# AN INTRODUCTION TO VALUED FIELDS

FRANZISKA JAHNKE

These lecture notes are a (slightly) extended version of my lecture course 'Valued Fields' as given during the first week of the Münster Month in Model Theory. They are heavily based on the book Valued Fields by Engler and Prestel, as well as (unpublished) lectures given by Jochen Koenigsmann at the University of Oxford in Hilary 2010. Many of the proofs presented are taken from (or at least inspired by) one of these two sources.

My eternal gratitude goes to Peter Sinclair who did the bulk of the typing of these notes!

## 1. Definitions and Basic Properties

Intuitively, a valuation measures the size of the elements of a field. Before we can formally define a valuation, we need to introduce ordered abelian groups. These will serve as the range of our valuation maps, i.e., their elements are the possible 'sizes'.

**Definition 1.1.** *An ordered abelian group is an abelian group* $(\Gamma, +)$ *with a relation* $<$ *on* $\Gamma$ *satisfing* $\forall \gamma, \delta, \lambda \in \Gamma$*:*

(O1) $\neg(\gamma < \gamma)$ *(*$<$ *is irreflexive)*
(O2) $\gamma < \delta \implies \neg(\delta < \gamma)$ *(*$<$ *is antisymmetric)*
(O3) $\gamma < \delta \wedge \delta < \lambda \implies \gamma < \lambda$ *(*$<$ *is transitive)*
(O4) $\gamma < \delta \vee \delta < \gamma \vee \delta = \gamma$ *(*$<$ *is total)*
(O5) $\gamma < \delta \implies \gamma + \lambda < \delta + \lambda$ *(compatibility of* $<$ *and* $+$*)*

The last condition implies in particular that any ordered abelian group which contains at least two elements is torsion free: if $\gamma > 0$ then

$$0 < \gamma < \gamma + \gamma < \gamma + \gamma + \gamma < \dots$$

so $\gamma$ is not a torsion element. The proof for $\gamma < 0$ is symmetric. In particular, any ordered abelian group is either trivial or infinite.

We start by giving some basic examples of ordered abelian groups.

**Examples 1.2.**

*(1)* $(\mathbb{R}, +, <)$ *is an ordered abelian group. Moreover, any subgroup* $(\Gamma, +)$ *of* $(\mathbb{R}, +)$ *with the induced ordering is again an ordered abelian group, e.g.,* $(\mathbb{Q}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Z} + \sqrt{2}\mathbb{Z}, +)$, $(\{0\}, +)$, *etc.*

*(2) If* $\Gamma_1, \Gamma_2$ *are ordered abelian groups, then the* lexicographic direct product $(\Gamma_1 \oplus \Gamma_2, +, <)$ *is also an ordered abelian group, with the ordering defined by*

$$(\gamma_1, \gamma_2) < (\delta_1, \delta_2) \iff \gamma_1 < \delta_1 \text{ or } \gamma_1 = \delta_1 \wedge \gamma_2 < \delta_2.$$

Note that an ordered abelian group might not carry a *unique* ordering, as the following exercise shows.

**Exercise 1.3.** *Show that there are two non-isomorphic expansions of* $(\mathbb{Z} \times \mathbb{Z}, +)$ *to an ordered group.*
Hint: $(\mathbb{Z} \oplus \mathbb{Z}, +)$ *with the lexicographic ordering is not isomorphic to* $(\mathbb{Z} + \sqrt{2}\mathbb{Z}, +)$ *as a subgroup of* $(\mathbb{R}, +)$*, even though we have* $\mathbb{Z} \oplus \mathbb{Z} \cong \mathbb{Z} + \sqrt{2}\mathbb{Z}$ *as groups. One way to show this is that* $\mathbb{Z} + \sqrt{2}\mathbb{Z}$ *does not have a minimal positive element; another one is to show that* $\mathbb{Z} + \sqrt{2}\mathbb{Z}$ *does not have a convex subgroup.*

**Definition 1.4.** *A* valuation *on a field* $K$ *is a surjective map* $v : K \to vK \cup \{\infty\}$*, where* $vK$ *is some ordered abelian group (called the* value group*) satisfying* $\forall\, x, y \in K$*:*

(V1) $v(x) = \infty$ *if and only if* $x = 0$
(V2) $v(xy) = v(x) + v(y)$
(V3) $v(x + y) \geq \min\{v(x), v(y)\}$

Note that in the above definition, we extend $+$ to $vK \cup \{\infty\}$ by setting $\gamma + \infty = \infty$ for all $\gamma \in vK \cup \{\infty\}$. We moreover extend the ordering to $vK \cup \{\infty\}$ by setting $\gamma < \infty$ for all $\gamma \in vK$.

**Examples 1.5.**

*(1) Let* $K$ *be any field. The map* $v : K \to \{0, \infty\}$ *with* $v(0) = \infty$ *and* $v(x) = 0$ *for all* $x \neq 0$ *is a valuation. It is called the* trivial valuation.
*(2) If* $K = \mathbb{Q}$ *and* $p$ *is a prime, we can write any* $x \in \mathbb{Q}^\times$ *in a unique way as* $p^\nu \frac{c}{d}$ *with* $c, d \in \mathbb{Z}$ *and* $\gcd(c, d) = 1$ *such that* $p \nmid c, d$ *holds. Setting* $v_p(x) = \nu$ *gives a valuation on* $\mathbb{Q}$ *with value group* $\mathbb{Z}$*; this is called the* $p$-adic valuation.
*(3) If* $K = k(t)$ *for some field* $k$ *and* $p \in k[t]$ *is irreducible, we can do the same: write* $f \in K$ *as* $p^\nu \frac{g}{h}$ *for* $g, h \in k(t)$ *with* $\gcd(g, h) = \gcd(p, g) = \gcd(p, h) = 1$ *and set* $v_p(f) = \nu$*. This is again called* $p$-adic valuation*, the value group is again* $\mathbb{Z}$*.*
*(4) If* $K = k(t)$*, we also get another valuation with value group* $\mathbb{Z}$*, namely the* degree valuation $v_\infty$*. Here, for* $f, g \in k(t) \setminus \{0\}$*, we set* $v_\infty(f/g) = \deg(g) - \deg(f)$*.*

*Note that for any* $p$*-adic valuation* $v_p$ *and as well as for* $v_\infty$ *on* $k(t)$*, we have* $v(x) = 0$ *for all* $x \in k$*.*

We now note some first properties.

**Basic Properties 1.6.** *Let* $(K, v)$ *be a valued field. Then, we have* $\forall x, y \in K$*:*

*(1)* $v(1) = 0$
*(2)* $v(x^{-1}) = -v(x)$
*(3)* $v(-x) = v(x)$
*(4)* $v(x) < v(y) \implies v(x + y) = v(x)$

*Proof.* The first three equations follow immediately from the definition. For last implication, consider $x, y \in K$ with $v(x) < v(y)$. Suppose for a contradiction that $v(x + y) > v(x)$ holds. Then, we have

$$v(x) = v(x + y - y) \geq \min\{v(x + y), v(y)\} > v(x)$$

which gives the desired contradiction. □

**Definition and Remark 1.7.** *The set* $\mathcal{O}_v = \{x \in K : v(x) \geq 0\}$ *is a* valuation ring *of* $K$*, meaning* $\mathcal{O}_v$ *is a subring of* $K$ *such that for all* $x \in K$*, we have either*

*$x \in \mathcal{O}_v$ or $x^{-1} \in \mathcal{O}_v$. Its group of units is $\mathcal{O}_v^\times = \{x \in K : v(x) = 0\}$. The remaining elements, $\mathfrak{m}_v := \{x \in K : v(x) > 0\}$, form the unique maximal ideal of $\mathcal{O}_v$ (in particular, $\mathcal{O}_v$ is a local ring). The quotient field $Kv = \mathcal{O}_v/\mathfrak{m}_v$ is called the* residue field *of $(K, v)$. For $a \in \mathcal{O}_v$, we write $\overline{a}$ for the corresponding element in $Kv$; the map $a \mapsto \overline{a}$ is called the* residue map.

It is easy to check that if $\mathrm{char}(K) = p > 0$ then $\mathrm{char}(Kv) = p$, and in case that $\mathrm{char}(K) = 0$ then we have $\mathrm{char}(Kv)$ is either 0 or $p$ for any prime $p$. We often write the characteristic of $K$ and $Kv$ as a pair, so $(\mathrm{char}(K), \mathrm{char}(Kv)) \in \{(0,0), (0,p), (p,p)\}$. In case $\mathrm{char}(K) = \mathrm{char}(Kv)$, we say that $(K, v)$ has equicharacteristic 0 or $p$ as appropriate. Otherwise, we say that $(K, v)$ has mixed characteristic.

We now return to the previous examples to work out their valuation rings, maximal ideals and residue fields.

**Examples 1.8.**

*(1) If $K$ is equipped with the trivial valuation $v$, we have $K = \mathcal{O}_v$ and hence $\mathfrak{m}_v = \{0\}$. In particular, we get $K = Kv$ and so* $\mathrm{char}(K) = \mathrm{char}(Kv)$.

