(f)} = \left(\frac{g}{h}\right)^{-f} A,$$

so that

$$|A^{(f)}|_g \leqslant g^f |A|_g \leqslant 1.$$

By §4, there exists a unique $A^{(f)} \epsilon M^{(f)}$ such that

$$|A^{(f)} - A^{(f)}|_g \leqslant \frac{1}{g}.$$

Put

$$A^{(f+1)} = \left(\frac{g}{h}\right)^{-1} (A^{(f)} - A^{(f)});$$

then

$$A^{(f)} = A^{(f)} + \frac{g}{h} A^{(f+1)}, \quad |A^{(f+1)}|_g \leqslant g |A^{(f)} - A^{(f)}|_g \leqslant 1.$$

There again exists a unique $A^{(f+1)}$ of $M^{(f+1)}$ such that

$$|A^{(f+1)} - A^{(f+1)}|_g \leqslant \frac{1}{g}.$$

Put

$$A^{(f+2)} = \left(\frac{g}{h}\right)^{-1} (A^{(f+1)} - A^{(f+1)});$$

then

$$A^{(f+1)} = A^{(f+1)} + \frac{g}{h} A^{(f+2)}, \quad |A^{(f+2)}|_g \leqslant g |A^{(f+1)} - A^{(f+1)}|_g \leqslant 1.$$

In this manner, we may continue indefinitely, and we so obtain for every suffix $m \geqslant f$

(i): a g-adic number $A^{(m)}$ satisfying

$$|A^{(m)}|_g \leqslant 1, \qquad \text{and}$$

(ii): a unique element $A^{(m)}$ of $M^{(m)}$ such that

$$A^{(m)} = A^{(m)} + \frac{g}{h} A^{(m+1)}, \quad |A^{(m)} - A^{(m)}|_g \leqslant \frac{1}{g}.$$

It follows that, for all $m \geqslant f$,

$$A^{(f)} = A^{(f)} + \frac{g}{h} A^{(f+1)} + \left(\frac{g}{h}\right)^2 A^{(f+2)} + \ldots + \left(\frac{g}{h}\right)^{m-f-1} A^{(m-1)} + \left(\frac{g}{h}\right)^{m-f} A^{(m)}.$$

Here

$$\left|\left(\frac{g}{h}\right)^{m-f} A^{(m)}\right|_g \leqslant g^{-(m-f)},$$

whence

$$\lim_{m\to\infty} \left|\left(\frac{g}{h}\right)^{m-f} A^{(m)}\right|_g = 0.$$

Therefore $A^{(f)}$ can be written as the convergent infinite series

$$A^{(f)} = A^{(f)} + \frac{g}{h} A^{(f+1)} + \left(\frac{g}{h}\right)^2 A^{(f+2)} + \dots \ (g).$$

Assume there is a second series

$$A^{(f)} = a^{(f)} + \frac{g}{h} a^{(f+1)} + \left(\frac{g}{h}\right)^2 a^{(f+2)} + \dots \ (g)$$

for $A^{(f)}$ where likewise $a^{(m)} \epsilon M^{(m)}$ for all $m \geqslant f$ and, say,

$$a^{(f)} = A^{(f)},\ a^{(f+1)} = A^{(f+1)},\ \dots,\ a^{(m-1)} = A^{(m-1)},\ a^{(m)} \neq A^{(m)}.$$

On subtracting the two series for $A^{(f)}$,

$$(A^{(m)} - a^{(m)})\left(\frac{g}{h}\right)^m = -\sum_{n=m+1}^{\infty} (A^{(n)} - a^{(n)}) \left(\frac{g}{h}\right)^n (g);$$

here, on the left-hand side,

$$A^{(m)} \neq a^{(m)},\ \text{hence}\ A^{(m)} \not\equiv a^{(m)} (g),\ \text{and therefore}\ |A^{(m)} - a^{(m)}|_g > \frac{1}{g},$$

whence

$$\left|(A^{(m)} - a^{(m)}) \left(\frac{g}{h}\right)^m\right|_g > g^{-(m+1)}.$$

On the right-hand side, $A^{(n)}$ and $a^{(n)}$ belong for all $n \geqslant m$ to $M^{(n)}$, so that

$$|A^{(n)}|_g \leqslant 1,\ |a^{(n)}|_g \leqslant 1,\ \text{hence}\ |A^{(n)} - a^{(n)}|_g \leqslant 1,$$

and therefore

$$\left|-\sum_{n=m+1}^{\infty} (A^{(n)} - a^{(n)}) \left(\frac{g}{h}\right)^n\right|_g \leqslant \max_{n\geqslant m+1} |A^{(n)} - a^{(n)}|_g\, g^{-n} \leqslant g^{-(m+1)}.$$

This contradiction proves that the series for $A^{(f)}$ is unique.

