Chapter 1

PRELIMINARIES: VALUATIONS

We develop the theory of non-Archimedean valuations only as far as is necessary for our functional analysis. This chapter contains no new results.

Throughout the chapter, K is a field. Its unit element we denote by 1_K. The symbol 1 refers to the unit element of $\mathbb{R}$. (We make this distinction in the first chapter only; after that we shall use 1 indiscriminately for both the real number and the unit element of K.)

A *valuation* on K is a function $|\ |: K \to \mathbb{R}$ with

i. $|x| \geq 0 \quad (x \in K)$

ii. $|x| = 0$ if and only if $x = 0 \quad (x \in K)$

iii. $|x + y| \leq |x| + |y| \quad (x,y \in K)$

iv. $|xy| = |x|\,|y| \quad (x,y \in K)$

$|x|$ is the *value* of x. The value of 1_K is 1.
A *valued field* is a pair consisting of a field K and a valuation $|\ |$ on K. Instead of "the valued field $\langle K, |\ |\rangle$" we shall mostly say "the valued field K."

A valuation $|\ |$ defines a metric ρ by

$$\rho(x,y) := |x - y| \quad (x,y \in K)$$

With respect to this metric, addition, multiplication and inversion are continuous. We call K *complete* if it is complete relative to this metric.

A valuation $|\ |$ is called *Archimedean* if the set $\{n1_K : n \in \mathbb{N}\}$ is unbounded; otherwise it is *non-Archimedean*. For non-Archimedean valuations the triangle inequality (iii) can be sharpened considerably:

1.1 THEOREM. *Let* $|\ |$ *be a valuation on* K. *The following conditions are equivalent.*

α. *The valuation is non-Archimedean.*

β. $|n1_K| \leq 1$ *for every* $n \in \mathbb{N}$.

γ. *For all* $a,b \in K$, $|a + b| \leq \max\{|a|, |b|\}$

δ. *If* $a,b \in K$ *and* $|a| < |b|$, *then* $|b - a| = |b|$.

PROOF. (β) ⇒ (α) is trivial; (γ) ⇒ (β) is easy.
(α) ⇒ (γ). Let $r := \sup\{|n1_K| : n \in \mathbb{N}\}$. Then $|nx| \leq r|x|$ for all $n \in \mathbb{N}$ and $x \in K$. Take $a,b \in K$ and put $s := \max\{|a|,|b|\}$.
For every $n \in \mathbb{N}$, $|a + b|^m = |(a + b)^m| \leq \sum_j |\binom{m}{j} a^j b^{m-j}| \leq (m+1)rs^m$.
Hence, $|a + b| \leq [\lim \sqrt[m]{(m + 1)r}]s = s = \max\{|a|,|b|\}$.
(γ) ⇒ (δ). $|b| \leq \max\{|a|,|b - a|\}$; hence, if $|b| > |a|$, then $|b| \leq |b - a| \leq \max\{|b|,|-a|\} = |b|$.
(δ) ⇒ (γ). If $|a + b| > |a|$, then $|b| = |(a + b) - a| = |a + b|$; in particular, $|a + b| \leq |b|$. Similarly, if $|a + b| > |b|$, then $|a + b| \leq |a|$.

Formula (γ) is known as the *strong triangle inequality*.

The simplest fields are the finite fields and the field $\mathbb{Q}$ of all rational numbers. On a finite field the only valuation is the trivial one, given by

$$|0| = 0 \qquad |x| = 1 \qquad (\text{if } x \neq 0)$$

(If $x \neq 0$ and $|x| \neq 1$, then $x, x^2, x^3, \ldots$, are distinct.) It follows that on a field of nonzero characteristic no valuation is Archmedean. On $\mathbb{Q}$ the absolute value function w is an

Archimedean valuation. Other Archimedean valuations on $\mathbb{Q}$ are the functions w^τ $(0 < \tau < 1)$. Every prime number p determines a non-Archimedean valuation (the *p-adic valuation*) $|\ |_p$ on $\mathbb{Q}$ by

$$|p|_p := p^{-1}$$
$$|n|_p := 1 \qquad (n \in \mathbb{N};\ n \text{ not divisible by } p.)$$

For every $\tau > 0$, $x \mapsto (|x|_p)^\tau$ is a valuation on $\mathbb{Q}$. The following theorem classifies all valuations on $\mathbb{Q}$.

1.2 THEOREM (Ostrowski). *Let* $|\ |$ *be a valuation on* $\mathbb{Q}$ *that is not trivial (i.e., there is an* $x \in \mathbb{Q}$, $x \neq 0$ *with* $|x| \neq 1$). *If* $|\ |$ *is Archimedean there exists a* $\tau \in (0,1]$ *such that* $|\ | = w^\tau$ *(w denotes the absolute value function). Otherwise there exist a prime* p *and a* $\tau > 0$ *such that* $|\ | = (|\ |_p)^\tau$.