*(2) The valued field $(\mathbb{Q}, v_p)$ has valuation ring*

$$\mathcal{O}_v = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, p \nmid b, \gcd(a,b) = 1 \right\} = \mathbb{Z}_{(p)},$$

*which is the localization of $\mathbb{Z}$ at the ideal generated by $p$. Its maximal ideal is*

$$\mathfrak{m}_v = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, p \mid a, \gcd(a,b) = 1 \right\} = p\mathbb{Z}_{(p)}.$$

*It follows immediately that the residue field*

$$Kv = \mathcal{O}/\mathfrak{m} = \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$$

*is the field containing $p$ elements, and so $(K, v)$ has mixed characteristic $(0, p)$.*

*(3) In analogy to the $p$-adic valuations on $\mathbb{Q}$: for $p \in k[t]$ irreducible, the $p$-adic valued field $(k(t), v_p)$ has valuation ring $k[t]_{(p)}$, maximal ideal $p \cdot k[t]_{(p)}$, and residue field $k[t]/p \cdot k[t]$, the latter being precisely the splitting field of $p$ over $k$.*

*(4) $(k(t), v_\infty)$ has residue field $k$.*

There are three different ways to think about valuations. One can either define valuations via the valuation map (as we have done), via valuation rings or via the residue map (often called a place). As we explain below, the last of these is the reason for the name 'valuation'. We now introduce places and show that the three notions all encode basically the same information.

**Definition 1.9.** *A* place *on a field $K$ is map $\phi : K \to k \cup \{\infty\}$ which maps surjectively onto some field $k$ satisfying $\forall x, y \in K$:*

*(P1)* $\phi(x + y) = \phi(x) + \phi(y)$

*(P2)* $\phi(1) = 1$

*(P3)* $\phi(xy) = \phi(x) \cdot \phi(y)$ *whenever $\phi(x) \cdot \phi(y)$ is defined.*

*Here, we extend $+$ to $k \cup \{\infty\}$ by setting $x + \infty = \infty + x = \infty + \infty = \infty$ for any $x \in k$. We extend $\cdot$ to $k^\times \cup \{\infty\}$ by setting $x \cdot \infty = \infty \cdot x = \infty \cdot \infty = \infty$ for $x \in K^\times$; both $0 \cdot \infty$ and $\infty \cdot 0$ are left undefined.*

It is clear that every valuation ring gives rise to a place and vice versa:

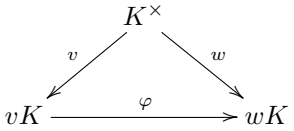
**Remark 1.10.** *Every valuation ring $\mathcal{O} \subseteq K$ determines a place mapping $a \in \mathcal{O}$ to $\overline{a} \in Kv$ and $a \in K \setminus \mathcal{O}$ to $\infty$. Conversely, given a place $\phi : K \to\!\!\!\!\to k \cup \{\infty\}$, $\phi^{-1}(k)$ is a valuation ring of $K$ with maximal ideal $\mathfrak{m} = \phi^{-1}(\{0\})$ and residue field $k$. These correspondences are inverse to one another.*

**Examples 1.11.**

(1) *Let $K$ be any field and $v$ the trival valuation. The associated place is the identity map $\phi : K \to K$.*
(2) *If $K = k(t)$ and $a \in k$, consider the $p$-adic valuation $v = v_p$ where $p$ is the irreducible polyonimal $p(t) = t - a$. Then $Kv = k$ and the associated place $\phi : \mathcal{O}_{v_p} \to k$ is the map $f/g \mapsto f(a)/g(a)$, namely the* evaluation map *at $a$.*

Before we can explain how valuation rings enter the picture, we need one further definition.

**Definition 1.12.** *Two valuations $v : K \to vK \cup \{\infty\}$ and $w : K \to wK \cup \{\infty\}$ are called* equivalent *if there is an isomorphism of ordered abelian groups $\varphi : vK \to wK$ such that the following diagram commutes:*




*In this case we write $v \sim w$.*

**Observation 1.13.** *The notions 'valuation', 'valuation ring' and 'place' coincide, in the following sense:*

$$\{v \text{ valuation on } K\}/\sim \overset{1:1}{\longleftrightarrow} \{\mathcal{O} \text{ valuation ring on } K\} \overset{1:1}{\longleftrightarrow} \{\text{places on } K\}$$

*In particular, a valuation ring $\mathcal{O} \subseteq K$ defines a valuation on $K$ which is unique up to isomorphism of valued fields.*

*Proof.* If two valuations are equivalent then they clearly have the same valuation ring. If $\mathcal{O}$ is a valuation ring on $K$, then $\Gamma := K^\times/\mathcal{O}^\times$ is an abelian group, and is in fact an ordered abelian group with the ordering defined by $x\mathcal{O}^\times \leq y\mathcal{O}^\times$ iff $yx^{-1} \in \mathcal{O}$. Now $v : K \to \Gamma \cup \{\infty\}$ with $v(0) = \infty$ and $v(x) = x\mathcal{O}^\times$ for $x \in K^\times$ is a valuation. If a valuation $w$ induces $\mathcal{O}$, then $w$ is equivalent to $v$ as constructed above since $\mathcal{O}^\times$ is exactly the kernel of the surjection $w : K^\times \to wK$. The previous remark gave the correspondence between places and valuation rings. □

From this point on, we consider valuations only up to equivalence. To get used to working with valuations, we now prove some simple facts about valuation rings.

**Proposition 1.14.** *If $\mathcal{O} \subseteq K$ is a valuation ring then $\mathcal{O}$ is integrally closed in $K$.*

*Proof.* Suppose $x \in K$ satisfies $x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$ for some $a_i \in \mathcal{O}$. We want to show that $x \in \mathcal{O}$. In case $K = \mathcal{O}$, the statement is clear. Otherwise, we have $\mathfrak{m} \supsetneq \{0\}$. If $x \notin \mathcal{O}$ then $x^{-1} \in \mathfrak{m}$, so (multiplying the original equation by $x^{-n}$), we get

$$\underbrace{a_{n-1}x^{-1} + \ldots + a_0x^{-n}}_{\in \mathfrak{m}} = -1$$

and so $-1 \in \mathfrak{m}$, which is impossible. Thus, $x \in \mathcal{O}$. □

**Proposition 1.15.** *Every non-trivial valuation ring $\mathcal{O}$ of $\mathbb{Q}$ is of the form $\mathcal{O} = \mathcal{O}_{v_p} = \mathbb{Z}_{(p)}$ for some prime $p \in \mathbb{Z}$.*

*Proof.* For a non-trivial valuation, we always have $\mathbb{Z} \subseteq \mathcal{O} \subsetneq \mathbb{Q}$. If $\mathbb{Z} \subseteq \mathcal{O}^\times$ then it follows immediately that we have $\mathcal{O} = \mathbb{Q}$. Assume $\mathbb{Z} \nsubseteq \mathcal{O}^\times$ and take $p \in \mathbb{Z}$ minimal such that we have $p > 0$ and $p \notin \mathcal{O}^\times$. By splitting $p$ into its prime factorization, it is easy to see that one of the prime factors of $p$ must have positive valuation; by minimality of $p$, we must have $p$ equal to this prime factor. For any prime $q \neq p$, there are $a, b \in \mathbb{Z}$ with $1 = ap + bq$ by the Euclidean algorithm. Since $v(1) = 0$ and $v(ap) \geq v(p) > 0$, we must have $v(bq) = 0$, and so $v(b) = v(q) = 0$ (since $b, q \in \mathbb{Z} \subseteq \mathcal{O}$). Thus $q \in \mathcal{O}^\times$ for all $q \neq p$, which means the only non-invertible elements in $\mathcal{O}$ are multiples of $p$, and hence $\mathcal{O} = \mathbb{Z}_{(p)}$. □

A similar argument shows that every non-trivial valuation on $k(t)$ that is trivial on $k$ is equal to $v_\infty$ or $v_p$ for some irreducible $p \in k[t]$.

**Proposition 1.16.** *Let $K$ be an algebraic extension of a finite field. Then $K$ admits only the trivial valuation.*

*Proof.* If $K$ is an algebraic extension of a finite field, $v$ a valuation on $K$, then for all $x \in K^\times$ there exists $n \in \mathbb{N}$ such that $x^n = 1$, which implies $v(x^n) = nv(x) = 0$. Thus, we conclude $v(x) = 0$ since $vK$ is torsion-free. □

We would like to show that algebraic extensions of finite fields are the only fields with no interesting valuations. To do this, note that every field $K$ which is not an algebraic extension of a finite field embeds either $\mathbb{Q}$ or $k(t)$ with $k = \mathbb{F}_p$ for some prime $p$. As $\mathbb{Q}$ and $\mathbb{F}_p(t)$ both admit non-trivial valuations, we now want to extend these to non-trivial valuations on $K$. Thus, we need to study extensions of valuations.

## 2. Extensions of Valuations

We now want to show that any (non-trivial) valuation on a subfield $K \subseteq F$ can be extended to a non-trivial valuation on $F$. This is a consequence of the next theorem.

