1. Valuation Theory

In this section we introduce the concept of valuations for the fields under consideration. Namely, any valuation can be used to turn those fields into normed vector spaces. Hence, we have the notion of distance between different elements. Eventually this can be used for a completion of those spaces so that we have the usual tools for Banach spaces at hand.

Of course, the concept of a valuation imitates the role of the usual absolute value in the real or complex numbers. If we study polynomial rings in non-zero characteristic a transfer of that concept is by no means obvious. The situation is even worse for multivariate polynomials. In that case the values of powers of different variables need to be compared. Hence, the values will e.g. not any more belong to an archimedian ordered group (or ring) like the real numbers. Since multivariate polynomials will occur rarely in this book we will keep up a totally general concept only at the very beginning of our considerations.

The major emphasis in our discussion is on rings and orders rather than fields. Since these rings are entire their quotient fields always exist and we shall study valuations of fields rather than rings in this section. The development of the theory becomes much easier this way.

The essential properties of the ordinary absolute value $|\ \ |$ for elements of $\mathbb{R}$ or $\mathbb{C}$ are:

(1) $|x| \geq 0$ for all elements x with equality exactly for $x = 0$;
(2) $|x + y| \leq |x| + |y|$ for all elements x, y;
(3) $|xy| = |x|\,|y|$ for all elements x, y.

If v is to become a valuation of a given field F then clearly the set of values $v(x)$ $(x \in F)$ should be contained in a totally ordered commutative ring Φ. We need a total ordering so that we can distinguish any two values in Φ. For the properties 2. and 3. we also need to add and multiply values. Hence, we let Φ be a ring with a total ordering $<$. For any two elements α, β of Φ we have exactly one of the possibilities:

$$\alpha < \beta,\ \alpha = \beta,\ \beta < \alpha\ .$$

Any non-zero element α is therefore either positive $(0 < \alpha)$ or negative $(\alpha < 0)$. Also, we have the law of transitivity, i.e. for $\alpha < \beta$ and $\beta < \gamma$ we have $\alpha < \gamma$.

What we additionally need is the compatibility of $<$ with addition and multiplication in Φ. Imitating the total ordering of $\mathbb{R}$ we stipulate the following 2 axioms for the elements α, β of Φ:

(1) $\beta < \alpha$ implies $\beta + \gamma < \alpha + \gamma\ \forall \gamma \in \Phi$,
(2) $0 < \alpha$ and $0 < \beta$ implies $0 < \alpha\beta$.

Definition 1.1. *A totally ordered commutative ring* Φ *with properties 1. and 2. is called* **algebraically ordered**.

We demonstrate that conditions 1. and 2. above are sufficient for establishing the usual rules known for the ordering $<$ in $\mathbb{R}$.

Lemma 1.2. *For algebraically ordered rings* Φ *we have*

(1) $0 < \alpha \Leftrightarrow -\alpha < 0$,
(2) $\beta < \alpha \Leftrightarrow 0 < \alpha - \beta$,
(3) $0 < \alpha \Leftrightarrow \beta < \beta + \alpha$,
(4) $0 < \alpha$ *and* $\alpha + \beta = 0$ *implies* $\beta < 0$,
(5) $\alpha < 0$ *and* $\beta < 0$ *implies* $0 < \alpha\beta$,
(6) $\alpha < 0$ *and* $0 < \beta$ *implies* $\alpha\beta < 0$,
hence algebraically ordered rings are necessarily entire.
If Φ *has a unit element* $1 \neq 0$ *with respect to multiplication then we also have*
(7) $0 < 1$,
(8) $1 < \alpha$ *and* $0 < \beta$ *implies* $\beta < \alpha\beta$,
(9) $\alpha < 1$ *and* $0 < \beta$ *implies* $\alpha\beta < \beta$
for all $\alpha, \beta \in \Phi$.

Proof For $0 < \alpha$ we obtain $-\alpha < \alpha + (-\alpha) = 0$ by the first axiom, and likewise $-\alpha < 0$ implies $0 = (-\alpha) + \alpha < 0 + \alpha = \alpha$. This proves the first part. The second is obtained by adding $-\beta$ to $\beta < \alpha$, respectively β to $0 < \alpha - \beta$. Part (3) is an immediate consequence of axiom (1), and (4) follows from (3). Part (5) is immediate from $\alpha\beta = (-\alpha)(-\beta)$, part (1) and axiom (2). Then (6) follows from $0 = \alpha\beta + \alpha(-\beta)$ and (4).
Part (7) results from $1 = 1^2 = (-1)^2$, $1 \neq 0$, (1) and (5). For (8) we note that $\beta < \alpha\beta$ is tantamount to $0 < \beta(\alpha - 1)$ because of (2); hence, the result follows from axiom (2). Similarly, (9) follows from (2) and axiom (2).
□

Besides the total order relation $<$ we will also frequently use the notation $\alpha \leq \beta$ for either $\alpha < \beta$ or $\alpha = \beta$. Also we write $\alpha > \beta$ for $\beta < \alpha$ and $\alpha \geq \beta$ if either $\alpha > \beta$ or $\alpha = \beta$ holds.

On the rational numbers $\mathbb{Q}$ K. Hensel introduced valuations which behave rather differently from the previously only known single one, the ordinary absolute value.

Example Fixing $p \in \mathbb{P}$ every non-zero rational number x can be uniquely written in the form $x = \pm p^m \frac{a}{b}$ with $m \in \mathbb{Z}$ and $a, b \in \mathbb{N}$ such

that $p \nmid (ab)$. Hensel noticed that

$$| \ |_p : \mathbb{Q} \to \mathbb{R} : x \mapsto \left\{ \begin{array}{ll} p^{-m} & \text{for } x \neq 0 \\ 0 & \text{for } x = 0 \end{array} \right\}$$

indeed has the properties of the ordinary absolute value stated above. Instead of the triangle inequality we even get the stronger result

$$|x + y|_p \leq \max(|x|_p, |y|_p) \ .$$

This has far reaching consequences. For example,

$$R_p := \{x \in \mathbb{Q} \mid |x|_p \leq 1\}$$

becomes a ring, the so-called valuation ring with respect to $| \ |_p$. It is easily seen that R_p is a local ring with unique maximal ideal $\mathfrak{m} = \{x \in \mathbb{Q} \mid |x|_p < 1\}$. We emphasize the difference of the topologies introduced in $\mathbb{Z}$ by $| \ |$ and by $| \ |_p$. For any $0 < \varepsilon < 1$ the ε–neighborhood of 0 consists of $\{0\}$ in the first case and of $\{m \in \mathbb{Z} \mid p^k | m \text{ for } k > \log(\varepsilon)/\log(p)\}$. It is noteworthy that besides the ordinary absolute value all valuations of $\mathbb{Q}$ of interest are of that form.

We therefore distinguish two types of valuations, the archimedian ones like $| \ |$, and the non-archimedian ones like $| \ |_p$.