PROOF. If the valuation is non-Archimedean, then by Theorem 1.1 $\{n \in \mathbb{Z} : |n| < 1\}$ is a prime ideal in $\mathbb{Z}$, so there exists a prime number p such that $\{n \in \mathbb{Z} : |n| = 1\} = \{n \in \mathbb{Z} : n$ is not a multiple of p$\}$. Take τ so that $|p| = p^{-\tau}$: then $|\ |^{1/\tau}$ is just the p-adic valuation.

Now assume the valuation is Archimedean. For $n \in \mathbb{N}$, let $L(n) := \max\{|n|, 1\}$. Take $m, n, k \in \{2, 3, \ldots\}$, and let s be the entire part of $k(\log m)(\log n)^{-1}$. As $m^k < n^{s+1}$, there exist $a_0, \ldots, a_s \in \{0, 1, \ldots, n - 1\}$ such that $m^k = a_0 + a_1 n + \ldots + a_s n^s$. Then $|m|^k = |m^k| \leq \sum_i |a_i|\ |n|^i \leq (s + 1)AL(n)^s$, where $A := \max\{|0|, |1|, \ldots, |n - 1|\}$. It follows that

$$\log L(m) \leq k^{-1}[\log(s + 1) + \log A + s \log L(n)]$$
$$\leq k^{-1} \log(k\frac{\log m}{\log n} + 1) + k^{-1} \log A + \frac{\log m}{\log n} \log L(n)$$

For given m and n this inequality holds for all $k \geq 2$; hence $\log L(m) \leq (\log m)(\log n)^{-1}\log L(n)$. By symmetry,

$$\frac{\log L(m)}{\log m} = \frac{\log L(n)}{\log n} \qquad (m, n = 2, 3, \ldots)$$

Then there exists a $\tau \geq 0$ such that $\log L(m) / \log m = \tau$ for all $m \in \mathbb{N}$, that is,

$$\max\{|m|, 1\} = m^{\tau} \qquad (m \in \mathbb{N})$$

Inductively one proves $|m| \leq m$; then $\tau \leq 1$. As the valuation is Archimedean, $\tau > 0$, so $|m| = m^{\tau}$ $(m \in \mathbb{N})$. Then $|x| = w(x)^{\tau}$ for all $x \in \mathbb{Q}$.

It is from Ostrowski's theorem that the non-Archimedean valuations derive their importance. In fact, let $|\ |$ be an Archimedean valuation on K. We have already seen that the characteristic of K must be 0, so K contains (a field isomorphic to) $\mathbb{Q}$, and on $\mathbb{Q}$ the valuation is of the form w^{τ}. It follows from a slight extension of the Gelfand-Mazur theorem (see Ref. 189) that K is essentially a subfield of $\mathbb{C}$. In particular, if K is complete under the induced metric, then either $K = \mathbb{R}$ or $K = \mathbb{C}$. Thus, "most" valuations are non-Archimedean.

Let $|\ |$ be a non-Archimedean valuation on K. $R := \{x \in K : |x| \leq 1\}$ is a subring of K; $I := \{x \in K : |x| < 1\}$ is an ideal in R. Every element of R that does not belong to I has an inverse in R, so I is a maximal ideal and R/I is a field. This field is the *residue class field* of K. The natural homomorphism $R \to R/I$ is usually written $x \mapsto \bar{x}$.

$\{|x| : x \in K, x \neq 0\}$ is a subgroup of the multiplicative group $(0,\infty)$; it is called the *value group* of the valuation. The valuation is called *trivial*, *discrete*, or *dense* accordingly as its value group is $\{1\}$, a discrete subset of $(0,\infty)$ or a dense subset of $(0,\infty)$. The valuation is either discrete or dense. If it is discrete and not trivial, then $\{|x| : |x| < 1\}$ contains a largest element, s. The value group is then $\{s^n : n \in \mathbb{Z}\}$.

If the characteristic of K is a prime numer p, then the characteristic of the residue class field is also p.

1.A Exercise. Let K be a complete non-Archimedean valued field. Let $x_1, x_2, \ldots \in K$.

i. If $\lim x_n = x \neq 0$, then $|x_n| = |x|$ for large n.

ii. If $\lim x_n = 0$, then Σx_n converges in K.

iii. If $\lim x_n = 0$ and if ρ is a permutation of $\mathbb{N}$, then $\sum_{n=1}^{\infty} x_n = \sum_{n=1}^{\infty} x_{\rho(n)}$.

iv. If $\lim x_n = 1$, then the infinite product Πx_n converges. Its value is 0 if and only if one of the x_n vanishes.

v. If $\lim x_n = 1$ and if ρ is a permutation of $\mathbb{N}$, then $\prod_{n=1}^{\infty} x_n = \prod_{n=1}^{\infty} x_{\rho(n)}$.

1.B Exercise. Let K be a field with a nontrivial non-Archimedean valuation.

i. K is not compact.

ii. If K is locally compact, then $\{x \in K : |x| \leq 1\}$ is compact, K is σ-compact and K is separable (as a metric space).

iii. The conditions (α) through (δ) are equivalent.