**Theorem 2.1** (Chevalley Extension Theorem)**.** *Let $F$ be a field, $R \subseteq F$ a subring, $\mathfrak{p} \subseteq R$ a prime ideal. Then there is a valuation ring $\mathcal{O}$ of $F$ with $R \subseteq \mathcal{O}$ and $\mathfrak{m}_v \cap R = \mathfrak{p}$.*

*Proof.* Consider the localization

$$R_\mathfrak{p} := \left\{ \frac{a}{b} : a \in R, b \in R \setminus \mathfrak{p} \right\} / \sim$$

of $R$ at $\mathfrak{p}$ where

$$\frac{a}{b} \sim \frac{c}{d} :\iff ad = bc.$$

This is a local ring with unique maximal ideal $\mathfrak{p}R_\mathfrak{p}$. Consider the set

$$\Sigma := \{(A, I) : A \subseteq F \text{ subring }, I \lneq A \text{ proper ideal}, R_\mathfrak{p} \subseteq A, \mathfrak{p}R_\mathfrak{p} \subseteq I\}.$$

Then $\Sigma$ is nonempty since it contains $(R_\mathfrak{p}, \mathfrak{p})$ and can be given a partial order via

$$(A, I) \leq (A', I') \iff A \subseteq A' \text{ and } I \subseteq I'.$$

Note that $\Sigma$ is obviously closed under chains. By Zorn's lemma, there exists a maximal element $(\mathcal{O}, \mathfrak{m}) \in \Sigma$. By maximality, $\mathfrak{m}$ is a maximal ideal of $\mathcal{O}$. Moreover,

$\mathfrak{m}$ is the unique maximal ideal of $\mathcal{O}$ as otherwise the localization $\mathcal{O}_\mathfrak{m}$ of $\mathcal{O}$ at $\mathfrak{m}$ together with the ideal $\mathfrak{m}\mathcal{O}_\mathfrak{m}$ would be an element of $\Sigma$ strictly bigger in the partial order that $(\mathcal{O}, \mathfrak{m})$. Hence, $(\mathcal{O}, \mathfrak{m})$ is a local ring. In particular, we have $\mathcal{O}^\times = \mathcal{O} \setminus \mathfrak{m}$.

**Claim:** $\mathcal{O}$ is a valuation ring of $F$.

*Proof of claim:* Assume not, then there is some $x \in F^\times$ with $x, x^{-1} \notin \mathcal{O}$. In particular, we get that $\mathcal{O}$ is properly contained in $\mathcal{O}[x]$ and $\mathcal{O}[x^{-1}]$. Since $(\mathcal{O}, \mathfrak{m})$ is maximal, the ideal $\mathfrak{m}\mathcal{O}[x]$ generated by $\mathfrak{m}$ in $\mathcal{O}[x]$ must be all of $\mathcal{O}[x]$, symmetrically $\mathfrak{m}\mathcal{O}[x^{-1}] = \mathcal{O}[x^{-1}]$. Thus, there exist elements $a_0, \dots, a_n, b_0, \dots, b_m \in \mathfrak{m}$ with

$$(\star) \qquad 1 = \sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{m} b_i x^{-i}.$$

We may assume that both $n$ and $m$ are minimal such that $(\star)$ is satisfied. Suppose that we have $m \leq n$. As $b_0 \in \mathfrak{m}$, we get

$$\sum_{i=1}^{m} b_i x^{-i} = 1 - b_0 \in \mathcal{O} \setminus \mathfrak{m} = \mathcal{O}^\times.$$

Thus, for $c_i := \frac{b_i}{1-b_0} \in \mathfrak{m}$, we have

$$1 = \sum_{i=1}^{m} c_i x^{-i}$$

and thus

$$x^n = \sum_{i=1}^{m} c_i x^{n-i}.$$

Plugging this into the equation $(\star)$ above, we get

$$1 = \sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{n-1} a_i x^i + a_n \sum_{i=1}^{m} c_i x^{n-i},$$

contradicting the minimality of $n$. The case $n \leq m$ works analogously by swapping $x$ and $x^{-1}$. This proves the claim.

By construction, we have $\mathfrak{p} \subseteq \mathfrak{m} \cap R$. What is left to show is that equality holds. However, we have

$$R \setminus \mathfrak{p} \subseteq (R_\mathfrak{p})^\times \subseteq \mathcal{O}^\times = \mathcal{O} \setminus \mathfrak{m}.$$

This implies $\mathfrak{p} \supseteq \mathfrak{m} \cap R$ and thus finishes the proof. □

**Definition 2.2.** *Let $(F, w)$ and $(K, v)$ be valued fields. We say that $(F, w)$ is an* extension *of $(K, v)$ if $K \subseteq F$ and $w|_K = v$ holds. In this case, we write $(K, v) \subseteq (F, w)$ and say that $w$ is a* prolongation *of $v$.*

Note that $(F, w)$ being an extension of $(K, v)$ is equivalent to $\mathcal{O}_v = \mathcal{O}_w \cap K$. Moreover, $vK$ is a subgroup of $wF$ and we have $\mathfrak{m}_v = \mathfrak{m}_w \cap K$. In particular, there is an induced embedding of $Kv$ into $Fw$.

**Corollary 2.3.** *Let $(K, v)$ be a valued field and $F$ a field extension of $K$. Then there is a prolongation $w$ of $v$ to $F$. Moreover, if $v$ is non-trivial then $w$ is non-trivial.*

*Proof.* Use Theorem 2.1 with $R = \mathcal{O}_v$ and $\mathfrak{p} = \mathfrak{m}_v$ to find $w$. If $v$ is non-trivial then we have $\{0\} \subsetneq vK \subseteq wF$, so $w$ is also non-trivial. □

As promised, we can now show the converse to Proposition 1.16:

**Corollary 2.4.** *If $K$ is any field which is not an algebraic extension of a finite field, then $K$ admits a non-trivial valuation.*

*Proof.* If $\mathrm{char}(K) = 0$ then $K$ is an extension of $\mathbb{Q}$, and if $\mathrm{char}(K) = p$ then $K$ is an extension of $\mathbb{F}_p(t)$. In either case, any non-trivial valuation (which exists by Examples 1.5) of the smaller field can be extended to $K$. □

**Example 2.5.** *Let $(K, v)$ be a valued field with value group $vK$ and $\Gamma$ an ordered abelian group with $\Gamma \geq vK$. Consider some $t$ which is transcendental over $K$ and any $\gamma \in \Gamma$. Define a valuation $w$ on $K(t)$ with values in $\Gamma$ via*

$$w(\sum_{i=0}^{n} a_i t^i) = min\{v(a_i) + i\gamma \,:\, 0 \leq i \leq n\}$$

*for $f = \sum_{i=0}^{n} a_i t^i \in K[t]$ and extend $w$ to all of $K(t)$ by setting*

$$w\left(\frac{f}{g}\right) = w(f) - w(g)$$

*for $f, g \in K[t] \setminus \{0\}$. Then $w$ is a well-defined valuation extending $v$ with value group $wK(t) = vK + \mathbb{Z} \cdot \gamma$. We now look at two special cases of this construction in more detail.*

1. *Consider the case $vK = \Gamma$ and $\gamma = 0$. Then $w$ is called the* Gauss extension *of $v$. In this case, $w$ is the unique extension of $v$ to $K(t)$ such that $w(t) = 0$ and the residue $\bar{t}$ of $t$ is transcendental over $Kv$ with residue field $K(t)w = Kv(\bar{t})$ (Exercise!).*
2. *In case $\gamma \notin vK$ and $vK \cap \mathbb{Z} \cdot \gamma = \{0\}$, we have $wK(t) = vK \oplus \mathbb{Z} \cdot \gamma$ and $K(t)w = Kv$.*

We have already noted above that if $(F, w)$ is an extension of $(K, v)$, we get induced embeddings of $vK$ into $wF$ and of $Kv$ into $Fw$. We now want to show that the index (respectively degree) of these can be linked to the degree of the field extension.

**Definition 2.6.** *Assume $(K, v) \subseteq (F, w)$ is an extension of valued fields. Then,*

$$e := e(w/v) := [wF : vK]$$

*is called the* ramification index *of $(K, v)$ in $(F, w)$. Furthermore,*

$$f := f(w/v) := [Fw : Kv]$$

*is called the* inertia degree *of the extension.*

We follow the usual convention that both $e$ and $f$ can be either finite or infinite, without distinguishing between different infinite cardinalities. Before we prove anything about these quantities, we start with some explicit examples.

**Examples 2.7.** *Let $p$ be a prime and consider the $p$-adic valuation $v_p$ on $\mathbb{Q}$.*

1. *We can extend $v_p$ to the Gauss extension $w$ on $\mathbb{Q}(t)$ by setting*

$$w(\sum_{i=0}^{n} a_i t^i) = min\{v(a_i)\},$$

*for* $\sum_{i=0}^{n} a_i t^i \in \mathbb{Q}[t]$, *e.g.*

$$w\left(\frac{1}{p}t - t^2 + p\right) = -1.$$

*In this case, we have* $e(w/v_p) = 1$ *and* $f(w/v_p) = \infty$.