Since $A = \left(\frac{g}{h}\right)^f A^{(f)}$, the following result has been obtained.

Let $h \not\equiv 0$ *be an integer prime to* g; *let* $M^{(m)}$ *for every integer* m *be a system of representatives; and let* A *be any* g*-adic number. Denote by* f *any integer satisfying* $g^{-f} \geqslant |A|_g$. *Then* A *can be written in a unique way as a convergent infinite series*

$$A = A^{(f)}\left(\frac{g}{h}\right)^f + A^{(f+1)}\left(\frac{g}{h}\right)^{f+1} + A^{(f+2)}\left(\frac{g}{h}\right)^{f+2} + \dots \ (g)$$

where $A^{(m)} \epsilon M^{(m)}$ *for all* $m \geq f$.

The series for A still depends on the choice of f, and entirely different series may be obtained for different values of f.

Assume, however, that all systems $M^{(m)}$ contain the number

$$A_0^{(m)} = 0.$$

If $A \neq 0$, denote by f' the integer satisfying

$$g^{-f'-1} < |A|_g \leq g^{-f'},$$

so that, necessarily, $f \leq f'$. The series for A corresponding to f now becomes

$$A = 0\cdot\left(\frac{g}{h}\right)^f + 0\cdot\left(\frac{g}{h}\right)^{f+1} + \dots + 0\cdot\left(\frac{g}{h}\right)^{f'-1} + A^{(f')}\left(\frac{g}{h}\right)^{f'} + \dots \ (g)$$

where

$$A^{(f')} \neq 0 \quad \text{and therefore} \quad |A|_g = g^{-f'}\,|A^{(f')}|_g.$$

In the excluded case $A = 0$ there are only the trivial series

$$0 = 0\cdot\left(\frac{g}{h}\right)^f + 0\cdot\left(\frac{g}{h}\right)^{f+1} + 0\cdot\left(\frac{g}{h}\right)^{f+2} + \dots \ (g).$$

Finally let all systems $M^{(m)}$ be identical with

$$M^{(m)} = \{0, 1, 2, \dots, g-1\}.$$

The result just proved now takes the following form.

Let $h \neq 0$ *be an integer prime to* g. *Every* g*-adic number can be written in a unique way as a convergent series*

$$A = A^{(f)}\left(\frac{g}{h}\right)^f + A^{(f+1)}\left(\frac{g}{h}\right)^{f+1} + A^{(f+2)}\left(\frac{g}{h}\right)^{f+2} + \dots \ (g)$$

where the coefficients $A^{(m)}$ *are numbers* 0, 1, 2,..., g-1 *as follows. If* $A = 0$, *all these coefficients vanish; if* $A \neq 0$, *then it may be assumed that* $A^{(f)} \neq 0$, *and then*

$$|A|_g = g^{-f}\,|A^{(f)}|_g.$$

In the special case when $h = 1$, the corresponding series

$$A = A^{(f)}g^f + A^{(f+1)}g^{f+1} + A^{(f+2)}g^{f+2} + \dots \ (g),$$

with coefficients that assume only the values 0, 1, 2,..., g-1, is called *the* g*-adic series for* A. In particular, when g is a prime p, it follows that every p-adic number α can in a unique way be written as the p*-adic series*

$$\alpha = A^{(f)}p^f + A^{(f+1)}p^{f+1} + A^{(f+2)}p^{f+2} + \dots \ (p)$$

where the coefficients are integers 0, 1, 2,..., p-1; for $\alpha = 0$ all these coefficients are zero, while for $\alpha \neq 0$ it may be assumed that $A^{(f)} \neq 0$ and then

$$|\alpha|_p = p^{-f} \quad \text{because} \quad |A^{(f)}|_p = 1.$$

All the developments for the g-adic number A studied in this section have one important property in common. If

$$A \leftrightarrow (\alpha_1, \ldots, \alpha_r)$$

is the decomposition of A into its p_1-adic,..., p_r-adic components, then *the same series converge also simultaneously to the limits* $\alpha_1, \ldots, \alpha_r$ *with respect to the valuations* $|a|_{p_1}, \ldots, |a|_{p_r}$, *respectively.*

Of particular importance are those g-adic numbers A which satisfy the inequality

$$|A|_g \leqslant 1$$

and are called g-*adic integers*. Their g-adic series do not contain non-zero terms $A^{(m)}g^m$ with negative exponents m. A proof just like that for the set I_g in § 2 shows that *the set* J_g, say, *of all* g-*adic integers forms a ring*. In the same way, the p-*adic integers* α are defined by the inequality

$$|\alpha|_p \leqslant 1.$$

Their ring J_p is a *domain of integrity*, and it has P_p as its quotient field.