Definition 1.3. *Let F be a field. A mapping v of F into an algebraically ordered unital ring Φ is called a* **valuation***, if it has the properties*

(1) $0 < v(x)$ *for all* $x \in F^\times$ *and* $v(0) = 0$,
(2) $v(xy) = v(x)v(y)$ *for all* $x, y \in F$,
and either
(3) $v(x+y) \leq \max(v(x), v(y))$ *for all* $x, y \in F$ *(***non-archimedian valuation***),*
or only the weaker condition
(4) $v(x + y) \leq v(x) + v(y)$ *for all* $x, y \in F$ *(***archimedian valuation***).*

A valuation v with $v(F) = \{0, 1\}$ is called **trivial**.
In case $\Phi = \mathbb{R}$ the valuation is called **real**.

Remark We emphasize that for non-archimedian valuations v the values $v(x)$ for $x \in F^\times$ just need to form a totally ordered group, say G. Hence, $v(F) = G \cup \{0\}$ if we require $v(x) > 0$ for $x \neq 0$. For example, the p–adic valuations on $\mathbb{Q}$ introduced above have non-zero values in $\{p^k \mid k \in \mathbb{Z}\} \subset \mathbb{R}^{>0}$. We will later see that they are a special case of so-called discrete valuations (see ...)

Example Let F be a finite field of q elements and ω be a generator of $F^\times$. Because of $\omega^{q-1} = 1_F$ any valuation of F satisfies $v(\omega) = 1_\Phi$ and therefore $v(x) = 1_\Phi$ for all non-zero $x \in F$. Hence, finite fields admit only trivial valuations.

In practice, we are sometimes in a situation where the field F under consideration is the quotient field of an entire ring R. If we have a map v from R into an algebraically ordered field Φ which satisfies the axioms for a valuation stated in the previous definition then v can be easily extended to a valuation of F by setting

$$v(\frac{a}{x}) := \frac{v(a)}{v(x)} \ \ (a, x \in R,\ x \neq 0) \ .$$

We just need to check that this extension of v from R to F indeed has the properties (1)-(4) of 1.3. The first two of those are obvious. For the value of a sum we obtain

$$v(\frac{a}{x} + \frac{b}{y}) = v(\frac{ay + bx}{xy})$$

from which the property (3), respectively (4), immediately follows.

Since the non-archimedian valuations are more frequent than the archimedian ones and also less familiar we will discuss some of their properties in greater detail.

Lemma 1.4. *A non-archimedian valuation v of a field F has the properties:*

(1) $v(1) = 1$,
(2) $v(-x) = v(x)$,
(3) $v(x + y) = \max(v(x), v(y))$ *in case* $v(x) \neq v(y)$

for all $x, y \in F$.

Proof We have $v(1) = v(1^2) = v(1)^2$ implying $v(1) > 0$. Hence, we obtain $v(1) = 1$ by 1.2. Similarly, we get $v(-1) = 1$ and therefore $v(-x) = v(-1)v(x) = v(x)$. To prove the last property we assume without loss of generality that $v(x) < v(y)$ and conclude

$$\begin{aligned} v(y) = v(y + x + (-x)) &\leq \max(v(y + x), v(x)) \\ &= v(y + x) \leq \max(v(x), v(y)) = v(y) \ , \end{aligned}$$

where we necessarily must have equality everywhere.
□

Corollary 1.5. *Let us assume that the non-zero element x is algebraic over a given field F. If v is a non-archimedian valuation of $F(x)$ with*

$v(a) \leq 1$ for all $a \in F$ then we obtain $v(x) \leq 1$. If v is trivial on F, i.e. $v(a) = 1$ for all $a \in F$, then we also get $v(x) = 1$.

Proof The element x satisfies an equation

$$x^n + a_1 x^{n-1} + ... + a_{n-1}x + a_n = 0 \ \ (a_i \in F,\ 1 \leq i \leq n) \ .$$

It follows that

$$1 \geq v(a_n) = v(-x)v(x^{n-1} + a_1 x^{n-2} + ... + a_{n-1})$$

which cannot be true for $v(x) > 1$. In case $v(a_n) = 1$ clearly $v(x) = 1$ is the only possibility.

□

From now on we stipulate that all occuring valuations are non-trivial.

From the definition of non-archimedian valuations it is obvious that the elements with value ≤ 1 form a subring of F.

Proposition 1.6. *Let F be a field with non-archimedian valuation v. Then*

$$R_v := \{x \in F \mid v(x) \leq 1\}$$

*is a local ring (***valuation ring***) with maximal ideal (***valuation ideal***)*

$$\mathfrak{m}_v := \{x \in F \mid v(x) < 1\} \ .$$

Proof Since v is non-trivial there exist elements $x, y \in F$ with $v(x) < 1 < v(y)$. Then it is straightforward that the unit group of R_v is

$$U(R_v) = \{x \in F \mid v(x) = 1\} \ .$$

□

As we noted in the preceding proof the ring R_v is a proper subring of F. We use this for a characterization of valuation rings.

Theorem 1.7. *Let F be a field and R be a proper unital subring of F. R is a valuation ring for a suitable (non-archimedian) valuation v on F if and only if R has the property that for any non-zero $x \in F$ we have $x \in R$ or $x^{-1} \in R$.*

Proof If R is a valuation ring of a valuation v of F then $0 \in R$ and an arbitrary non-zero element $x \in F$ either satisfies $v(x) \leq 1$ or $v(x) > 1 > v(x^{-1})$.

The second part of the proof is quite tedious since we actually need to construct a valuation for F from the few prerequisites. The basic idea is to put elements $x, y \in F$ which will get the same value into

an equivalence class. From the definition of a valuation ring it is clear that non-zero x, y will have the same values if and only if $\frac{x}{y}$ is a unit in R.

In a first step we therefore introduce the following relation on F. We set

$$x \sim y :\Leftrightarrow (x = y = 0 \vee (\frac{x}{y} \wedge \frac{y}{x} \in R)) \ .$$

We remark that the only element related to 0 is 0 itself. Hence, we can reduce almost all of the following considerations to non-zero elements. We show that $\sim$ is an equivalence relation.
Because of $1 \in R$ the relation $\sim$ is reflexive. It is obviously symmetric. For the transitivity we note that $x \sim y$ and $y \sim z$ imply that $\frac{x}{z} = \frac{x}{y}\frac{y}{z}$ and $\frac{z}{x} = \frac{z}{y}\frac{y}{x}$ both belong to R, hence $x \sim z$.
Next we show that $\sim$ is compatible with multiplication.
For $x \sim y$ and $u \sim v$ we have $\frac{x}{y}$, $\frac{y}{x}$, $\frac{u}{v}$, $\frac{v}{u} \in R$. But then also $\frac{xu}{yv}$, $\frac{yv}{xu}$ belong to R implying that $xu \sim yv$.

Hence, the equivalence classes $C_a := \{x \in F \mid x \sim a\}$ $(a \in F^\times)$ form a multiplicative group G with unit element C_1. Clearly, $C_a^{-1} = C_{a^{-1}}$.