(2) *Consider* $\sqrt{2} \in \mathbb{Q}^{alg}$. *We want to extend* $v_p$ *to* $\mathbb{Q}(\sqrt{2})$ *for different primes* $p$.
   (a) *If* $p = 2$, *we get* $w(\sqrt{2}) = \frac{1}{2}v_2(2) = \frac{1}{2}$ *and* $\overline{\alpha} = 0$ *for any extension* $w$ *of* $v_2$ *to* $\mathbb{Q}(\sqrt{2})$. *Thus, we have* $e(w/v_2) = 2$ *and* $f(w/v_2) = 1$.
   (b) *If* $p = 3$, *we get* $w(\sqrt{2}) = \frac{1}{2}v_3(2) = 0$ *and* $\overline{\alpha} = \sqrt{2}$ *over* $\mathbb{F}_3$ *for any extension* $w$ *of* $v_3$ *to* $\mathbb{Q}(\sqrt{2})$. *Thus, we conclude for the residue field* $\mathbb{Q}(\sqrt{2})w = \mathbb{F}_3(i)$ *and so we have* $e(w/v_3) = 1$ *and* $f(w/v_3) = 2$.
   (c) *If* $p = 7$, *we have again* $w(\sqrt{2}) = \frac{1}{2}v_7(2) = 0$ *and* $\overline{\alpha} = \sqrt{2}$ *over* $\mathbb{F}_7$ *for any extension* $w$ *of* $v_7$ *to* $\mathbb{Q}(\sqrt{2})$. *As both* 3 *and* 4 *are square roots of* 2 *in* $\mathbb{F}_7$, *there are two possible prolongations of* $v_7$ *to* $\mathbb{Q}(\sqrt{2})$, *in either case we have* $e(w/v_7) = f(w/v_7) = 1$.

We now show that the degree of a field extension bounds both the inertia degree and the ramification index.

**Theorem 2.8** (Fundamental Inequality, version 1)**.** *Suppose* $(K, v) \subseteq (F, w)$ *is an extension of valued fields. Then* $ef \leq [F : K]$.

*Proof.* Choose $\{\gamma_i : i \in I\} \subseteq wF$ representatives of different cosets of $wF/vK$ and $\{\alpha_j : j \in J\} \in Fw$ such that $\{\alpha_j\}$ are linearly independent over $Kv$ for $e = |I|$, $f = |J|$ finite. Take $\{g_i\}_{i\in I} \subseteq F$ with $w(g_i) = \gamma_i$ for all $i \in I$ and $\{a_j\}_{j\in J} \subseteq \mathcal{O}_w^\times$ with $\overline{a}_j = \alpha_j$ for all $j \in J$.

**Claim:** The products $\{a_j g_i : i \in I, j \in J\}$ are linearly independent over $K$.

*Proof of claim:* Take $r_{ij} \in K$ not all zero. We will show that the element

$$\sum r_{ij} a_j g_i =: z$$

has valuation

$$w(z) = \min_{i,j}\{w(r_{ij}a_j g_i)\} =: \delta,$$

and hence is not zero. Choose $i_0$ and $j_0$ so that we have $w(r_{i_0 j_0} g_{i_0}) = \delta$ and note that we can drop the $a_j$ factor since we have $w(a_j) = 0$ for all $j \in J$.

Suppose there is $i \neq i_0$ and $j \in J$ (maybe $j = j_0$) so that we have $w(r_{ij}g_i) = w(r_{i_0 j_0} g_{i_0})$. Rearranging, and using the fact that $w(g_i) = \gamma_i$, we get

$$-\gamma_{i_0} + \gamma_i = -w(g_{i_0}) + w(g_i) = w(r_{i_0 j_0}) - w(r_{ij}) \in vK$$

contradicting the fact that $\gamma_{i_0}$ and $\gamma_i$ are in different cosets of $vK$. Thus, if $w(r_{ij}g_i) = w(r_{i_0 j_0} g_{i_0})$ holds, we must have $i = i_0$.

Now, suppose for a contradiction that $w(z) > \delta$ holds and write $y := r_{i_0 j_0} g_{i_0}$. Then, by our assumption, we have $zy^{-1} \in \mathfrak{m}_w$. By the previous argument, this implies $r_{ij} g_i y^{-1} \in \mathfrak{m}_w$ for all $i \neq i_0$. Consider

$$\sum_{j\in J} r_{i_0 j} g_{i_0} a_j = z - \sum_{i\neq i_0, j\in J} r_{ij} g_i a_j.$$

Multiplying this equation with $y^{-1}$, we get

$$\sum_{j\in J} r_{i_0 j} g_{i_0} a_j (r_{i_0 j_0} g_{i_0})^{-1} = \underbrace{zy^{-1}}_{\in \mathfrak{m}_w} - \sum_{i\neq i_0, j\in J} \underbrace{r_{ij} g_i a_j y^{-1}}_{\in \mathfrak{m}_w} \in \mathfrak{m}_w.$$

This implies for the residue of the left hand side that

$$\sum_{j\in J} \overline{r_{i_0 j}} (\overline{r_{i_0 j_0}})^{-1} \overline{a_j} = \overline{0} \in Kv$$

holds. But this contradicts the linear independence of the $\overline{a_j} = \alpha_j$, and hence we must have $w(z) = \delta$.

From the claim, we are done: we conclude

$$ef = |\{a_j g_i : j \in J,\, i \in I\}| \leq [F : K].$$

□

**Corollary 2.9.** *Assume $(K, v) \subseteq (F, w)$ is algebraic. Then*

*(1) $wF/vK$ is a torsion group and*
*(2) $Fw$ is an algebraic extension of $Kv$.*

*Proof.* Ad (1): Assume $(K, v) \subseteq (F, w)$ algebraic. Take any $\gamma \in wF$ and choose some $g \in F$ with $w(g) = \gamma$. Consider $K \subseteq K(g) = L \subseteq F$ and $u = w|_L$. By the Fundamental Inequality (Theorem 2.8), $[vL : vK]$ is finite, so there is some $n \in \mathbb{N}$ with $n\gamma \in vK$. Part (2) is proved similarly. □

Our next aim is to prove the Conjugation Theorem, that is that if $L/K$ is a normal extension and $v$ is a valuation of $K$, then any two prolongations of $v$ to $L$ are conjugate by a $K$-automorphism of $L$.

**Proposition 2.10.**

*(1) Suppose $L/K$ is an algebraic extension, $v$ a valuation on $K$, and let $w_1$ and $w_2$ be prolongations of $v$ to $L$. If $\mathcal{O}_{w_1} \subseteq \mathcal{O}_{w_2}$ holds, then we have $\mathcal{O}_{w_1} = \mathcal{O}_{w_2}$.*
*(2) Assume $L/K$ is purely inseparable, i.e., $\mathrm{char}(K) = p > 0$ and every $x \in L$ satisfies $x^{p^n} \in K$ for some $n \in \mathbb{N}$. Then every valuation on $K$ extends uniquely to $L$.*

*Proof.* (1) Let $(K, v)$ be a valued field, $F$ an algebraic extension of $K$, $w_1$, $w_2$ prolongations of $v$ to $F$ with $\mathcal{O}_{w_1} \subseteq \mathcal{O}_{w_2}$. We remark first that $\mathcal{O}_{w_1} \subseteq \mathcal{O}_{w_2} \subseteq L$ implies $\mathfrak{m}_{w_1} \supseteq \mathfrak{m}_{w_2}$: to see this, note that we have

$$\begin{aligned} x \in \mathfrak{m}_{w_2} &\implies x \in \mathcal{O}_{w_2} \wedge x^{-1} \notin \mathcal{O}_{w_2} \\ &\implies x^{-1} \notin \mathcal{O}_{w_1} \implies x \in \mathfrak{m}_{w_1}. \end{aligned}$$

Consider $\mathcal{O}_{w_1}/\mathfrak{m}_{w_1} \subseteq \mathcal{O}_{w_2}/\mathfrak{m}_{w_2} = Lw_2$. Then (exercise!) $\mathcal{O}_{w_1}/\mathfrak{m}_{w_2}$ is a valuation right of $Lw_2$.

We claim that $\mathcal{O}_{w_1}/\mathfrak{m}_{w_2} = L_{w_2}$ holds. Take $\alpha \in Lw_2$. By Corollary 2.9, $\alpha$ is algebraic over $Kv$. Moreover, $Kv = \mathcal{O}_v/\mathfrak{m}_v$ embeds into $\mathcal{O}_{w_1}/\mathfrak{m}_{w_2}$. Now the minimal polynomial of $\alpha/Kv$ is monic and has coefficients in $Kv \subseteq \mathcal{O}_{w_1}/\mathfrak{m}_{w_2}$, so by Proposition 1.14, we get $\alpha \in \mathcal{O}_{w_1}/\mathfrak{m}_{w_2}$.

This implies $\mathcal{O}_{w_1}/\mathfrak{m}_{w_2} = Lw_2$, and hence $\mathfrak{m}_{w_2}$ is a maximal ideal of $\mathcal{O}_{w_1}$. But valuation rings have unique maximal ideals, which means $\mathfrak{m}_{w_2} = \mathfrak{m}_{w_1}$, and hence $\mathcal{O}_{w_1} = \mathcal{O}_{w_2}$.

(2) Assume $L/K$ is purely inseparable and $v$ is a valuation on $K$. Take $x \in L$ and $n \in \mathbb{N}$ with $x^{p^n} \in K$. Let $w$ be any extension of $v$ to $L$. By Proposition 2.9, $wL/vK$ is torsion, so $wL$ embeds into the divisible hull $D$ of $vK$. $D$ is again an ordered abelian group, and hence in particular torsion-free. Now, we get $p^n w(x) = v(x^{p^n}) \in vK$; since $D$ is torsion-free, this determines $w(x)$ uniquely. □

Our next theorem is a version of the Chinese remainder theorem for valuations. The analogue of coprime integers is given by incomparable valuation rings.