The g-adic series for A and its special case, the p-adic series for α, are extremely useful for actual computations with such numbers. The technique of such computations is explained, with many examples, in Hensel's book "Zahlentheorie".

We conclude this section with a nearly trivial remark. There are infinitely many distinct g-adic numbers

$$A \leftrightarrow (\alpha_1, \ldots, \alpha_r)$$

with one and the same first component α_1, but with varying other components, at least if $r \geqslant 2$. Each of these numbers can be written as a g-adic series

$$A = A^{(f)}g^f + A^{(f+1)}g^{f+1} + A^{(f+2)}g^{f+2} + \ldots \ (g),$$

and then the same series converges to its first component α_1 with respect to the valuation $|a|_{p_1}$. Furthermore, different g-adic numbers naturally are represented by different g-adic series.

Hence there are infinitely many distinct g-*adic series*

$$\alpha_1 = A^{(f)}g^f + A^{(f+1)}g^{f+1} + A^{(f+2)}g^{f+2} + \ldots \ (p_1)$$

for any given p_1-*adic number*, provided only that g is divisible by at least one further prime distinct from p_1.

6. Series for g*-adic numbers.

The results obtained in § 5 lead also to convergent series for g*-adic numbers

$$A^* \leftrightarrow (\alpha, \alpha_1, \ldots, \alpha_r).$$

It is convenient to decompose such numbers into their real and g-adic components and to write

$$A^* \leftrightarrow (\alpha, A)$$

where

$$A \leftrightarrow (\alpha_1, \ldots, \alpha_r).$$

As before, the integer $h \neq 0$ is assumed to be relatively prime to g; in addition, let

$$\left|\frac{g}{h}\right| < 1.$$

Further, if ρ is any real number, denote by $M(\rho)$ that system of representatives which consists of the integers k satisfying

$$\rho - g < k \leq \rho.$$

The construction of the series for A^* proceedes now as follows. Choose any integer f for which

$$\left|\left(\frac{g}{h}\right)^{-f} \alpha\right| < |h|, \quad \left|\left(\frac{g}{h}\right)^{-f} A\right|_g \leq 1,$$

and put

$$A^{*(f)} = \left(\frac{g}{h}\right)^{-f} A^* \leftrightarrow (\alpha^{(f)}, A^{(f)}), \text{ where } A^{(f)} \leftrightarrow (\alpha_1^{(f)}, \ldots, \alpha_r^{(f)}).$$

Then

$$\alpha^{(f)} = \left(\frac{g}{h}\right)^{-f} \alpha, \; A^{(f)} = \left(\frac{g}{h}\right)^{-f} A$$

and hence

$$|\alpha^{(f)}| < |h|, \; |A^{(f)}|_g \leq 1.$$

By §4, there exists a unique $A^{(f)} \epsilon M(\alpha^{(f)})$ satisfying

$$|A^{(f)} - A^{(f)}|_g \leq \frac{1}{g};$$

from this definition, also

$$\alpha^{(f)} - g < A^{(f)} \leq \alpha^{(f)} \quad \text{and hence} \quad 0 \leq \alpha^{(f)} - A^{(f)} < g.$$

Put

$$A^{*(f+1)} = \left(\frac{g}{h}\right)^{-1} (A^{*(f)} - A^{(f)}) \leftrightarrow (\alpha^{(f+1)}, A^{(f+1)}), \text{ where } A^{(f+1)} \leftrightarrow (\alpha_1^{(f+1)}, \ldots, \alpha_r^{(f+1)}),$$

so that

$$A^{*(f)} = A^{(f)} + \frac{g}{h} A^{*(f+1)}, \quad \alpha^{(f+1)} = \left(\frac{g}{h}\right)^{-1} (\alpha^{(f)} - A^{(f)}), \; A^{(f+1)} = \left(\frac{g}{h}\right)^{-1} (A^{(f)} - A^{(f)})$$

and therefore

$$|\alpha^{(f+1)}| < \left|\frac{g}{h}\right|^{-1} g = |h|, \quad |A^{(f+1)}|_g \leq g \cdot \frac{1}{g} = 1.$$