We show that G will be equipped with a total ordering if we define:

$$C_a > C_b :\Leftrightarrow (a \not\sim b \wedge a^{-1}b \in R) \ .$$

We need to prove that this definition is independent of the choice of representatives in the equivalence classes. For $a^{-1}b \in R$, $C_a = C_{\tilde{a}}$ and $C_b = C_{\tilde{b}}$ we have $a\tilde{a}^{-1}$, $\tilde{a}a^{-1}$, $b\tilde{b}^{-1}$, $\tilde{b}b^{-1} \in R$ implying $\tilde{a}^{-1}\tilde{b} = (\tilde{a}^{-1}a)(a^{-1}b)(b^{-1}\tilde{b}) \in R$, hence $C_{\tilde{a}} > C_{\tilde{b}}$. For $a, b \in F^\times$ there holds exactly one of the three relations

(1) $C_a = C_b$ in case $\frac{a}{b}, \frac{b}{a}$ are both contained in R,
(2) $C_a > C_b$ in case $\frac{b}{a} \in R$ and $\frac{a}{b} \notin R$,
(3) $C_b > C_a$ in case $\frac{a}{b} \in R$ and $\frac{b}{a} \notin R$.

Additionally we require $C_a > C_0$ for all $a \in F^\times$ which is compatible with the group operations. Henceforth we identify C_0 and 0.

Next we want to introduce a valuation of F with values in $G \cup \{0\}$. For this we put

$$\varphi : F \to G \cup \{0\} : a \mapsto C_a \ .$$

We need to verify the axioms of a valuation. According to our construction we have $v(a) \geq 0$ with equality exactly for $a = 0$. For the multiplicativity of v we note that $v(ab) = C_{ab} = C_aC_b = v(a)v(b)$ for all $a, b \in F$. Finally, we need to show $v(a+b) \leq \max(v(a), v(b))$. This is obvious if one of the summands is zero or if $a + b \sim a$, respectively $a + b \sim b$. We therefore assume that $C_a \neq C_{a+b} \neq C_b$ and have to show that $C_{a+b} > C_a$ and $C_{a+b} > C_b$ cannot both hold. Namely, in that

case we had $a(a+b)^{-1}$, $b(a+b)^{-1} \in R$ and $(a+b)a^{-1}$, $(a+b)b^{-1} \notin R$. Because of $1 \in R$ the latter implies $\frac{b}{a}, \frac{a}{b} \notin R$, which is in contradiction with our assumptions on R.

We will also show how to obtain a valuation from this in accordance with Definition 1.3. This means that we have to embed $G \cup \{0\}$ into a suitable algebraically ordered ring. The easiest way to do this is to introduce the group ring

$$\Phi := \mathbb{Z}[G] = \left\{ \sum_{g \in G} m_g g \,\middle|\, m_g \in \mathbb{Z},\ m_g = 0 \text{ for almost all } g \in G \right\} \ .$$

The group G is embedded into Φ via

$$\tilde{\iota} : G \to \Phi : g \mapsto 1 \cdot g \ .$$

We also obtain the zero element of Φ as unique image of C_0 so that the embedding can be canonically extended to

$$\iota \,:\, G \cup \{0\} \to \Phi \,:\, g \mapsto \begin{cases} 1 \cdot g & \text{for } g \neq 0 \\ 0 & \text{for } g = 0 \end{cases} \ .$$

Next we introduce an ordering of Φ via

$$\sum_{g \in G} m_g g > \sum_{g \in G} n_g g \quad :\Leftrightarrow \ (\exists g_0 \in G \ : \ m_{g_0} > n_{g_0} \\ \wedge (\forall g \in G :\ g > g_0 \Rightarrow m_g = n_g)) \ .$$

It is easily seen that $>$ is indeed a total ordering of Φ. What we need, however, is that Φ is algebraically ordered. According to Definition 1.1 we must verify for $\alpha := \sum_{g \in G} m_g g$, $\beta := \sum_{g \in G} n_g g \in \Phi$ that

(1) $\alpha > 0$ implies $\beta + \alpha > \beta$ for all α, $\beta \in \Phi$.
In case $\alpha > 0$ there is an element $g_a \in G$ with $m_{g_a} > 0$ and $m_g = 0$ for all $g \in G$, $g > g_a$. But then the highest index for which the sums for $\beta + \alpha$ and β differ is also g_a, and we clearly have $m_{g_a} + n_{g_a} > n_{g_a}$.

(2) $\alpha > 0$ and $\beta > 0$ yields $\alpha\beta > 0$.
We take up the notations for α, β in 1. and also require that $g_b \in G$ satisfies $n_{g_b} > 0$ and $n_g = 0$ for all $g > g_b$ in G. Then we get

$$\alpha\beta = \sum_{g \in G} \left(\sum_{g_1 g_2 = g} m_{g_1} n_{g_2} \right) g \ .$$

For $g > g_a g_b$ in $g = g_1 g_2$ we must have either $g_1 > g_a$ with $m_{g_1} = 0$ or $g_2 > g_b$ with $n_{g_2} = 0$, in each case the inner sum is zero. Similarly, we see that the highest non vanishing coefficient occurs for $g = g_a g_b$. It equals $m_{g_a} n_{g_b} > 0$.

Since the embedding ι of $G \cup \{0\}$ into Φ obviously satisfies $\iota(g) > \iota(h)$ for $g > h$ we have indeed obtained a valuation of F with values in an algebraically ordered ring.

□

We list a few consequences of that theorem.

Lemma 1.8. *If the ring R is a valuation ring then any two ideals $\mathfrak{a}, \mathfrak{b}$ satisfy either $\mathfrak{a} \subseteq \mathfrak{b}$ or $\mathfrak{b} \subseteq \mathfrak{a}$.*

Proof. We assume that neither $\mathfrak{a}$ is contained in $\mathfrak{b}$ nor $\mathfrak{b}$ in $\mathfrak{a}$. Then there are (non-zero) elements $a \in \mathfrak{a} \setminus \mathfrak{b}, b \in \mathfrak{b} \setminus \mathfrak{a}$. Then either $\frac{a}{b}$ or $\frac{b}{a}$ belongs to R and we get $\frac{a}{b}b = a \in \mathfrak{b}$ in the first case or $\frac{b}{a}a = b \in \mathfrak{a}$ in the second. This contradicts the choice of a, b.

□

Corollary 1.9. *A noetherian valuation ring is a principal ideal domain.*

Proof. Let $a_1, ..., a_n$ be generators of an ideal $\mathfrak{a}$, i.e. we have $\mathfrak{a} = Ra_1 + ... + Ra_n$. Among the ideals $Ra_i \ \ (1 \leq i \leq n)$ there is a largest one and without loss of generality we can assume that this is Ra_1. This yields $\mathfrak{a} \supseteq Ra_1 \supseteq Ra_1 + ... + Ra_n = \mathfrak{a}$, hence $\mathfrak{a} = Ra_1$.

□

Next we show that non-trivial non-archimedian valuations exist for fields with suitable subrings. (The prerequisites clearly exclude finite fields.)

Lemma 1.10. *(Chevalley) Let F be a field and R be a proper subring of F containing 1 and a non-zero prime ideal $\mathfrak{p}$. Then there exists a valuation ring Φ of F with maximal ideal $\mathfrak{m}$ satisfying $R \subset \Phi$ and $\mathfrak{m} \cap R = \mathfrak{p}$.*

Proof The general case is reduced to the one in which R is a local ring. We start with that reduction.