**Definition 2.11.** *Let $\mathcal{O}_1$ and $\mathcal{O}_2$ be valuation rings of a field $K$. We say that $\mathcal{O}_1$ and $\mathcal{O}_2$ are* comparable *if either $\mathcal{O}_1 \subseteq \mathcal{O}_2$ or $\mathcal{O}_2 \subseteq \mathcal{O}_1$ holds.*

**Theorem 2.12.** *(Weak Approximation Theorem) Let $\mathcal{O}_1, \ldots, \mathcal{O}_n$ be incomparable valuation rings of $K$ and consider any elements $x_i \in \mathcal{O}_i$ for $1 \leq i \leq n$. Then there exists some $x \in K$ with $x - x_i \in \mathfrak{m}_i$ for all $1 \leq i \leq n$.*

*Proof.* Define $R := \bigcap_{i=1}^n \mathcal{O}_i$ and $\mathfrak{p}_i := R \cap \mathfrak{m}_i$ for $1 \leq i \leq n$; observe that each $\mathfrak{p}_i$ is a prime ideal of $R$.

**Claim 1:** For all $1 \leq i \leq n$, we have $\mathcal{O}_i = R_{\mathfrak{p}_i}$.

*Proof of claim:* Note that $R_{\mathfrak{p}_i} \subseteq \mathcal{O}_i$ holds, since we have merely added inverses for elements in $R \setminus \mathfrak{p}_i \subseteq \mathcal{O}_i \setminus \mathfrak{m}_i$, and every element in $\mathcal{O}_i \setminus \mathfrak{m}_i$ has an inverse in $\mathcal{O}_i$. Now take $a \in \mathcal{O}_i$, define $I_a := \{j \in \{1, \ldots, n\} : a \in \mathcal{O}_j\}$ and write $\alpha_j = a + \mathfrak{m}_j \in \mathcal{O}_j/\mathfrak{m}_j$ for each $j \in I_a$. Choose a prime $p$ such that we have $p > \mathrm{char}(\mathcal{O}_j/\mathfrak{m}_j)$ and such that $\alpha_j$ is not a primitive $p$th root of unity in $\mathcal{O}_j/\mathfrak{m}_j$ for all $j \in I_a$.

Define $b := 1 + a + \ldots + a^{p-1}$. We show that we have $b^{-1}, ab^{-1} \in \mathcal{O}_j$ for all $j$. We consider three cases:

(1) If $a \in \mathcal{O}_j$ and $\alpha_j = 1$ then $\overline{b} = 1 + 1 + \ldots + 1 = p \neq 0$, so we get $b \in \mathcal{O}_j^\times$. As we have assumed $a \in \mathcal{O}_j$, we get $b^{-1}, ab^{-1} \in \mathcal{O}_j$ in this case.
(2) If $a \in \mathcal{O}_j$ and $\alpha_j \neq 1$ then $\overline{b} = \frac{1-\alpha_j^p}{1-\alpha_j} \neq 0$, so again we have $b \in \mathcal{O}_j^\times$ and hence $b^{-1}, ab^{-1} \in \mathcal{O}_j$.
(3) In case $a \notin \mathcal{O}_j$, note that $a^{-1} \in \mathfrak{m}_j$ holds. Thus, we have $1 + a^{-1} + \ldots + a^{-(p-1)} \in \mathcal{O}_j^\times$, implying

$$b^{-1} = a^{-(p-1)}(1 + a^{-1} + \ldots + a^{-(p-1)})^{-1} \in \mathcal{O}_j$$

and

$$ab^{-1} = a^{-(p-2)}(1 + a^{-1} + \ldots + a^{-(p-1)})^{-1} \in \mathcal{O}_j.$$

Hence, we have $b^{-1}, ab^{-1} \in \mathcal{O}_j$ for each $j$, so we get $b^{-1}, ab^{-1} \in R$. As we have $b \in \mathcal{O}_i$, we obtain $b^{-1} \notin \mathfrak{m}_i \cap R = \mathfrak{p}_i$. Thus, we conclude $a = ab^{-1}/b^{-1} \in R_{\mathfrak{p}_i}$ which proves the claim.

**Claim 2:** $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are exactly the maximal ideals of $R$.

*Proof of claim:* We first show that each $\mathfrak{p}_i$ is a maximal ideal of $R$. Assume that for some $i$, $\mathfrak{p}_i$ is not a maximal ideal. Then there is some maximal ideal $\mathfrak{b} \leq R$ with $\mathfrak{p}_i \subsetneq \mathfrak{b}$ and some $\mathfrak{m} \leq \mathcal{O}_i$ maximal with $\mathfrak{b} \subseteq \mathfrak{m}$. As $\mathfrak{m}_i$ is the unique maximal ideal of $\mathcal{O}_i$, this implies $\mathfrak{m}_i = \mathfrak{m}$ and hence $\mathfrak{m}_i \cap \mathcal{O}_i = \mathfrak{b}$, contradicting $\mathfrak{b} \neq \mathfrak{p}_i$. Thus, $\mathfrak{p}_i$ is maximal.

Now, let $\mathfrak{m}$ be a maximal ideal of $R$. Suppose for a contradiction that $\mathfrak{m} \neq \mathfrak{p}_i$ holds for all $1 \leq i \leq n$. Then, for all $1 \leq i \leq n$ there is some $m_i \in \mathfrak{m}$ and $p_i \in \mathfrak{p}_i$ with $1 = p_i + m_i$. So, we have

$$\prod_{1 \leq i \leq n} (1 - m_i) = 1 + m = \prod_{1 \leq i \leq n} p_i$$

for some $m \in \mathfrak{m}$. Note that we have

$$R^\times = \bigcap_{1 \leq i \leq n} \mathcal{O}_i^\times = R \setminus (\mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_n).$$

As we have $\mathfrak{m} \subseteq R \setminus R^\times$, we get $m \in \mathfrak{p}_j$ for some $1 \leq j \leq n$. This implies

$$1 = \left( \prod_{1 \leq i \leq n} p_i \right) - m \in \mathfrak{p}_j,$$

a contradiction to $\mathfrak{p}_j$ being a proper ideal of $R$. This proves the claim.

Note that we have $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$ for all $j$, since otherwise we would have $\mathcal{O}_j = R_{\mathfrak{p}_j} \subseteq R_{\mathfrak{p}_i} = \mathcal{O}_i$. Thus, we have for $i \neq j$ that $\mathfrak{p}_i + \mathfrak{p}_j$ is an ideal which strictly contains a maximal ideal, i.e., $\mathfrak{p}_i + \mathfrak{p}_j = R$ for all $i \neq j$. By the Chinese Remainder Theorem, the canonical map

$$R \to R/\mathfrak{p}_1 \times \ldots \times R/\mathfrak{p}_n$$

is surjective. Thus, since

$$R/\mathfrak{p}_i \cong R_{\mathfrak{p}_i}/\mathfrak{p}_i R_{\mathfrak{p}_i} = \mathcal{O}/\mathfrak{m}_i,$$

the induced map

$$R \to \mathcal{O}_1/\mathfrak{m}_1 \times \ldots \times \mathcal{O}_n/\mathfrak{m}_n$$

is also surjective, and hence there is an $x$ with $x \in x_i + \mathfrak{m}_i$ for all $i$, as desired. □

Using the Weak Approximation Theorem, we can now prove the finite version of the Conjugation Theorem.

**Theorem 2.13.** *(Conjugation Theorem) Let $L/K$ be a finite normal extension of fields. Suppose $\mathcal{O}_v$ is a valuation ring of $K$ and that $\mathcal{O}_{w_1}, \mathcal{O}_{w_2}$ are valuation rings of $L$ extending $\mathcal{O}_v$. Then $\mathcal{O}_{w_1}$ and $\mathcal{O}_{w_2}$ are conjugate over $K$, i.e., there is some $\sigma \in G = \mathrm{Aut}(L/K)$ with $\sigma(\mathcal{O}_{w_1}) = \mathcal{O}_{w_2}$.*

*Proof.* We first reduce to the case $L/K$ Galois. Fix an algebraic closure $K^{\mathrm{alg}}$ of $K$ with $L \subseteq K^{\mathrm{alg}}$. Define $K^{\mathrm{sep}} = \{a \in K^{\mathrm{alg}} : a \text{ separable over } K\}$ and consider $K \subseteq K^{\mathrm{sep}} \cap L \subseteq L$. As $K^{\mathrm{sep}} \cap L \subseteq L$ is a purely inseparable extension, every valuation on $K^{\mathrm{sep}} \cap L$ has a unique extension to $L$ by Proposition 2.10. Moreover, there is a canonical isomorphism $\mathrm{Aut}(L \cap K^{\mathrm{sep}}/K) \cong \mathrm{Aut}(L/K)$. Thus, we may assume that $L = K^{\mathrm{sep}} \cap L$, and hence that $L/K$ is Galois.

Let $\widetilde{\mathcal{O}}$ be the integral closure of $\mathcal{O}_v$ in $L$.