α. K is locally compact.

β. $\{x \in K : |x| \leq 1\}$ is compact.

γ. Every closed bounded subset of K is compact.

δ. K is complete, the valuation is discrete, and the residue class field is finite.

(Hint for the implication $(\delta) \Rightarrow (\beta)$: Take $a \in K$, $|a| < 1$ such that $\{|a|^n : n \in \mathbb{Z}\}$ is the value group of K. Let X be a subset of the additive group $\{x : |x| \leq 1\}$ that contains exactly one point of every coset of the subgroup $\{x : |x| < 1\}$. Show that for every x with $|x| \leq 1$ and for every $n \in \mathbb{N}$, there exist $x_0, \ldots, x_n \in X$ such that $|x - \sum_{i \leq n} x_i a^i| \leq |a|^{n+1}$. Now prove that the map $X^{\mathbb{N}} \to K$ defined by $(x_0, x_1, \ldots) \mapsto \Sigma x_i a^i$ is a homeomorphism onto $\{x : |x| \leq 1\}$.)

1.C Exercise. Let $| \ |$ be a non-Archimedean valuation on K. Let $\overline{K}$ be the metric completion of K. Then there is a natural way to give $\overline{K}$ the structure of a complete valued field such that the embedding $K \to \overline{K}$ is an isometric field isomorphism. K and $\overline{K}$ have the same value group and isomorphic residue class fields.

1.D Exercise. If $| \ |$ is a non-Archimedean valuation on K and if $\varepsilon < 1$, then $\{x \in K : |x - 1_K| \leq \varepsilon\}$ is a group under multiplication.

1.E Exercise. Let K be a non-Archimedean valued field with residue class field k. If the characteristic of K is not 0, then k and K have the same characteristic. (See exercise 1.F for an example where K and k have unequal characteristics.)

The completion of $\mathbb{Q}$ relative to the p-adic valuation is the field $\mathbb{Q}_p$ of the *p-adic numbers*. The set $\mathbb{Z}_p := \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$ is the ring of the *p-adic integers*. $\mathbb{Q}_p$ is the simplest example of a nontrivial non-Archimedean valued field. It has many features in common with $\mathbb{R}$ and $\mathbb{C}$ (e.g., local compactness, separability) but in other respects it is completely different from them (e.g., algebraic closedness, connectedness). We present a few facts on $\mathbb{Q}_p$ and $\mathbb{Z}_p$ that are of use in subsequent sections. For more information, see Ref. 8.

1.F Exercise. Let p be a prime number, let $S_p := \{0, 1, \ldots, p - 1\}$.

i. The valuation of $\mathbb{Q}_p$ is discrete: its value group is $\{p^n : n \in \mathbb{Z}\}$. $\mathbb{Q}_p$ contains no element whose square is p. $\mathbb{Q}_p \neq \mathbb{Q}$. As a field, $\mathbb{Q}_p$ is not isomorphic to $\mathbb{R}$ or $\mathbb{C}$.

ii. The sets $s + p\mathbb{Z}_p$ $(s \in S_p)$ are the cosets of $p\mathbb{Z}_p$ in $\mathbb{Z}_p$.

iii. The residue class field of $\mathbb{Q}_p$ is a field of p elements.

iv. For every $a \in \mathbb{Z}_p$ there exist $s_0, s_1, \ldots \in S_p$ such that $a = \sum_{s=0}^{\infty} s_i p^i$, convergence being in the sense of $| \ |_p$. (Hint: Make $s_0, s_1, \ldots,$ so that for every $N \in \mathbb{N}$, $|a - \sum_{i=0}^{N-1} s_i p^i|_p \leq p^{-N}$.)

v. The formula

$$(s_0, s_1, \ldots) \mapsto \sum_{i=0}^{\infty} s_i p^i \qquad (s_i \in S_p)$$

yields a homeomorphism of $S_p^{\mathbb{N}}$ onto $\mathbb{Z}_p$.

vi. $\mathbb{Z}_p$ is compact; $\mathbb{Q}_p$ is locally compact.

vii. Let K be a complete non-Archimedean valued field of characteristic 0 such that its residue class field has characteristic p. Then there exists a field isomorphism T of $\mathbb{Q}_p$ onto the closure K_0 of the prime field of K and there exists a $\tau \in (0,\infty)$ such that $|Tx| = (|x|_p)^{\tau}$ for all $x \in \mathbb{Q}_p$.

1.G Exercise. Let $| \ |$ be a non-Archimedean valuation on K. For a polynomial $f = \Sigma a_i X^i$, set $||f|| := \max\{|a_i|\}$. The function $|| \ ||$ on the ring K[X] of all polynomials over K has an extension to a non-Archimedean valuation on the field K(X) of all rational functions over K. This valuation extends the given valuation of K.

In the following exercise we introduce a valuation on K(X) that does not presuppose a valuation on K.