In case R itself is not a local ring we obtain upon localization with respect to $\mathfrak{p}$:

$$R \subset \tilde{R} := \frac{R}{R \setminus \mathfrak{p}} \subset F \ .$$

$\tilde{R}$ is a local ring with maximal ideal $\tilde{\mathfrak{p}} = \frac{\mathfrak{p}}{R \setminus \mathfrak{p}}$. Assuming the result for local rings there exists a valuation ring Φ with $\tilde{R} \subset \Phi$ and the maximal ideal $\mathfrak{m}$ of $\tilde{R}$ satisfies $\mathfrak{m} \cap \tilde{R} = \tilde{\mathfrak{p}}$. Clearly, R is contained in Φ and for the intersection of $\mathfrak{m}$ with R we obtain

$$\mathfrak{m} \cap R \ = \ \mathfrak{m} \cap (\tilde{R} \cap R) \ = \ (\mathfrak{m} \cap \tilde{R}) \cap R \ = \ \tilde{\mathfrak{p}} \cap R \ = \ \mathfrak{p} \ .$$

Henceforth, we assume that R itself is local. To exhibit a candidate for Φ we consider the set

$$\mathcal{M} := \{S \mid R \subseteq S \subset F\,,\ S \text{ a ring with } 1 \notin \mathfrak{p}S\}\ .$$

$\mathcal{M}$ is not empty since it contains R. According to Zorn's lemma it contains a maximal element, say T. We will show that T is indeed the valuation ring we are looking for. From our assumptions we know that $1 \notin \mathfrak{p}T$, hence $\mathfrak{p}$ is contained in a maximal ideal $\mathfrak{a}$ of T. Then $\mathfrak{a}$ does not contain 1 either, and 1 is also not an element of $\mathfrak{p}\frac{T}{T\setminus\mathfrak{a}}$ because of $T \cap \frac{\mathfrak{p}T}{T\setminus\mathfrak{a}} \subseteq T \cap \frac{\mathfrak{a}}{T\setminus\mathfrak{a}} = \mathfrak{a}$. Hence, the localization of T at $\mathfrak{a}$ belongs to $\mathcal{M}$, it must therefore coincide with T, i.e. T is a local ring. According to our assumptions we know that R is a subring of T. Also, the maximal ideal $\mathfrak{a}$ of T intersects R in $\mathfrak{p}$ since R is a local ring.

We still need to show that T is a valuation ring, i.e. that for $x \in F\setminus T$ the inverse element x^{-1} is in T. Because of $T \subset T[x]$ we must have $1 \in \mathfrak{p}T[x]$, and there exists a presentation

$$1 = -\sum_{i=0}^{m} a_i x^i \ \ (a_i \in \mathfrak{a},\ a_m \neq 0)\ .$$

If there exist elements $x \in F$ with $x \notin T$ and $x^{-1} \notin T$ we choose such an x which has a representation of 1 in which the exponent of the maximal occuring power x^m is as small as possible. The element $1 + a_0$ is not in $\mathfrak{a}$ and is therefore a unit of T. Setting $b_i = \frac{a_i}{1+a_0}$ the representation of 1 becomes

$$1 + \sum_{i=1}^{m} b_i x^i \ = \ 0\ ,$$

or

$$(x^{-1})^m + \sum_{i=1}^{m} b_i (x^{-1})^{m-i} \ = \ 0\ .$$

This has the consequence that the proper overring $T[x^{-1}]$ of T equals the finite sum $\sum_{i=0}^{m-1} Tx^{-i}$. Hence, we obtain $1 \in \mathfrak{a}[x^{-1}] = \sum_{i=0}^{m-1} \mathfrak{a}x^{-i}$ and therefore a representation of 1 for which the maximal occuring exponent is smaller. Consequently, every element x of F either belongs to T or its inverse x^{-1} does. This means that T is indeed a valuation ring of F.

□

Corollary 1.11. *Let F be a field and R be a proper subring of F containing 1 and a non-zero ideal $\mathfrak{b} \subset R$. Then there exists a valuation ring Φ of F with maximal ideal $\mathfrak{m}$ satisfying $R \subset \Phi$ and $\mathfrak{b} \subset \mathfrak{m}$.*

Next we study the extension of valuations for field extensions. From the simple example $E = \mathbb{Q}(\sqrt[3]{2})$ we conclude that an extension of the 2-adic valuation from $\mathbb{Q}$ to E must satisfy $\mid \sqrt[3]{2} \mid_2 = 2^{-1/3}$. We must therefore assume that the algebraically ordered ring Φ contains the appropriate elements.

Definition 1.12. *A group G is called* **divisible** *if the equation $x^n = \alpha$ has a solution $x \in G$ for every $\alpha \in G$ and every $n \in \mathbb{N}$.*

Theorem 1.13. *(Chevalley) Any non-archimedian valuation v of a field F into an algebraically ordered ring Φ with divisible multiplicative group can be extended to a valuation of every field E containing F.*

Proof We consider the set $\mathcal{S}$ of all fields K between F and E to which v can be extended. Because of $F \in \mathcal{S}$ the set $\mathcal{S}$ contains a maximal element, say K_0. We need to consider the following two cases separately:
(i) there is an element $x \in E \setminus K_0$ which is transcendental over K_0;
(ii) E is algebraic over K_0.

In the first case we extend the prolongation of v from F to K_0 (which we again denote by v) to a valuation w of $K_0(x)$. We define

$$w : K_0[x] \to \Phi : f(x) = \sum_{i=0}^{n} a_i x^i \mapsto \max\{v(a_i) \mid 0 \leq i \leq n\}$$

and verify that w satisfies the axioms of a valuation on $K_0[x]$. Clearly, $w(f(x)) \geq 0$ for all polynomials $f(x)$ and $w(f(x))$ equals 0 if and only if $f(x) = 0$. For polynomials $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{i=0}^{n} b_i x^i$ (here we admit 0 for the leading coefficient to make the presentation easier) we get

$$\begin{aligned} w(f(x)+g(x)) &= \max\{v(a_i+b_i) \mid 0 \leq i \leq n\} \\ &\leq \max\{\max\{v(a_i), v(b_i)\} \mid 0 \leq i \leq n\} \\ &\leq \max\{\max\{v(a_i) \mid 0 \leq i \leq n\}, \max\{v(b_i) \mid 0 \leq i \leq n\}\} \\ &= \max\{w(f(x)), w(g(x))\} \end{aligned}$$

For the verification of the multiplicativity of w we assume that $\rho, \sigma \in \{0, 1, ..., n\}$ are minimal subject to $v(a_\rho) = w(f(x))$, $v(b_\sigma) = w(g(x))$.