**Claim:** $\widetilde{\mathcal{O}} = \bigcap_{\sigma \in G} \sigma \mathcal{O}_{w_1}$

*Proof of claim:* Since each $\sigma \mathcal{O}_{w_1}$ is a valuation ring, each is integrally closed by Proposition 1.14. As we have $\mathcal{O}_v \subseteq \sigma \mathcal{O}_{w_1}$ for all $\sigma \in G$, the inclusion '$\subseteq$' holds.

Conversely, take $x \in \bigcap_{\sigma \in G} \sigma \mathcal{O}_{w_1}$ and consider the distinct conjugates $x = x_1, \ldots, x_n$ of $x$ over $K$. Then, the minimal polyomial of $x$ over $K$ is of the form

$$f(t) = \prod_{\sigma \in H} t - \sigma(x) \in K[t]$$

for an appropriate $H \subseteq G$. As $x \in \bigcap_{\sigma\in G} \sigma\mathcal{O}_{w_1}$, we have $\tau(x) \in \bigcap_{\sigma\in G} \sigma\mathcal{O}_w$ for each $\tau \in G$. Thus, the minimal polynomial

$$f(t) \in K[t] \cap \bigcap_{\sigma\in G} \sigma\mathcal{O}_w[t] = \mathcal{O}_v[t],$$

and so $x$ is integral over $\mathcal{O}_v$, i.e., $x \in \widetilde{\mathcal{O}}$ holds. This proves the claim.

Now assume for a contradiction that we have $\mathcal{O}_{w_2} \neq \sigma\mathcal{O}_{w_1}$ for any $\sigma \in G$. Then, $\sigma\mathcal{O}_{w_1}$ and $\mathcal{O}_{w_2}$ are incomparable for all $\sigma \in G$ by Proposition 2.10. Then, by the Weak Approximation Theorem (Theorem 2.12), there exists some $x \in \mathfrak{m}_{w_2}$ with $x \in (\sigma\mathcal{O}_{w_1})^\times$ for all $\sigma$. Now, we have $x^{-1} \in \bigcap_{\sigma\in G} \sigma\mathcal{O}_{w_1} \setminus \mathcal{O}_{w_2}$, and hence

$$\widetilde{\mathcal{O}} \overset{1.14}{\subsetneq} \mathcal{O}_{w_2} \cap \bigcap_{\sigma\in G} \sigma\mathcal{O}_{w_1} \subsetneq \bigcap_{\sigma\in G} \sigma\mathcal{O}_{w_1} = \widetilde{\mathcal{O}}$$

which is a contradiction. □

**Fact 2.14.** *The Conjugation Theorem also holds for arbitrary (not necessarily finite) normal extensions $L/K$.*

*Proof.* For infinite extensions, use Theorem 2.13 and Zorn's lemma. Alternatively, see [EP05, Theorem 3.2.15]. □

We now draw some corollaries from Theorem 2.13 and its proof.

**Corollary 2.15.** *(from the proof of Theorem 2.13) Suppose $L/K$ is finite and Galois, $v$ a valuation on $K$, $\widetilde{\mathcal{O}}$ the integral closure of $\mathcal{O}_v$ in $L$. Then, we have $\widetilde{\mathcal{O}} = \bigcap \mathcal{O}_w$, where $w$ ranges over all prolongations of $v$ to $L$.*

**Corollary 2.16.** *Suppose $L/K$ is finite, $v$ a valuation on $K$. Then $v$ has only finitely many extensions to $L$.*

*Proof.* Consider $N$, the normal hull of $L/K$, namely the smallest normal extension of $K$ containing $L$ in a given algebraic closure $K^{\text{alg}}$ of $K$. If $[L : K] = n$ then $[N : K] \leq n!$, so $v$ has at most $n!$ extensions to $N$, hence also to $L$. □

The Fundamental Inequality (Theorem 2.8) above can in fact be strengthened to an equality in certain settings. The proof of this fact is beyond the scope of this course and uses both the Conjugation Theorem (Theorem 2.13) and sophisticated Galois Theory (some but not all of which is developed in Section 4). In this course, we will not use the stronger version. For a proof, we refer the reader to [EP05].

**Fact 2.17** (Fundamental Inequality Revisited, [EP05, Theorems 3.3.3 and 3.3.5])**.** *Suppose $L/K$ is a field extension with $[L : K] = n$, $v$ a valuation on $K$, and $w_1, \ldots, w_r$ the prolongations of $v$ to $L$. Write $e_i = e(w_i/v)$ and $f_i = f(w_i/v)$. Then, we have*

$$\sum_{i=1}^{r} e_i f_i \leq n$$

*and equality holds if either* $\operatorname{char}(Kv) = 0$*, or $(K, v)$ has mixed characteristic and with $v(p)$ finite (i.e., the set $\{\gamma \in vK : 0 \leq \gamma \leq v(p)\}$ is finite).*

## 3. Hensel's Lemma

3.1. **Completions.** In this section, we consider completions of valued fields. First, we need the notion of a Cauchy sequence:

**Definition 3.1.** *Let $(K, v)$ be a valued field with $vK \leq (\mathbb{R}, +)$ and $(a_i)_{i\in\mathbb{N}}$ a sequence in $K$. We say that $(a_i)_{i\in\mathbb{N}}$ is* Cauchy *if for all $\gamma \in \Gamma$ there exists $N \in \mathbb{N}$ such that for all $n, m > N$, we have*

$$v(a_n - a_m) > \gamma.$$

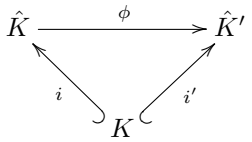
Let $K$ be any field. Recall that a map $|\cdot| : K \to \mathbb{R}$ is an *absolute value* if it satisfies $\forall x, y \in K$:

(AV1) $|x| = 0$ if and only if $x = 0$
(AV2) $|xy| = |x||y|$
(AV3) $|x + y| \leq |x| + |y|$

An absolute value is called *ultrametric* if the third condition (the triangle inequality) can be strengthened to $|x + y| \leq \max\{|x|, |y|\}$.

**Remark 3.2.** *If $(K, v)$ is a valued field with $vK \leq (\mathbb{R}, +)$, then $K$ has an absolute value (in fact, an ultrametric absolute value) defined by $|x|_v = e^{-v(x)}$. A sequence is Cauchy in the valuation theoretic sense if and only if it is Cauchy with respect to $|\cdot|_v$ in the 'classical' sense.*

**Theorem 3.3.** *Let $(K, |\cdot|)$ be a field with an absolute value. Then, there is a field $\hat{K}$ which is complete with respect to $|\cdot|$ and an embedding $i : K \hookrightarrow \hat{K}$ which preserves $|\cdot|$, such that $K$ is dense in $\hat{K}$. Moreover, if $(\hat{K}', i')$ is another such pair, then there exists a unique continuous isomorphism $\phi : \hat{K} \to \hat{K}'$ preserving $|\cdot|$ such that the diagram*




*commutes. $\hat{K}$ is called the* completion *of $K$ with respect to $|\cdot|$.*

*Proof.* Exactly the same as the construction of the reals from the rationals as Cauchy sequences, i.e., $\hat{K}$ is the ring of Cauchy sequences modulo the maximal ideal of zero sequences. Details can be found in [EP05, Theorem 1.1.4]. □

We now study the completion of $\mathbb{Q}$ with respect to the $p$-adic absolute value. The resulting structure is called the *field of $p$-adic numbers*.

**Example 3.4.** *Let $K = \mathbb{Q}$ and $v = v_p$ for some prime $p$. We define $\mathbb{Q}_p$, the $p$-adic numbers, to be the completion of $\mathbb{Q}$ with respect to $|\cdot|_p := |\cdot|_{v_p}$. We claim that there is a canonical isomorphism $\mathbb{Q}_p \cong R$, where*

$$R = \{\sum_{i=m}^{\infty} a_i p^i : a_i \in \{0, \ldots, p-1\}, m \in \mathbb{Z}\}.$$

*Clearly, we have $\mathbb{N} \subseteq R$; writing a natural number $n$ base $p$ gives finitely many $a_i$ such that $n = \sum_{i=0}^{k} a_i p^i \in R$, e.g., for $p = 2$ we have*

$$5 = 1 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2 \in R.$$

*It is easy to check that $R$ is a commutative ring with the obvious addition and multiplication (componentwise mod $p$ with carrying over), e.g. again for $p = 2$, we have*

$$5 \cdot 6 = (1 \cdot 2^0 + 1 \cdot 2^2)(1 \cdot 2^1 + 1 \cdot 2^2) = 2^1 + 2^2 + 2^3 + 2^4$$

*and*

$$\begin{aligned} 5 + 6 = (1 \cdot 2^0 + 1 \cdot 2^2) + (1 \cdot 2^1 + 1 \cdot 2^2) &= 2^0 + 2^1 + 2 \cdot 2^2 \\ &= 2^0 + 2^1 + 2^3. \end{aligned}$$

*The trick for additive inverses is to have infinite carryovers with remainder zero. For example,*

$$-5 = 2^0 + 2^1 + \sum_{i=3}^{\infty} 2^i.$$

*Finally, multiplicative inverses exist in $R$; in the special case of*

$$a = \sum_{i=0}^{\infty} a_i p^i \text{ with } a_0 = 1$$

*we have*

$$\begin{aligned} a^{-1} = (1 + p\sum_{i=0}^{\infty} a_{i+1} p^i)^{-1} &= \big(1 - p \underbrace{\left( -\sum_{i=0}^{\infty} a_{i+1} p^i \right)}_{=:x} \big)^{-1} \\ &= 1 + px + (px)^2 + (px)^3 + (px)^4 + (px)^5 + \dots \end{aligned}$$