1.H Exercise. Let F be a field. Take an irreducible polynomial $f_0 \in F[X]$. There exists a (unique) non-Archimedean valuation $|| \ ||$ on F(X) for which $||f_0|| = e^{-1}$ (where e = 2.7182...) and $||f|| = 1$ if $f \in F[X]$ is not divisible by f_0.

(The analogy with $|\ |_p$ is plain.) The restriction of this valuation to F is trivial. In particular, for f_0 we take the polynomial X. Let $R := \{f \in F(X) : ||f|| \leq 1\}$, $I := \{f \in F(X) : ||f|| < 1\}$. Then $R \supset K[X]$. The map $f \mapsto f(0)$, $f \in K[X]$, extends uniquely to a ring homomorphism of R into F whose kernel is I. Thus the residue class field of F(X) is isomorphic to F itself.

For another example of a non-Archimedean valued field we need some additional terminology. (See Ref. 256, Vol. II.)

Let F be a field. By a *formal Laurent series* over F we mean a two-sided sequence $(\ldots, a_{-1}, a_0, a_1, \ldots)$ of elements of F for which there exists an $N \in \mathbb{Z}$ such that $a_n = 0$ for all $n < N$. A *formal power series* over F is a formal Laurent series $(\ldots, a_{-1}, a_0, a_1, \ldots)$ such that $a_n = 0$ for all $n < 0$. Instead of $(\ldots, a_{-1}, a_0, a_1, \ldots)$ we also write $\Sigma a_n X^n$ or, if $a_n = 0$ for all $n < N$, $\sum_N^\infty a_n X^n$. The formal Laurent series over F constitute a field F((X)) under the operations

$$\Sigma a_n X^n + \Sigma b_n X^n := \Sigma (a_n + b_n) X^n$$

$$(\Sigma a_n X^n)(\Sigma b_n X^n) := \Sigma c_n X^n$$

where $c_n := \sum_i a_i b_{n-1}$. (Observe that in the expression $\Sigma a_i b_{n-i}$ only finitely many nonzero terms occur.)

The formal power series form a subring F[[X]] of F((X)). The natural map $F[X] \to F[[X]]$ is an injective ring homomorphism extending to an injective homomorphism $F(X) \to F((X))$. In the following we view F[X] and F(X) as subsets of F[[X]] and F((X)), respectively.

1.I Exercise. Define a real-valued function $|\ |$ on F((X)) by

$$|\Sigma a_n X^n| := 0 \qquad (\text{if } a_n = 0 \text{ for all } n)$$

$$|\Sigma a_n X^n| := e^{-N} \qquad (\text{if } N = \min\{n : a_n \neq 0\})$$

Then $|\ |$ is a non-Archimedean valuation. Relative to this valuation, F((X)) is complete and $F[[X]] = \{f \in F((X)) : |f| \leq 1\}$. The value group of K((X)) is $\{e^n : n \in \mathbb{Z}\}$; its residue class field is isomorphic to F.

F((X)) is (isometrically isomorphic to) the metric completion of F(X), where F(X) carries the valuation introduced in the last part of Exercise 1.H.

For every element $\sum_N^\infty a_n X^n$ of F((X)) we have $\sum_N^\infty a_n X^n = \lim_M \sum_N^M a_n X^n$. Thus, the expression $\Sigma a_n X^n$ may be regarded ex post facto as referring to a convergent sum.

Apparently, for every field F one can make a (complete) non-Archimedean valued field whose residue class field is isomorphic to F and whose value group is $\{e^n : n \in \mathbb{Z}\}$.

1.3 THEOREM. *Let* F *be a field and* Σ *an additive subgroup of* $\mathbb{R}$. *There exists a non-Archimedean valued field* K *whose residue class field is isomorphic to* F *and whose value group is* $\{e^s : s \in \Sigma\}$.

PROOF. Let $\mathcal{S} := \{S \subset \Sigma :$ for every $s \in \mathbb{R}$, $S \cap (-\infty, s)$ is a finite set$\}$. This $\mathcal{S}$ has the following properties:

i. $\{s\} \in \mathcal{S}$ for all $s \in \Sigma$.

ii. If $S \in \mathcal{S}$ and $S \neq \emptyset$, then S has a smallest element.

iii. If $S \in \mathcal{S}$ and $T \subset S$, then $T \in \mathcal{S}$.

iv. If $S, T \in \mathcal{S}$, then $S \cup T \in \mathcal{S}$.

v. If $S, T \in \mathcal{S}$, then $S + T \in \mathcal{S}$, where $S + T := \{s + t : s \in S, t \in T\}$.

vi. If $S, T \in \mathcal{S}$ and $u \in \Sigma$, then there exist only finitely many elements s of S for which $u - s \in T$.

vii. If $S \subset \Sigma$ and if $a_1, a_2, \ldots \in \mathbb{R}$ are such that $\lim a_n = \infty$ while $(-\infty, a_n) \cap S \in \mathcal{S}$ for each n, then $S \in \mathcal{S}$.