Also we put $a_i = 0, b_i = 0$ for $i = n+1, ..., 2n$. Then

$$\begin{aligned} w(f(x)g(x)) &= \max\{v\left(\sum_{k=0}^{i} a_k b_{i-k}\right) \mid 0 \leq i \leq 2n\} \\ &\leq \max\{\max\{v(a_k), v(b_{i-k}) \mid 0 \leq k \leq i\} \mid 0 \leq i \leq 2n\} \\ &\leq \max\{v(a_i) \mid 0 \leq i \leq n\} \max\{v(b_i) \mid 0 \leq i \leq n\} \\ &= w(f(x))w(g(x)) \end{aligned}$$

and

$$v\left(\sum_{k=0}^{\rho+\sigma} a_k b_{\rho+\sigma-k}\right) \;=\; v(a_\rho)v(b_\sigma) \;=\; w(f(x))w(g(x))$$

prove that w is indeed multiplicative.

Eventually we must extend w from $K_0[x]$ to the quotient field $K_0(x)$ by setting

$$w : K_0(x) \to \Phi : \frac{f(x)}{g(x)} \mapsto \frac{w(f(x))}{w(g(x))} \quad .$$

We already proved that this extension of a valuation w from a ring to its quotient ring yields a valuation of the latter.

Since it extends v this is a contradiction to the maximal choice of K_0.

In the second case we either have $K_0 = E$ and we are done, or there exists an element $x \in E \setminus K_0$ which is algebraic over K_0. Let $f(t) \in K_0[t]$ be the minimal polynomial of such an element x, say of degree $n > 1$.

According to Chevalley's Lemma 1.10 there exists a valuation w of $K_1 := K_0(x)$ such that the correswponding valuation ring R_w contains R_v and that the intersection of the valuation ideal $\mathfrak{m}_w$ with R_v equals $\mathfrak{m}_v$. We note that any element $z \in K_0 \setminus R_v$ satisfies $v(z^{-1}) < 1$ so that z^{-1} is in $\mathfrak{m}_v$. Therefore z^{-1} also belongs to $\mathfrak{m}_w$ and we have $z \notin \mathfrak{m}_w$. This yields

$$\mathfrak{m}_w \cap K_0 \;=\; \mathfrak{m}_v \quad .$$

We recall that $H = v(K_0^\times)$ and $\tilde{H} = w(K_1^\times)$ are algebraically ordered abelian groups. Because of

$$\forall z \in K_0 \;:\; v(z) < 1 \Leftrightarrow w(z) < 1$$

we get

$$\forall y, z \in K_0 \;:\; v(y) < v(z) \Leftrightarrow w(y) < w(z)$$

and the mapping

$$\tau \;:\; H \to \tilde{H} \;:\; v(z) \mapsto w(z)$$

is an order preserving group monomorphism. We want to show that the image $\tau(H)$ is of finite index in $\tilde{H}$.

For arbitrary $s \in \mathbb{N}$ we choose $y_1, ..., y_s \in K_1^\times$ such that $w(y_i)\tau(H)$ are pairwise distinct elements of $\tilde{H}/\tau(H)$. We will show that $y_1, ..., y_s$ are K_0 linearly independent with the consequence that the index of $\tau(H)$ in $\tilde{H}$ is bounded by $n = [K_1 : K_0]$. For any representation of 0 of the form

$$0 \ = \ \sum_{i=1}^{s} a_i y_1 \ \ (a_i \in K_0)$$

we obtain

$$\begin{aligned} 0 = w(0) &= w(\sum_{i=1}^{s} a_i y_i) \\ &= \max\{w(a_i y_i) \mid 1 \leq i \leq s\} \ \text{(since these values are all different)} \\ &= \max\{w(a_i)w(y_i) \mid 1 \leq i \leq s\} \ , \end{aligned}$$

hence, $w(a_i) = 0$ implying $a_i = 0$ for $i = 1, ..., s$ and $y_1, ..., y_s$ are K_0-linearly independent.

Consequently, there is a fixed exponent m such that for every $g \in \tilde{H}$ we have $g^m \in \tau(H)$, respectively for all $y \in K_1^\times$ there is $z \in K_0^\times$ with $w(y)^m = \tau(v(z))$. We can therefore define the mapping

$$T \ : \ \tilde{H} \to \Phi \ : \ w(y) \mapsto v(z)^{1/m} \ .$$

It is well defined since τ is injective and Φ algebraically ordered and divisible. It is also multiplicative since τ has this property. The mapping T is used to extend v to K_1 via

$$\hat{v} \ : \ K_1 \to \Phi \ : \ y \mapsto \begin{cases} 0 & \text{for } y = 0 \\ T(w(y)) & \text{otherwise} \end{cases} \ .$$

Clearly, $\hat{v} \mid_{K_0} = v$. It remains to show that $\hat{v}$ has the properties of a valuation. $\hat{v}(0) = 0$ and $\hat{v}(y) > 0 \forall y \in K_1^\times$ follow immediately from the definition of $\hat{v}$. For $y, \tilde{y} \in K_1^\times$ there are $z, \tilde{z} \in K_0^\times$ subject to $w(y)^m = \tau(v(z)$ and $w(\tilde{y})^m = \tau(v(\tilde{z})$. Since τ is multiplicative we obtain $w(y\tilde{y})^m = \tau(v(z\tilde{z})$. From this $\hat{v}(y\tilde{y}) = \hat{v}(y)\hat{v}(\tilde{y})$ is obvious (also for $y = 0$ or $\tilde{y} = 0$). Eventually, we need to show the strong triangular inequality. We have

$$w(y + \tilde{y})^m \leq (\max\{w(y), w(\tilde{y})\})^m = \max\{w(y)^m, w(\tilde{y})^m\}$$

and fix $\acute{z} \in K_0^\times$ subject to $\tau(v(\acute{z})) = w(z + \tilde{z})^m$. Since τ is order preserving we know that $v(\acute{z}) \leq \max\{v(z), v(\tilde{z})\}$ and therefore also $v(\acute{z})^{1/m} \leq \max\{v(z)^{1/m}, v(\tilde{z})^{1/m}\}$. From this $T(w(y + \tilde{y})) \leq$

$\max\{T(w(y)), T(w(\tilde{y}))\}$ and $\hat{v}(y+\tilde{y}) \leq \max\{\hat{v}(y), \hat{v}(\tilde{y})\}$ are immediate.

□

As shortly discussed in the example about Hensel's p-adic valuations for the rational number field any valuation of a field F defines a topology for F.

Definition 1.14. *Two valuations v_i $(i = 1, 2)$ of a field F are called* **equivalent** *if they define the same topology on F, i.e. the sets $\{x \in F \mid v_1(x) < 1\}$ and $\{x \in F \mid v_2(x) < 1\}$ coincide.*

For example, the archimedian valuations $|\ \ |$ and $|\ \ |^c$ for any real number $0 < c \leq 1$ are equivalent on $\mathbb{C}$. The same holds for the p-adic valuations $|\ \ |_p$ and $|\ \ |_p^c$ on $\mathbb{Q}$. Usually, we are only interested in the topology and will therefore consider classes of equivalent valuations rather than a single representative of any such class. We note that for non-archimedian valuations the valuation rings and valuation ideals coincide for all valuations within a fixed equivalence class.