By the same reasoning as a few lines back there further exists a unique $A^{(f+1)} \epsilon M(\alpha^{(f+1)})$ satisfying

$$0 \leq \alpha^{(f+1)} - A^{(f+1)} < g, \quad |A^{(f+1)} - A^{(f+1)}|_g \leq \frac{1}{g}.$$

On putting

$$A^{*(f+2)} = \left(\frac{g}{h}\right)^{-1}(A^{*(f+1)} - A^{(f+1)}) \leftrightarrow (\alpha^{(f+2)}, A^{(f+2)}),\ A^{(f+2)} \leftrightarrow (\alpha_1^{(f+2)}, \ldots, \alpha_r^{(f+2)}),$$

it follows that

$$A^{*(f+1)} = A^{(f+1)} + \frac{g}{h} A^{*(f+2)},\ \alpha^{(f+2)} = \left(\frac{g}{h}\right)^{-1}(\alpha^{(f+1)} - A^{(f+1)}),$$

$$A^{(f+2)} = \left(\frac{g}{h}\right)^{-1}(A^{(f+1)} - A^{(f+1)}),$$

whence

$$|\alpha^{(f+2)}| < |h|,\ \ |A^{(f+2)}|_g \leqslant 1.$$

This construction can be repeated indefinitely, and we so obtain for every suffix $m \geqslant f$

(i): a g^*-adic number

$$A^{*(m)} \leftrightarrow (\alpha^{(m)}, A^{(m)})$$

satisfying

$$|\alpha^{(m)}| < |h|,\ \ |A^{(m)}|_g \leqslant 1, \qquad \text{and}$$

(ii): a unique element $A^{(m)}$ of $M(\alpha^{(m)})$ such that

$$0 \leqslant \alpha^{(m)} - A^{(m)} < g,\ \ |A^{(m)} - A^{(m)}|_g \leqslant \frac{1}{g}$$

and

$$A^{*(m)} = A^{(m)} + \frac{g}{h} A^{*(m+1)}.$$

Then for all $m \geqslant f$,

$$A^{*(f)} = A^{(f)} + \frac{g}{h} A^{(f+1)} + \left(\frac{g}{h}\right)^2 A^{(f+2)} + \ldots + \left(\frac{g}{h}\right)^{m-f-1} A^{(m-1)} + \left(\frac{g}{h}\right)^{m-f} A^{*(m)}.$$

Here

$$\left|\left(\frac{g}{h}\right)^{m-f}\alpha^{(m)}\right| < \left|\frac{g}{h}\right|^{m-f}|h|,\ \ \left|\left(\frac{g}{h}\right)^{m-f}A^{(m)}\right|_g \leqslant g^{-(m-f)},$$

so that both expressions tend to 0 as $m \to \infty$. It follows that

$$\lim_{m\to\infty}\left|\left(\frac{g}{h}\right)^{m-f} A^{*(m)}\right|_{g^*} = 0.$$

Hence $A^{*(f)}$ can be written as the convergent series

$$A^{*(f)} = A^{(f)} + \frac{g}{h} A^{(f+1)} + \left(\frac{g}{h}\right)^2 A^{(f+2)} + \ldots \ (g^*),$$

and since $A^* = \left(\frac{g}{h}\right)^f A^{*(f)}$, it also follows that

$$A^* = A^{(f)}\left(\frac{g}{h}\right)^f + A^{(f+1)}\left(\frac{g}{h}\right)^{f+1} + A^{(f+2)}\left(\frac{g}{h}\right)^{f+2} + \ldots \ (g^*).$$

In these two series the coefficients $A^{(m)}$ are integers such that

$$0 \leq \alpha^{(m)} - A^{(m)} < g, \quad \text{where} \quad |\alpha^{(m)}| < |h|.$$

Their absolute values are therefore smaller than $g+|h|$, and hence

$$|A^{(m)}| \leq g + |h| - 1 \qquad \text{for } m \geq f.$$

In the special case when h is positive and when $\alpha \geq 0$, it is easily deduced from the definition of the real numbers $\alpha^{(m)}$ that all these numbers are non-negative. We therefore find now that

$$-g \leq \alpha^{(m)} - g < A^{(m)} \leq \alpha^{(m)} < h$$

and hence

$$-(g-1) \leq A^{(m)} \leq h-1.$$

Thus the following result has been obtained.