*where the right hand side is a well-defined element in $R$ as we only need to calculate a finite sum to determine each coefficient. For example, if $p = 2$ we have*

$$\begin{aligned} 5^{-1} = (1 - 2 \cdot (-2))^{-1} &= 2^0 - 2^2 + 2^4 - 2^6 + 2^8 - 2^{10} + \dots \\ &= 2^0 + 2^2 + 2^3 + 2^6 + 2^7 + 2^{10} + 2^{11} + 2^{14} + \dots \end{aligned}$$

*To invert a general $\sum_{i=m}^{\infty} a_i p^i$ with $a_m \neq 0$, we first invert $p^{-m} a_m^{-1} \sum_{i=m}^{\infty} a_i p^i$, then multiply the result by $a_m \cdot p^m$.*

*Thus, $R$ is a field, and so we have $\mathbb{Q} \subseteq R$. We can extend $v_p$ (and thus $|\cdot|_p$) to $R$ via*

$$v_p \left( \sum_{i=m}^{\infty} a_i p^i \right) = \min\{i : a_i \neq 0\}.$$

*This is a valuation with value group $\mathbb{Z}$ and residue field $\mathbb{F}_p$ (since the residue field is a field with $p$ elements).*

*We now show that $\mathbb{Q}$ is dense in $R$: every $a = \sum_{i=m}^{\infty} a_i p^i \in R$ is the limit of $\left( \sum_{i=m}^{m+n} a_i p^i \right)_{n \geq 0}$. Note that this is a Cauchy sequence since for any $\gamma \in \mathbb{Z}$ we can choose any $N > \gamma$ and have*

$$\forall n, n' \geq N : \; v_p( \sum_{i=m}^{m+n} a_i p^i - \sum_{i=m}^{m+n'} a_i p^i ) \geq \min\{n, n'\} > \gamma$$

*and it clearly converges to $a$. Moreover, $\left( \sum_{i=m}^{m+n} a_i p^i \right)_{n \geq 0}$ is a sequence in $\mathbb{Q}$ since it is the product of $p^m$ and the finite sum $\sum_{i=0}^{n} a_{i+m} p^i$, and sums of this form are precisely the representations of natural numbers base $p$.*

*Finally, the fact that $(R, |\cdot|_p)$ is complete is easy to check: if $(b_n)_{n\in\mathbb{N}}$ is a Cauchy sequence, then $v(b_n - b_{n'}) > \gamma$ means that $b_n$ and $b_{n'}$ agree on the first $\gamma$-many terms in their sums. We can form a limit $b = \sum c_i p^i$ by choosing $c_i = (b_n)_i$ for $n$ large enough such that $(b_{n'})_i = (b_n)_i$ holds for $n' \geq n$. Then, we have $b \in R$. Thus, we have $R \cong \mathbb{Q}_p$, and its valuation ring with respect to the $p$-adic valuation is given by*

$$\mathbb{Z}_p := \mathcal{O}_{v_p} = \left\{ \sum_{i=0}^{m} a_i p^i : m \in N, a_i \in \{0, \dots, p-1\} \right\}.$$

**Example 3.5.** *Let $k$ be a field and consider the field $k(t)$ with the $t$-adic valuation which is defined as*

$$v_t\left(\sum_{i=0}^{n} a_i t^i\right) = \min\{i : a_i \neq 0\}$$

*on $k[t]$ and extended to the quotient field $k(t)$ in the usual way. The completion of $(k(t), v_t)$ is the power series field $k((t))$ with valuation*

$$v_t\left(\sum_{i=m}^{\infty} a_i t^i\right) = \min\{i : a_i \neq 0\}.$$

*The proof is a simplified version of the one given in the previous example, as there is no need to deal with carrying over.*

**Theorem 3.6** (Hensel's Lemma for complete valued fields)**.** *Let $(K, v)$ be a valued field with $vK \leq \mathbb{R}$ such that $K$ is complete with respect to $|\cdot|_v$. Given $a \in \mathcal{O}_v$ and $f \in \mathcal{O}_v[x]$ such that $v(f(a)) > 2v(f'(a))$ holds, there is some $b \in \mathcal{O}_v$ such that we have $f(b) = 0$ and $v(b - a) > v(f'(a))$.*

The proof works via Newton's method. The idea is that if $f(a)$ is 'close' to zero (i.e., has 'big' valuation), then $f(a - \frac{f(a)}{f'(a)})$ is 'even closer'. Before we get to the proof, we show a helpful lemma:

**Lemma 3.7.** *Suppose $(K, v)$ is a valued field, $f \in \mathcal{O}_v[X]$. Then, there is some $g(X, Y) \in \mathcal{O}_v[X, Y]$ with $f(X + Y) = f(X) + f'(X)Y + Y^2 g(X, Y)$.*

*Proof.* Assume $f(X) = \sum_{i=0}^{d} c_i X^i$ for some $c_i \in \mathcal{O}_v$. Then, we have

$$f(X+Y) = \sum_{i=0}^{d} c_i (X+Y)^i = c_0 + \sum_{i=1}^{d} c_i (X^i + iX^{i-1}Y + g_i(X,Y)Y^2)$$

for some appropriate $g_i \in \mathcal{O}_v[X, Y]$

$$= \underbrace{\sum_{i=0}^{d} c_i X^i}_{f(X)} + \underbrace{\sum_{i=1}^{d} i c_i X^{i-1} Y}_{f'(X)Y} + \underbrace{\sum_{i=1}^{d} c_i g_i(X,Y)}_{=:g(X,Y)}.$$

□

*Proof of Theorem 3.6.* Consider a valued field $(K, v)$, an element $a \in \mathcal{O}_v$ and a polynomial $f \in \mathcal{O}_v[X]$ satisfying the assumptions of the theorem. We will use Newton's method, starting at $a$, to construct a Cauchy sequence; $b$ will be the limit of said Cauchy sequence.

Choose $\varepsilon \in \mathbb{R}_{>0}$ such that $v(f(a)) = 2v(f'(a))+\varepsilon$ holds. Note that since we have $v(f(a)) > 2v(f'(a))$, we get in particular $f'(a) \neq 0$ and $f(a)/f'(a) \in \mathfrak{m}_v$. Define $a_1 := a - \frac{f(a)}{f'(a)}$, so we have $a_1 \in \mathcal{O}_v$. Applying Lemma 3.7, we get

$$f(a_1) = f(a) + f'(a)\left(-\frac{f(a)}{f'(a)}\right) + \left(\frac{f(a)}{f'(a)}\right)^2 \cdot d = \left(\frac{f(a)}{f'(a)}\right)^2 \cdot d$$

for some $d \in \mathcal{O}_v$. Thus, we have

$$v(f(a_1)) \geq 2v(f(a)/f'(a)) = 2v(f(a)) - 2v(f'(a)) = 2v(f'(a)) + 2\varepsilon$$

and, using Lemma 3.7 again,

$$v(f'(a_1)) = v(f'(a) + \frac{f(a)}{f'(a)} \underbrace{\left(-f''(a) + \frac{f(a)}{f'(a)} \cdot \widetilde{d}\right)}_{=:e \in \mathcal{O}_v}) = v(f'(a))$$

since $v(f'(a)) < v(f(a)/f'(a))$ holds by assumption. In particular, we get $f'(a_1) \neq 0$. Note that by the definition of $a_1$, we have $v(a_1 - a) = v(f'(a)) + \varepsilon$.

We now set $a_0 := a$ and define a sequence in $K$ via $a_{n+1} = a_n - f(a_n)/f'(a_n)$ for $n \geq 0$. Then, we can inductively repeat the argument replacing $a_1$ with $a_{n+1}$ and $a$ with $a_n$. For any $n \geq 1$, we get

$$v(f'(a_{n+1})) = v(f'(a_n)) = v(f'(a))$$

and hence $f'(a_n) \neq 0$ which implies that the sequence is well-defined. Moreover, we have

$$v(f(a_{n+1})) \geq 2v(f'(a_n)) + (n+1)\varepsilon = 2v(f'(a)) + (n+1)\varepsilon,$$

which implies that if the sequence coverges, it must converge towards a root of $f$ as the sequence of its values is cofinal in $vK \leq \mathbb{R}$, and

$$\begin{aligned} v(a_{n+1} - a_n) &= v(\frac{f(a_n)}{f'(a_{n+1})}) \\ &\geq 2v(f'(a_n)) + (n+1)\varepsilon - v(f'(a)) \\ &= v(f'(a)) + (n+1)\varepsilon \end{aligned}$$

which implies that the sequence is Cauchy. Since $(K, v)$ is complete, there is a limit $b \in K$ with $f(b) = 0$. Finally, as we have

$$v(a_n - a) \geq \min_{0 \leq m < n} \{v(a_{m+1} - a_m)\} > v(f'(a)),$$

we conclude that $v(b) > v(f'(a))$ holds. □

Our next main aim is to find an alternative to completions in case the value group is not a subgroup of $(\mathbb{R}, +)$. The goal is to find a smallest extension of a valued field such that the conclusion of Theorem 3.6 holds. These will be called henselizations.