We already saw that non-archimedian valuations v of fields F have values $v(x)$ for $x \neq 0$ in an algebraically ordered group. For our purposes it is most interesting when the image $v(F^\times)$ is a cyclic group, say $\langle\gamma\rangle$. Then there exists an element π in the valuation ideal $\mathfrak{m}_v$ of v with $v(\pi) = \gamma$ and we can identify $v(F^\times)$ with $\mathbb{Z}$. Non-trivial non-archimedian valuations with this property are called **discrete**. Discrete valuations will play a predominant role in what follows since they have special important properties. One of those is described in the next lemma.

Lemma 1.15. *The valuation ring R_v of a discrete valuation v is a principal ideal ring. Its proper ideals are of the form $\mathfrak{a} = \mathfrak{m}_v^k$ with $k \in \mathbb{N}$.*

Proof There is an element π - naturally in $\mathfrak{m}_v$ - with $v(\pi)$ generating $v(F^\times)$. We claim that $\mathfrak{m}_v$ coincides with πR_v. Clearly, we have $\pi R_v \subseteq \mathfrak{m}_v$. On the other hand, for any $x \in \mathfrak{m}_v$ we get $x/\pi \in R_v$ and therefore $\mathfrak{m}_v \subseteq \pi R_v$.
For non-zero ideals $\mathfrak{a}$ of R_v we conclude analogously that any $\alpha \in \mathfrak{a}$ subject to $v(\alpha) = \max\{v(x) \mid x \in \mathfrak{a}\}$ satisfies

$$\mathfrak{a} = \alpha R_v = \pi^{\nu_v(\alpha)} R_v$$

for a suitable exponent $\nu_v(\alpha)$ depending on v and α. □

Hence, discrete valuations can also be written additively rather than multiplicatively. For his we choose a generating element π of $\mathfrak{m}_v$. Then

for any non-zero $x \in F$ there is a unique exponent m such that $x\pi^{-m}$ is a unit of the valuation ring R_v. Since two different generators of $\mathfrak{m}_v$ also differ by a unit of R_v we can define the map

$$\nu = \nu_v := F \to \mathbb{Z} \cup \{\infty\} : x \mapsto \begin{cases} m & \text{for} \quad x \neq 0 \\ \infty & \text{for} \quad x = 0 \end{cases}$$

The map ν is called an **exponential valuation** of F. The properties of v immediately yield the correponding ones for exponential valuations:

(1) $\nu(x) = \infty$ if and only if $x = 0$;
(2) $\nu(xy) = \nu(x) + \nu(y)\ \forall x, y \in F$;
(3) $\nu(x + y) \geq \min(\nu(x), \nu(y)) \forall x, y \in F$;
(4) $\nu(\pi) = 1$, hence, the map ν is surjective.

Any non-archimedian valuation v of a finite extension E of F restricts to a valuation v_0 on F. The group $v(F^\times)$ is a subgroup of finite index in $v(E^\times)$ according to the proof of Chevalley's Theorem. If v is discrete then the same holds for v_0. We can therefore attach an exponential valuation to it similar as above. However, we note that if ν is an exponential valuation on E then its restriction ν_0 to F is in general not surjective anymore.

Conversely, if we start with a discrete valuation v_0 on F it has prolongations v to any finite extension E of F according to Chevalley's Theorem and $G := v(F^\times)$ is of finite index, say k, in $v(E^\times)$. Let $\xi_1, ..., \xi_k \in R_v \subset E$ subject to

$$v(E^\times) = \dot{\bigcup_{i=1}^{k}} v(\xi_i)G$$

and

$$v(\xi_i) > \max\{v(x) \mid x \in F \cap R_{v_0}\} \ .$$

The values $v(\xi_i)$ are pairwise distinct and we can assume that $v(\xi_1) > v(\xi_j)$ for $2 \leq j \leq k$. But then we obtain exponents m_j satisfying $v(\xi_1^{m_j}) = v(\xi_j)$. But this yields $v(E^\times) = \langle v(\xi_1) \rangle$ showing that v is necessarily discrete.

From now on we assume that all valuations v of a given field are real, i.e. $v(F) \subseteq \mathbb{R}^{\geq 0}$.

We will see that this restriction is still sufficient to cover all valuations of global fields and we can additionally use all the properties of real numbers, especially limits of sequences.

Proposition 1.16. *(Characterization of archimedian valuations) Let F be a field with a valuation $v : F \to \mathbb{R}^{\geq 0}$. Then v is non-archimedian if and only if the set of values $v(\mathbb{N})$ is bounded. (Here $\mathbb{N}$ denotes the natural numbers viewed as sums of ones which are contained in F.)*

Proof If v is non-archimedian then the set $v(\mathbb{N})$ is bounded because of $v(n) \leq v(1)$ for all $n \in \mathbb{N}$.
On the other hand, let us assume that $v(n) \leq M$ holds for all natural numbers n. Then we obtain for $x, y \in F$ with $\max\{v(x), v(y)\} = W$

$$\begin{aligned} v(x+y)^n &= v(\sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}) \\ &\leq \sum_{i=0}^{n} MW^n \\ &= (n+1)MW^n \end{aligned}$$

Hence,

$$v(x+y) \leq ((n+1)M)^{1/n} W \ ,$$

where the right-hand side converges to W for $n \to \infty$.
□

We are now in a position to determine - up to equivalence - all non-trivial valuations of our base fields, the field of rational numbers and rational function fields in one variable over finite fields.

Example
(i) We want to determine all non-trivial valuations v of the rational numbers.
In the first part we assume that $v(n) \leq 1$ for all natural numbers n, and therefore also for all elements of $\mathbb{Z}$. Since v is non-trivial there exists a smallest natural number bigger than one, say p, with $c := v(p) < 1$. It is easy to see that p must be a prime number. If q is a prime number different from p, then we must necessarily have $v(q) = 1$. Namely, in case $v(q) < 1$ there exists a natural number n such that $v(p^n) < \frac{1}{2}$, $v(q^n) < \frac{1}{2}$ and the extended Euclidean algorithm yields elements $\mu, \nu \in \mathbb{Z}$ with $\mu p^n + \nu q^n = 1$. This yields the contradiction

$$1 = v(1) \leq v(\mu p^n) + v(\nu q^n) \leq v(p^n) + v(q^n) < 1 \ .$$

Now, every non-zero element $x \in \mathbb{Q}$ can be uniquely written in the form $x = p^\kappa \frac{r}{s}$ with $\kappa \in \mathbb{Z}$ and $r \in \mathbb{Z} \setminus \{0\}, s \in \mathbb{N}$ such that p does not divide rs. Then the v-value of x is $v(x) = c^\kappa$. This and $v(0) = 0$ imply that v is equivalent to the p-adic valuation of $\mathbb{Q}$. For the latter we normalize to $c = \frac{1}{p}$.