Let $h \neq 0$ *be an integer prime to* g *such that* $\left|\frac{g}{h}\right| < 1$, *and let* $A^* \leftrightarrow (\alpha, A)$ *be any* g*-*adic number. Denote by* f *any integer satisfying*

$$\left|\left(\frac{g}{h}\right)^{-f}\alpha\right| < |h|, \quad \left|\left(\frac{g}{h}\right)^{-f}A\right|_g \leq 1.$$

Then A^* *can be written as a convergent infinite series*

$$A^* = A^{(f)}\left(\frac{g}{h}\right)^f + A^{(f+1)}\left(\frac{g}{h}\right)^{f+1} + A^{(f+2)}\left(\frac{g}{h}\right)^{f+2} + \ldots \quad (g^*)$$

where all coefficients $A^{(m)}$ *are integers at most of absolute values* $g+|h|-1$. *If* $h > 0$ *and* $\alpha \geq 0$, *it may be assumed that these coefficients satisfy the stronger condition* $-(g-1) \leq A^{(m)} \leq h-1$.

A look through the proof shows that this result remains valid even when A^* reduces to its real component α, i.e., when $g = 1$, $r = 0$, and there is no g-adic component. We then obtain the classical representation

$$\alpha = A^{(f)}h^{-f} + A^{(f+1)}h^{-f-1} + A^{(f+2)}h^{-f-2} + \ldots$$

of the real number α to the basis h, with "digits" $A^{(m)}$ that assume only the integral values 0, 1, 2, ..., h-1.

In the g-adic case the set J_g of all g-adic integers, i.e., of all g-adic numbers A satisfying $|A|_g \leq 1$, was found to be a ring, due to $|a|_g$ being Non-Archimedean. In addition, the g-adic series for the elements of J_g consisted of terms $A^{(m)}g^m$ that were rational integers; hence g-adic integers have the characteristic property of being limits of sequences of rational integers. It might seem appropriate to introduce also the set J_g^* of all g*-adic numbers A^* satisfying $|A^*|_{g^*} \leq 1$ and to call its elements g*-adic integers. However, since $|a|_{g^*}$ is now Archimedean, J_g^* is no longer a ring, but is closed only under multiplication. Moreover, the elements of J_g^* distinct from 0, +1, and -1 cannot be approximated arbitrarily closely by sequences of rational integers. There is thus no justification for singling out the elements of J_g^* among other g*-adic numbers.

The series studied in this chapter give explicit expressions for the elements of P, P_p, P_g, and P_{g^*}, and their finite sections give rational

approximations. The same series will be applied in Chapter 4 to the construction of continued fractions for g-adic and g*-adic numbers.

7. Sequences that converge with respect to all valuations of Γ.

Let $\{p_m\}$ be the sequence of all prime numbers 2, 3, 5,... written in ascending order, and let α be a real number, while α_M, for M = 1, 2, 3,..., is a p_M-adic number. We conclude the chapter with the following simple remark.

There exists an infinite sequence $\{a_m\}$ *of rational numbers such that, simultaneously,*

$$\lim_{m\to\infty} a_m = \alpha; \quad \lim_{m\to\infty} a_m = \alpha_M (p_M) \quad \text{for all } M.$$

For, as we saw, the different valuations are independent and hence it is possible to find, for each suffix m, a rational number a_m such that

$$|a_m - \alpha| < \frac{1}{m}; \ |a_m - \alpha_1|_{p_1} < \frac{1}{m}, \ |a_m - \alpha_2|_{p_2} < \frac{1}{m}, \ldots, \ |a_m - \alpha_m|_{p_m} < \frac{1}{m}.$$

Then the sequence $\{a_m\}$ has the required properties.

A similar proof shows that if each α_M is a p_M-adic *integer,* a sequence $\{a_m\}$ of rational *integers* can be found such that

$$\lim_{m\to\infty} a_m = \alpha_M (p_M) \text{ for all } M.$$

This result is easily seen to be equivalent to the following one.

There exists an infinite sequence $\{A_m\}$ *of rational integers satisfying* $0 \leq A_m \leq m$ *such that, simultaneously,*

$$A_1 \cdot 1! + A_2 \cdot 2! + A_3 \cdot 3! + \ldots = \alpha_M (p_M) \text{ for all } M.$$

Infinite series of this kind were first studied by D. van Dantzig.