For a map f of Σ into F, set $\text{supp } f := \{s \in \Sigma : f(s) \neq 0\}$. Let K be the set of all $f : \Sigma \to F$ for which $\text{supp } f \in \mathcal{S}$. For $s \in \Sigma$, let e_s denote the F-valued characteristic function of $\{s\}$; then $e_s \in K$. Under pointwise operations, K is a vector space over F. [Here we use (iii) and (iv).] It follows from (vi) (take $S := \text{supp } f$ and $T := \text{supp } g$) that for all $f, g \in K$ we can define $f * g : \Sigma \to F$ by

$$(f * g)(u) := \sum_s f(s)g(u - s) \qquad (u \in \Sigma)$$

According to (v) and (iii), $f * g \in K$. It is easy to see that K has become a commutative ring in which e_0 serves as an identity element.

Next we prove that K actually is a field. Take $f \in K$, $f \neq 0$. Let s be the smallest element of supp f. If $f * e_{-s}$ is invertible, then $(f * e_{-s})^{-1} * e_{-s}$ is an inverse of f. Now the smallest element of supp $f * e_{-s}$ is 0. [In fact, $(f * e_{-s})(t) = f(t + s)$ for all $t \in \Sigma$.] Thus, *we may assume that the smallest element of* supp f *is* 0. Since then $f(0) \neq 0$, it is also clear that *we may assume* $f(0) = 1$.

Let $S := \text{supp } f$. Then $S \subset [0,\infty)$ and S generates a subsemigroup [S] of $[0,\infty)$. Applying (ii) to $S \setminus \{0\}$ we see that there exists an $a > 0$ such that all nonzero elements of S are greater than a. For $n \in \mathbb{N}$, let $S_n := \{s_1 + \ldots + s_n : s_1, \ldots, s_n \in S\}$. By (v), $S_n \in \mathcal{S}$. Furthermore $[S] \cap (-\infty, na) \subset S_n$. It follows from (vii) that $[S] \in \mathcal{S}$.

An inverse of f will be an element g of K for which

1. $f(0)g(0) = 1$

2. $\sum_s f(s)g(u - s) = 0 \qquad (u \in \Sigma, u \neq 0)$

If we choose $g : \Sigma \to F$ so that $g(0) = 1$ and $\text{supp } g \subset [S]$, then $g \in K$, g satisfies (1), and the equation in (2) holds for all $u \in \Sigma \setminus [S]$. As $f(0) = 1$, we now only have to construct g in such a way that

$$g(u) = -\sum_{\substack{s\in\Sigma \\ s>0}} f(s)g(u - s) \qquad (u \in [S], u > 0)$$

With a as above, this is the same as

$$g(u) = -\sum_{\substack{s\in\Sigma \\ s>a}} f(s)g(u - s) \qquad (u \in [S], u > 0)$$

It is clear how one defines such a g successively on $[S] \cap (0,a)$, $[S] \cap [a,2a)$, $[S] \cap [2a,3a)$, ...

Thus, K is a field. For $f \in K \setminus \{0\}$, let r(f) denote the smallest element of supp f. Set

$$|f| := e^{-r(f)} \qquad (f \in K, f \neq 0)$$

$$|0| := 0$$

Then $|\ |$ is a valuation on K. The value group is just $\{e^s : s \in \Sigma\}$.

For $f,g \in K$ and $\varepsilon > 0$, we have

(†) $|f - g| \leq \varepsilon$ if and only if $f = g$ on $(-\infty, -\log \varepsilon)$. It follows easily that $f \mapsto f(0)$ is a ring homomorphism of $\{f \in K : |f| \leq 1\}$ onto F whose kernel is $\{f \in K : |f| < 1\}$. Thus, the residue class field of K is isomorphic to F.

A few remarks about Theorem 1.3 and its proof:

i. Take $\Sigma = \mathbb{Z}$. To every $f \in K$ we assign the formal Laurent series $\sum f(n)X^n$. Thus we obtain an isometric isomorphism of K onto the field constructed at the end of exercise 1.H.

ii. *The field* K *we have made in the proof of Theorem 1.3 is metrically complete*. Proof. Let $\varepsilon_1, \varepsilon_2, \ldots,$ be a decreasing sequence of positive numbers that tends to 0, and let $f_1, f_2, \ldots,$ be a sequence in K such that $|f_i - f_j| \le \varepsilon_n$ as soon as $i,j \ge n$. By (†),

$$f_i = f_j \text{ on } (-\infty, -\log \varepsilon_n) \qquad (i,j \ge n)$$

Hence, there is an $f : \Sigma \to F$ such that for all n,

$$f = f_n \text{ on } (-\infty, -\log \varepsilon_n)$$

By property (vii) of $\mathcal{S}$, $f \in K$. Applying (†) again, we see that $|f - f_n| \le \varepsilon_n$ for each n. Thus, $f = \lim f_n$.

iii. Take a prime number p. Let $F = \mathbb{F}_p$ and $\Sigma = \{n \log p : n \in \mathbb{Z}\}$. The field K constructed above and the field $\mathbb{Q}_p$ are both metrically complete, they have the same value group and isomorphic residue class fields. However, they are not isomorphic since the characteristic of K is p while $\mathbb{Q}_p$ has characteristic 0.

iv. The reader will have noticed that in the proof of Theorem 1.3 we have used no properties of $\mathcal{S}$ other than (i)-(vii). It follows that we can set up the same construction for any system $\mathcal{S}$ of subsets of Σ that has these seven properties. This we do in exercise 1.J.