Alternatively, let us assume that there exists an element $b \in \mathbb{N}$, more precisely $b \in \mathbb{Z}^{>1}$, with $v(b) > 1$. We fix b. Now let g be an arbitrary element of $\mathbb{Z}^{>1}$. We consider the g-adic expansion of b^n for $n \in \mathbb{N}$:

$$b^n \ = \ \sum_{m=0}^{N_n} c_{nm} g^m \ \ (0 \leq c_{nm} < g, c_{nN_n} \neq 0) \ .$$

As a consequence we have $b^n \leq g^{N_n}$, hence $N_n \leq n \log b / \log g$. Because of $v(0) = 0$ and $v(1) = 1$ the trinagle inequality yields $v(m) \leq m$ for all $m \in \mathbb{Z}^{\geq 0}$. Setting $M := \max\{1, v(g)\}$ we obtain

$$v(b)^n \leq \sum_{m=0}^{N_n} v(c_{nm} g^m) \leq g(N_m{+}1) M^{N_n} \leq g \left(\frac{n \log b}{\log g} + 1 \right) \left(M^{\log b / \log g} \right)^n \ .$$

At this stage we need a result from elementary calculus:
Because of

$$\forall \varepsilon > 0 \forall n \in \mathbb{N} \ : \ (1+\varepsilon)^n \geq 1 + n\varepsilon + \frac{n(n-1)}{2} \varepsilon^2$$

all $\gamma \in \mathbb{R}^{>0}$ for which the sequence $\left(\frac{\gamma^n}{n}\right)_{n \in \mathbb{N}}$ is bounded in $\mathbb{R}$ must lie in the half open interval $]0, 1]$.

Applying this result to $\gamma := v(b) / M^{\log b / \log g}$ we see that $\gamma \leq 1$ and conclude that $M > 1$ with the consequence $M = v(g)$. But then $\gamma \leq 1$ is tantamount to $\log v(b) / \log b \leq \log v(g) / \log g$.
Because of $v(g) > 1$ we can interchange the rôles of b and of g and get

$$s := \log v(b) / \log b = \log v(g) / \log g$$

for all $g \in \mathbb{Z}^{>1}$, respectively $v(g) = g^s$. Hence, v is equivalent to the ordinary absolute value on $\mathbb{Q}$. We note that s is necessarily bounded from above by 1 since otherwise the triangle inequality is violated: $2^s = |1+1|^s$ should be bounded by $1^s + 1^s = 2$.

(ii) Let $K := \mathbb{F}_q(t)$ be the rational function field over the finite field $\mathbb{F}_q$ with $q = p^n$ elements, p a prime number. We shall see that in this case all non trivial valuations on K are non archimedian.

We recall that every valuation acts trivial on $\mathbb{F}_q$. Imitating our conclusions for $\mathbb{Q}$ we distinguish the following two cases. At first we assume that $v(f) \leq 1$ for all f in $\mathbb{F}_q[t]$. Again, since v shall not be trivial there must exist a polynomial of lowest (positive) degree, say π, with $c := v(\pi) < 1$ and this polynomial is necessarily irreducible. Without loss of generality we can assume that π is monic, hence a prime polynomial of $\mathbb{F}_q[t]$. As in (i) we deduce that every prime polynomial ψ of $\mathbb{F}_q[t]$ different from π must have v-value 1. Also in this case every non zero element of $\mathbb{F}_q[t]$ can be written in the form $x = \pi^\kappa \frac{f}{g}$ with $\kappa \in \mathbb{Z}$

and $r \in \mathbb{F}_q[t] \setminus \{0\}, s \in \mathbb{F}_q[t]$ such that π does not divide fg. Then the v-value of x is $v(x) = c^\kappa$. This and $v(0) = 0$ imply that v is equivalent to the π-adic valuation of $\mathbb{F}_q$ which is obtained upon normalizing the constant c to $q^{-\deg(\pi)}$.

We remark that the normalization of the non trivial valuations of $\mathbb{Q}$ (p-adic valuations, respectively the ordinary absolute value) leads to the so-called **product formula**. We denote the set of all those valuations of $\mathbb{Q}$ by $V_\mathbb{Q}$ and get

$$\prod_{v \in V_\mathbb{Q}} v(x) \;=\; 1 \;\; \forall x \in \mathbb{Q} \setminus \{0\} \;\; .$$

The proof of that formula is straightforward and left as an exercise to the reader. Analogously, the normalization of the valuations of a rational function field over a finite field of constants yields a product formula. Again, we leave the proof as an exercise to the reader.

We will now demonstrate that field elements of a global field F can be approximated with respect to inequivalent valuations. In the next two sections we will learn that the set R of F defined by

$$R := \{x \in F \mid m_{x/F_0}(t) \in R_0[t]\}$$

is a subring of F which is also a free R_0-module of rank $n = (F : F_0)$. R is even a **Dedekind Ring** meaning that every non-zero ideal of R is a product of prime ideals. That presentation is unique up to the order of the factors. This additional information allows us to determine all non-trivial non-archimedian valuations in F up to equivalence. We recall that two non-archimedian valuations of a field are called equivalent if their valuation rings coincide.

By Chevalley's Lemma we know that for every non-zero prime ideal $\mathfrak{p}$ of R there is a valuation ring R_v of F with maximal ideal $\mathfrak{m}_v$ such that $R \subseteq R_v$ and $\mathfrak{m}_v \cap R = \mathfrak{p}$. We want to show that any such valuation ring R_v coincides with $\tilde{R} := \frac{R}{R \setminus \mathfrak{p}}$. Since in that ring all occuring denominators are units in R_v it is contained in any valuation ring R_v with the stipulated properties $R \subseteq R_v$ and $\mathfrak{m}_v \cap R = \mathfrak{p}$.

We show that $\tilde{R} \subseteq R_v$ implies equality. Since the intersection $\tilde{R} \cap \mathfrak{m}_v$ contains the maximal ideal $\tilde{\mathfrak{p}}$ of $\tilde{R}$ both ideals must coincide. We will show below that $\tilde{R}$ is the valuation ring of the $\mathfrak{p}$-adic valuation $v_\mathfrak{p}$ of F. Then any element $x \in F$ satisfies

$$v_\mathfrak{p}(x) \leq 1 \;\text{ implies }\; v(x) \leq 1$$

since $\tilde{R}$ is contained in R_v, and also $v_{\mathfrak{p}}(x) > 1$ implies $v(x) > 1$ since $1/x$ is in $\tilde{\mathfrak{p}}$ and therefore in $\mathfrak{m}_v$. Hence, both valuation rings indeed coincide.

We still need to show that $\tilde{R}$ is a valuation ring. We recall that R is a Dedeking ring. In Section ... we show that every non-zero ideal $\mathfrak{a}$ of R is a product of prime ideals and that presentation is unique up to the order of the factors. For each non-zero prime ideal $\mathfrak{p}$ of R we can therefore define a map

$$\nu_{\mathfrak{p}} = \nu \,:\, R \to \mathbb{Z} \cup \{\infty\} \,:\, x \mapsto \begin{cases} \infty & \text{for } x = 0 \\ m & \text{for } x \neq 0\,,\ xR = \mathfrak{p}^m\mathfrak{q} \text{ with } \mathfrak{p} \nmid \mathfrak{q} \end{cases}$$

which clearly satisfies the axioms of a non-archimedian exponential valuation. We leave this as an exercise to the reader. The proof is analogous to that for the p-adic valuations of $\mathbb{Z}$. Extending ν to the quotient field F of R we obtain the so-called **$\mathfrak{p}$-adic exponential valuation** of F.