1.J Exercise. Let F and Σ be as in Theorem 1.3. Let $\mathcal{S}$ be the collection of all well-ordered subsets of Σ. Then $\mathcal{S}$ has properties (i)-(vii) mentioned in the proof of Theorem 1.3. Let L be the set of all maps $f : \Sigma \to F$ for which $\operatorname{supp} f \in \mathcal{S}$. In complete analogy to the proof of Theorem 1.3, L can be given the structure of a metrically complete non-Archimedean valued field whose value group is $\{e^s : s \in \Sigma\}$ and whose residue class field is isomorphic to F. The field K of the proof of Theorem 1.3 is a closed subfield of L. The fields coincide if and only if Σ is a discrete subgroup of $\mathbb{R}$.

There are various fields of formal Laurent series that, in more or less natural ways, can be given valuations. The following example is a generalization of exercise 1.G.

1.K Exercise. Let K be a complete non-Archimedean valued field. Let $\rho > 0$. By $K_\rho\{X\}$ we denote the set of all formal power series $\Sigma\, a_n X^n$ for which $\lim_n |a_n|\rho^n = 0$. This $K_\rho\{X\}$ is a subring of $K[[X]]$. Define

$$\|\Sigma\, a_n X^n\| := \max\{|a_n|\rho^n\} \qquad (\Sigma\, a_n X^n \in K_\rho\{X\})$$

For all $f,g \in K\{X\}$ we have $\|f\| > 0$ if and only if $f \ne 0$, $\|f + g\| \le \max\{\|f\|,\|g\|\}$ and $\|fg\| \le \|f\|\,\|g\|$. To prove that $\|fg\| \ge \|f\|\,\|g\|$, let $f = \Sigma\, a_n X^n$, $g = \Sigma\, b_n X^n$, and $fg = \Sigma\, c_n X^n$. Assume $f \ne 0$ and $g \ne 0$. Let $n := \max\{i : |a_i|\rho^i = \|f\|\}$ and $m := \max\{j : |b_j|\rho^j = \|g\|\}$. Then

$$(\dagger) \quad c_{n+m} = a_n b_m + \sum_{i<n} a_i b_{n+m-i} + \sum_{j<m} a_{n+m-j} b_j$$

For $i < n$, we have $|a_i b_{n+m-i}|\rho^{n+m} = |a_i|\rho^i |b_{n+m-i}|\rho^{n+m-i} < \|f\|\,\|g\| = |a_n b_m|\rho^{n+m}$, so $|a_i b_{n+m-i}| < |a_n b_m|$. Similarly, $|a_{n+m-j} b_j| < |a_n b_m|$ for all $j < m$. By 1.1 (δ) and (†) we have $|c_{n+m}| = |a_n b_m|$, and therefore $\|fg\| \ge \|f\|\,\|g\|$.

It follows that $\|\ \|$ extends to a valuation on the quotient field of $K_\rho\{X\}$. This quotient consists of the formal Laurent series $\sum_N^\infty a_n X^n$ for which $\lim_n |a_n|\rho^n = 0$; the value of $\sum_N^\infty a_n X^n$ is just $\max_n\{|a_n|\rho^n\}$. Both $K_\rho\{X\}$ and its quotient field are metrically complete. The quotient field of $K_1\{X\}$ is the completion of the valued field $K(X)$ constructed in exercise 1.G. (These statements are not trivial, but we confidently leave them to the reader to prove.)

The following lemma is a non-Archimedean *regula falsi*.

1.4 LEMMA. *Let* K *be a complete non-Archimedean valued field. Let* $r > 0$, *and let* B *be either* $\{x \in K : |x| < r\}$ *or* $\{x \in K : |x| \le r\}$. *Let* $0 < c < 1$, *and let* $f : B \to K$ *be so that*

$$f(0) = 0$$

$$\left|\frac{f(x) - f(y)}{x - y} - 1\right| \le c \qquad (x,y \in B,\ x \ne y)$$

Then f *is an isometry of* B *onto* B.

PROOF. For $x \ne y$, we have $|[f(x) - f(y)] - (x - y)| < |x - y|$; so $|f(x) - f(y)| = |x - y|$ [1.1(δ)]. It follows that f is an isometry of B into B. In particular, f is continuous. Take $a \in B$; we construct an $x \in B$ with $f(x) = a$. For simplicity, define $f = 0$ on $K \setminus B$. Define $x_n \in K$ by

$$x_0 := 0$$

$$x_{n+1} := x_n + a - f(x_n) \qquad (n = 0,1,\ldots)$$

If, for certain n, we have $x_0,\ldots,x_n \in B$, then $f(x_n) \in B$; so $x_{n+1} \in B$. Consequently, all x_n lie in B. Moreover,

$$|x_{n+1} - x_n| = |(x_n - x_{n-1}) - [f(x_n) - f(x_{n-1})]|$$
$$\le c|x_n - x_{n-1}|$$

As $c < 1$, $\lim|x_{n+1} - x_n| = 0$. It follows that the x_n form a Cauchy sequence, so that $x := \lim x_n$ exists. Then $x \in B$ and $0 = \lim(x_n - x_{n-1}) = \lim a - f(x_{n-1}) = a - f(x)$.

This lemma leads to a connection between the roots of unity in K and those in the residue class field.

1.L Exercise. Let K be a complete non-Archimedean valued field, k its residue class field, q the characteristic of k (possibly, $q = 0$). Let T_k be the group of all roots of unity of k, and T_K the group of those roots of unity of K whose orders are not divisible by q. (This restriction is, of course, void if $q = 0$.) Then the natural map $\{x \in K : |x| \le 1\} \to k$ yields a group isomorphism of T_K onto T_k. (Note that the order of a root of unity of k cannot be divisible by q.)

If the characteristic of K is not 0 and if k is finite, then T_K is a subfield of K that is isomorphic to k.

Let p be a prime number, $p > 2$. Let $x \in \mathbb{Q}_p$, $x^p = 1$. We prove $x = 1$. Take $y \in \mathbb{Q}_p$ such that $x = 1 + y$. Then $|y| \le 1$ and

$$|y|^p = \left|\sum_{i=1}^{p-1} \binom{p}{i} y^i\right| \le \max_i\{|\tbinom{p}{i}||y|^i\} \le \frac{1}{p}|y|$$

[Notice that every occurring $\binom{p}{i}$ is divisible by p.]
Hence, $|y| < 1$ and therefore $|y| \le 1/p$. But then, as $(1 + y)^p = 1$,

$$\frac{1}{p}|y| = |\tbinom{p}{1}y| = \left|\sum_{i=2}^{p} \binom{p}{i} y^i\right|$$

$$\le \max\{\max_{2\le i<p}\{|\tbinom{p}{i}y^i|\},\ |y|^p\} \le \frac{1}{p}|y|^2$$

This is possible only if $y = 0$ and $x = 1$.

We see that for $K = \mathbb{Q}_p$, T_K is the group of all roots of unity.

1.M Exercise.

i. Let p be a prime. If $p \ne 2$, the roots of unity of $\mathbb{Q}_p$ form a cyclic group of order $p - 1$. In $\mathbb{Q}_2$, 1 and -1 are the only roots of unity.

ii. If p and q are distinct prime numbers, then $\mathbb{Q}_p$ and $\mathbb{Q}_q$ are not isomorphic (as fields).

1.N Exercise. Let p be a prime, $m \in \mathbb{N}$. We consider the map $x \mapsto x^m$ of the set $\{x \in \mathbb{Q}_p : |x| = 1\}$ into itself.

If $p \ne 2$, this map is injective if and only if m and $p - 1$ are relatively prime; it is isometric if and only if in addition m is not a multiple of p. For p = 2, the map is injective if and only if m is odd; then it is automatically an isometry.

There are many nontrivial relations between the algebraic properties of K and those of its residue class field and its value group. We mention only the following.

1.5 THEOREM (Rychlik). *Let* K *be algebraically closed. Then its residue class field* k *is algebraically closed and its value group* Γ *is divisible.*

PROOF. The divisibility of Γ is easy: If $a \in K$ and $n \in \mathbb{N}$, there must exist an $x \in K$ with $x^n = a$; then $|x| = \sqrt[n]{|a|}$

Further, any nonconstant polynomial over k can be written as $\overline{a_0}X^n + \overline{a_1}X^{n-1} + \ldots + \overline{a_n}$, where $n \in \mathbb{N}$, $a_i \in K$, $|a_i| \leq 1$, and $|a_0| = |a_n| = 1$. ($x \mapsto \overline{x}$ is again the natural map of $\{x \in K : |x| \leq 1\}$ onto k.) There exist $b_1, \ldots, b_n \in K$ such that $\Sigma\, a_i X^{n-i} = a_0 \Pi(X - b_i)$ in K[X]. As $|a_0 \Pi b_i| = |a_n|$, there must be an i with $|b_i| \leq 1$. Now $\overline{b_i}$ is a root of the given polynomial over k.