Hence, we have shown that the non-trivial non-archimedian valuations of F which contain R in their valuation ring are exactly the $\mathfrak{p}$-adic valuations. Those are discrete.

Theorem 1.17. *(***Weak Approximation Theorem***)*
Let $v_1, ..., v_n$ be pairwise inequivalent non-archimedian real valuations of the global field F and let $x_1, ..., x_n \in F$. Then for every $\varepsilon > 0$ there exists an element $x \in F$ satisfying $v_i(x - x_i) < \varepsilon$ $(1 \leq i \leq n)$.

Since every v_i coresponds to a unique prime ideal of R the theorem coincides with the Chinese Remainder Theorem if the elements x_i $(1 \leq i \leq n)$ belong to R and R is contained in the valuation rings R_{v_i}.

Proof The proof is done in 3 steps.

(1) We show by induction on n that F contains an element a with the properties $v_1(a) > 1$ and $v_i(a) < 1$ $(2 \leq i \leq n)$.

We start with $n = 2$. Because of $R_{v_1} \neq R_{v_2}$ the valuation rings cannot be contained in each other (see above) and there exist elements $b, c \in F$ subject to $c \in R_{v_1} \setminus R_{v_2}$, $b \in R_{v_2} \setminus R_{v_1}$. Then $a := b/c$ satisfies $v_1(a) > 1 > v_2(a)$. For the induction step from $n-1$ to n we can assume that there exist elements $b, c \in F$ with $v_1(b) > 1$, $v_i(b) < 1$ $(2 \leq i \leq n-1)$, $v_1(c) > 1$, $v_n(c) < 1$.

In case of $v_n(b) < 1$ the element $a := b^m c$ does the job for every sufficiently large exponent $m \in \mathbb{N}$. For $v_n(b) > 1$, however, we set $a := b^m c/(1 + b^m)$.

(2) For every $\varepsilon > 0$ there exists an element $b \in F$ satisfying $v_1(1-b) < \varepsilon$, $v_i(b) < \varepsilon$ $(2 \leq i \leq n)$.

We chosse $a \in F$ with the properties of (i) and put $b := a^m/(1+a^m)$ for sufficiently large $m \in \mathbb{N}$. Clearly, $v_i(b)$ tends to 0 for $m \to \infty$, and because of

$$1 - b \;=\; \frac{1}{1+a^m} \;=\; \frac{1}{a^m}\;\frac{1}{1+a^{-m}}$$

the same holds for $v_1(1-b)$.

(3) Now we prove the theorem.

Let $x_1, ..., x_n \in F$ be given. We put $M := \max\{v_j(x_i) \mid 1 \leq i, j \leq n\}$. According to step (ii) there exist elements $b_1, ..., b_n \in F$ with the properties

$$v_i(1-b_i) < \frac{\varepsilon}{Mn}\ ,\ v_j(b_i) < \frac{\varepsilon}{Mn}\ \ (1 \leq i, j \leq n\,,\, i \neq j)\ .$$

The element $x := x_1b_1 + ... + x_nb_n$ then does what we want:

$$\begin{aligned} v_i(x - x_i) &= v_i\left(\sum_{j=1}^{n} x_jb_j \;-\; x_i\right) \\ &\leq v_i(x_ib_i - x_i) + \sum_{\substack{j=1 \\ j\neq i}}^{n} v_i(x_jb_j) \\ &\leq v_i(x)\frac{\varepsilon}{Mn} + (n-1)M\frac{\varepsilon}{Mn} \;\leq\; \varepsilon\ \ (1 \leq i \leq n)\ . \end{aligned}$$

□

Theorem 1.18. *(***Strong Approximation Theorem***)*
Let $v_1, ..., v_n$ be pairwise inequivalent non-archimedian real valuations of the global field F and let $x_1, ..., x_n \in F$. Then for every $\varepsilon > 0$ there exists an element $x \in F$ satisfying $v_i(x - x_i) < \varepsilon$ $(1 \leq i \leq n)$ and $v(x) \leq 1$ for all non-archimedian valuations of F not belonging to $\{v_1, ..., v_n\}$ but for which the ring of integers R of F is contained in the valuation ring R_v.

Proof Let us assume that $\pi_1, ..., \pi_s$ are all prime elements of the base field F_0 which are contained in one of the prime ideals $\mathfrak{p}_i$ $(1 \leq i \leq n)$ of R belonging to the valuations v_i. We enlarge the set $\{\mathfrak{p}_1, ..., \mathfrak{p}_n\}$ to $\mathcal{M} = \{\mathfrak{p}_1, ..., \mathfrak{p}_w\}$ with $w \geq n$ such that $\mathcal{M}$ contains all prime ideals of R containing one of the prime elements $\pi_1, ..., \pi_n$. We put $x_i = 1$ for $i = n+1, ..., w$. According to the preceding theorem there is an element $y \in F$ satisfying $v_i(x - x_i) < \varepsilon$ $(1 \leq i \leq w)$. Let $y = y_1/y_2$

with $y_1, y_2 \in R$ and assume that

$$y_2 R = \left(\prod_{i=1}^{w} \mathfrak{p}_i^{m_i} \right) \mathfrak{a}$$

is the prime ideal decomposition of $y_2 R$, i.e. $\mathfrak{a}$ is not contained in any of the $\mathfrak{p}_i$. We choose $\delta, \kappa \in \mathbb{N}$ such that

(1) $v_i(x) < \varepsilon$ is satisfied for $x \in F$ if we have $x \in \mathfrak{p}_i^{\delta}$ for $1 \leq i \leq w$,
(2) $y\mathfrak{p}_i^{\kappa} \subseteq \mathfrak{p}_i^{\delta}$ $(1 \leq i \leq w)$,

and put

$$\mathfrak{b} := \left(\prod_{i=1}^{w} \mathfrak{p}_i \right)^{\max(\delta,\kappa)} .$$

By the Euclidean algorithm in R_0 we compute elements $k, l \in R_0$ satisfying $kN(\mathfrak{a}) + lN(\mathfrak{b}) = 1$. (We recall that $N(\mathfrak{a}) = (R : \mathfrak{a})$ is contained in $\mathfrak{a}$, hence $N(\mathfrak{a}R)$ is the product of $\mathfrak{a}$ and another ideal of R.) We claim that $x := kN(\mathfrak{a})y$ has the properties stated in the theorem. Because of the choice of $\mathfrak{a}$ we have $v(x) \leq 1$ for all valuations which are not equivalent to a v_i $(1 \leq i \leq w)$. Because of $x = (1 - lN(\mathfrak{b}))y$ we get $x - x_i = y - x_i - lN(\mathfrak{b})y$ and therefore $v_i(x - x_i) \leq \max\{v_i(y - x_i)\,,\, v_i(lN(\mathfrak{b})y)\} \leq \varepsilon$ for $1 \leq i \leq w$.

□