Notes

For the algebraic theory of valuations we refer the reader to Refs. 26, 58, 94, 122, 173, 187, 214, 218 and 243. Theorems on the structure of non-Archimedean valued fields are to be found in Refs. 95, 110, 111, 122, 132, 133, 134 and 214. It should be noted that from the algebraic point of view it is sometimes convenient not to consider the function $|\ |$ itself but the function $v : K \to \mathbb{R} \cup \{\infty\}$ defined by $v(x) := -\log |x|$.

We briefly return to valuation theory in the last part of Chapter 3.

We quote one theorem from the literature.

1.6 THEOREM (Gravett). *Let* K *be a non-Archimedean valued field with residue class field* k *and value group* Γ. *Then* $\#K \leq (\#k)^{\#\Gamma}$.

A proof is given by F.J.Rayner in Ref. 182.

We shall not occupy ourselves with trivially valued fields. This does not mean that functional analysis over such fields is uninteresting. But for part of our theory it is essential that the valuation be nontrivial and we are simply too lazy to keep making exceptions. Some information on the subject is given by K. Gravett [82], P. Robert [195], and S. Warner [245].

For calculus over a non-Archimedean valued field, see the books of K. Mahler [137] and G. Bachman [8]. We restrict ourselves to making a few remarks about differentiation and power series.

Let K be a non-Archimedean valued field that is complete with respect to its valuation, the latter being nontrivial. Let X be a nonempty subset of K without isolated points. The derivative f' of a function $f : X \to K$ is defined in the usual manner. We have the ordinary formulas like $(fg)' = f'g + fg'$, $(f \circ g)' = (f' \circ g)g'$, $(d/dx)x^n = nx^{n-1}$. Antiderivation, however, causes great problems: it is not true that a function $f : K \to K$ has to be constant if $f' = 0$. In fact, as we shall see in the next chapter, K has many subsets that are both open and closed; the characteristic function of such a set has derivative 0.

What is worse, a function with derivative 0 may still be one to one. For an example, take the function $x \mapsto x^2$ for a field K that has characteristic 2. Another example is the function $\mathbb{Z}_p \to \mathbb{Q}_p$ that in the terminology of 1.F(iv) is given by

$$\sum_i s_i p^i \mapsto \sum_i s_i p^{2i} \qquad (s_i \in \{0, \ldots, p-1\})$$

This function was found by Dieudonné [46]. He also proved that every continuous function $\mathbb{Z}_p \to \mathbb{Q}_p$ has an antiderivative and that for every continuous map $F : \mathbb{Z}_p \times \mathbb{Q}_p \to \mathbb{Q}_p$ the differential equation $y' = F(x,y)$ has many solutions. Further, he proves an analogue of Sard's lemma: If $f : \mathbb{Z}_p \to \mathbb{Q}_p$ is differentiable, then the set $\{f(x) : x \in \mathbb{Z}_p, f'(x) = 0\}$ is negligible with respect to the Haar measure of (the locally compact group) $\mathbb{Q}_p$.

Examples of continuous, nowhere differentiable functions $\mathbb{Z}_p \to \mathbb{Q}_p$ are (for $p \neq 2$)

$$\sum_i s_i p^i \mapsto \sum_i s_i p^{2i} \qquad (s_i \in \{0, \ldots, p-1\})$$

(Dieudonné [46]) and Mahler's function [136]

$$x \mapsto \sum_n p^n \binom{x}{p^n}$$

where $\binom{x}{p^n} := \frac{x(x-1)\ldots(x-p^n+1)}{(p^n)!}$

Let K be a complete non-Archimedean valued field whose valuation is nontrivial. Let $a_0, a_1, a_2, \ldots \in K$. The set of all $x \in K$ for which the power series $\Sigma\, a_n x^n$ converges is

$$U := \{x \in K : \lim a_n x^n = 0\}$$

Therefore, there exists an $R \in [0,\infty]$ such that either $U = \{x : |x| < R\}$ or $U = \{x : |x| \leq R\}$. It turns out that the sum function

$$f : x \mapsto \sum_0^\infty a_n x^n \qquad (x \in U)$$

is differentiable (if $R \neq 0$) and that

$$f'(x) = \sum_1^\infty n a_n x^n \qquad (x \in U)$$

By means of power series one can define an exponential function and a logarithm in case the characteristic of K is not 0:

$$\exp x := \sum_0^\infty \frac{x^n}{n!}$$

$$\log(1-x) := -\sum_1^\infty \frac{x^n}{n}$$

(Both power series have positive convergence radii.) For the behavior of these functions and for the relations between them, see Bachman's book [8].

Let a_n, U and f be as above. J. de Groot [83] proved the following: If $c \in U$, there exist (unique) $b_0, b_1, \ldots,$ such that

$$f(x) = \Sigma\, b_n (x-c)^n \qquad (x \in U)$$

The series in the right-hand member converges if and only if $x \in U$. Thus, we have no analytic continuation.

A few references for power series are Refs. 2, 4, 34, 50, 51, 83, 123, 124 and 131.

In Chapter 6 we shall briefly consider Banach spaces and algebras that consist of power series.