3.2. **Henselian Fields.** In this chapter, we study fields for which the conclusion of Theorem 3.6 holds, roughly speaking 'if a polynomial takes a value close to zero, then it has a root close by'. We first give an alternative definition:

**Definition 3.8.** *A valued field $K$ is called* henselian *if $v$ extends uniquely to every finite (algebraic) extension of $K$.*

**Remark 3.9.** *It follows from Proposition 2.10 that $(K, v)$ is henselian if and only if $v$ extends uniquely to every finite separable extension of $K$. Fix an algebraic closure $K^{alg}$ of $K$. Recall that the separable closure $K^{sep}$ of $K$ (in $K^{alg}$) is exactly the compositum of all finite separable extensions of $K$ (in $K^{alg}$). Thus, $(K, v)$ is henselian if and only if $v$ extends uniquely to $K^{sep}$. Proposition 2.10 implies moreover that $v$ extends uniquely to $K^{sep}$ if and only if it extends uniquely to $K^{alg}$.*

We now show that henselianity is indeed equivalent to the fact that 'Hensel's Lemma holds'.

**Theorem 3.10** (Hensel's Lemma)**.** *For a valued field $(K, v)$, the following are equivalent:*

*(1) $(K, v)$ is henselian.*
*(2) Hensel's Lemma holds: for all $f \in \mathcal{O}_v[X]$, $a \in \mathcal{O}_v$ with $v(f(a)) > 2v(f'(a))$, there exists some $b \in \mathcal{O}_v$ satisfying $f(b) = 0$ and $v(a - b) > v(f'(a))$.*
*(3) Simple zeroes lift: For each $f \in \mathcal{O}_v[X]$ and $a \in \mathcal{O}_v$ with $\overline{f}(\overline{a}) = \overline{0}$ and $\overline{f}'(\overline{a}) \neq \overline{0}$ in the residue field, there exists some $b \in \mathcal{O}_v$ such that $f(b) = 0$ and $\overline{b} = \overline{a}$ holds.*
*(4) Every polynomial of the form $X^n + X^{n-1} + a_{n-2}X^{n-2} + \ldots + a_0$ with $a_i \in \mathfrak{m}_v$ for $0 \leq i \leq n - 2$ has a zero in $K$.*

Before we prove the theorem, we turn to another helpful lemma. This lemma also explains where the Gauss extension of a valuation (as defined in Example 2.5) gets its name from.

**Lemma 3.11** (Gauss's Lemma)**.** *Suppose $(K, v)$ is a valued field, and consider some $f \in \mathcal{O}_v[X]$. Then there are $h_1, \ldots, h_n \in \mathcal{O}_v[X]$, which are irreducible in $K[X]$, with*

$$f = h_1 \cdots h_n.$$

*Proof.* Let $f = g_1 \cdots g_n$ be a factorization of $f$ into irreducible factors in $K[X]$. Consider the Gauss extension $\widetilde{v}$ of $v$ to $K(X)$, so

$$\widetilde{v}(\sum_{i=0}^{d} a_i X^i) = \min_{0 \leq i \leq d} \{v(a_i)\}.$$

We can write $f, g_1, \ldots, g_n$ as $f = a\widetilde{f}$ and $g_i = b_i \widetilde{g}_i$ with $a, b_1, \ldots, b_n \in K$ and $\widetilde{v}(\widetilde{f}) = \widetilde{v}(\widetilde{g}_i) = 0$ for all $1 \leq i \leq n$. Note that $f \in \mathcal{O}_v[X]$ implies $a \in \mathcal{O}_v$ and $\widetilde{v}(\widetilde{g}_i) = 0$ implies $\widetilde{g}_i \in \mathcal{O}_v[X]$. Since we have

$$v(b_1 \cdots b_n) = \sum_{i=1}^{n} \widetilde{v}(g_i) = \widetilde{v}(f) = v(a),$$

we get $b = b_1 \cdots b_n \in O_v$. Now, defining $h_1 := b\widetilde{g}_1$, $h_i := \widetilde{g}_i$ for $i \geq 2$ gives a factorization of $f$ as desired. □

*Proof of Theorem 3.10.* (2) ⇒ (3): Assume we have $f \in \mathcal{O}_v[X]$ and $a \in O_v$ with $\overline{f}(\overline{a}) = 0$ and $\overline{f}'(\overline{a}) \neq 0$. This implies $f(a) \in \mathfrak{m}_v$ and $f'(a) \notin \mathfrak{m}_v$. Thus, we get

$$v(f(a)) > 0 = 2v(f'(a))$$

and hence, if (2) holds, there is some $b \in \mathcal{O}_v$ with $f(b) = 0$ and $v(b-a) > v(f'(a)) = 0$, in particular $a - b \in \mathfrak{m}_v$. Thus, statement (3) holds.

(3) ⇒ (4): Given a polynomial of the form

$$X^n + X^{n-1} + a_{n-2}X^{n-2} + \cdots + a_0$$

with $a_i \in \mathfrak{m}_v$, we have $\overline{f} = X^n + X^{n-1} = (X+1)X^{n-1}$. Thus, $-1$ is a simple zero of $\overline{f}$ in $Kv$ and, if (3) holds, $f$ has a zero in $K$.

(1) ⇒ (3): Take $f \in \mathcal{O}_v[X]$, $a \in \mathcal{O}_v$ with $\overline{f}(\overline{a}) = \overline{0}$ and $\overline{f}'(\overline{a}) \neq \overline{0}$. By Lemma 3.11, we may assume that $f$ is irreducible: otherwise, we replace $f$ by some irreducible component $h \in \mathcal{O}_v[X]$ with $\overline{h}(\overline{a}) = \overline{0}$ and $\overline{h}'(\overline{a}) \neq \overline{0}$.

Moreover, $f$ is separable: if $f$ is inseparable, then we have $f = g(x^p)$ for some $g \in \mathcal{O}_v[X]$ and in that case $\overline{f}'$ would be identically zero, which contradicts $\overline{f}'(\overline{a}) \neq \overline{0}$.

Now, let $L$ be the splitting field of $f$ over $K$. Then there are $a_1, \ldots, a_n \in L$ with $f = c\prod(X - a_i)$ for some $c \in \mathcal{O}_v^\times$ (again, $\overline{f}' \equiv 0$ otherwise); we may assume that $\overline{a}_1 = \overline{a}$. If (1) holds, let $w$ be the unique extension of $v$ to $L$ and assume $n > 1$ (otherwise, $a_1 \in K$ and we are done). By Galois Theory, there is some $\sigma \in \mathrm{Gal}(L/K)$ with $\sigma(a_1) = a_2$. As $w$ is the unique extension of $v$, $\sigma$ induces an automorphism $\overline{\sigma} \in \mathrm{Gal}(Lw/Kv)$ such that

$$\overline{a}_2 = \overline{\sigma}(\overline{a}_1) = \overline{\sigma}(\overline{a}) = \overline{a} = \overline{a}_1$$

(note that $\overline{a} \in Kv$ is fixed by $\overline{\sigma}$). But then $\overline{a} = \overline{a}_1 = \overline{a}_2$ is not a simple root, a contradiction!

(3) ⇒ (2): Take $f$ and $a$ as in (2). By Lemma 3.7, we have

$$f(a - X) = f(a) - f'(a)X + X^2 g(a, X)$$

for some $g(Y, X) \in \mathcal{O}_v[Y, X]$; write $\widetilde{g}(X) = g(a, X) \in \mathcal{O}_v[X]$. As $f'(a) \neq 0$ by assumption, consider $Y = X/f'(a)$. Then, we have

$$h(Y) := \frac{f(a - f'(a)Y)}{f'(a)^2} = \frac{f(a)}{f'(a)^2} - Y + \widetilde{g}(f'(a)Y)Y^2 \in \mathcal{O}_v[Y]$$

and $\overline{h}(\overline{0}) = \overline{0} \neq -1 = \overline{h}(\overline{0})$. If (3) holds, there exists some $\alpha \in \mathcal{O}_v$ such that $h(\alpha) = 0$. Choose $b = a - f'(a)\alpha \in \mathcal{O}_v$; check that this is a zero of $f$ satisfying $v(b - a) > v(f'(a))$.

(4) ⇒ (1): We show ¬(1) ⇒ ¬(4). Assume $(K, v)$ is not henselian, so there is some finite Galois extension $N/K$ with $G = \mathrm{Gal}(N/K)$ such that $v$ has more than one prolongation to $N$; we fix one of these and denote it by $w$. Define $D := \{\sigma \in G : \sigma(\mathcal{O}_w) = \mathcal{O}_w\}$; and note that it is a subgroup of $G$. Moreover, since $v$ has more than one extension to $N$, the Conjugation Theorem (Theorem 2.13) implies $D \lneq G$. Consider the fixed field $L := \mathrm{Fix}(D)$; since $D \neq G$, we conclude that $L$ is a proper extension of $K$. Let $\mathcal{O}_w = \mathcal{O}_1, \ldots, \mathcal{O}_n$ be the conjugates of $\mathcal{O}_w$ in $N$ (by Theorem 2.13, these are the valuation rings of all prolongations of $v$ to $N$), and define $\mathcal{O}_i' := \mathcal{O}_i \cap L$. By the definition of $L$ and Theorem 2.13, $\mathcal{O}_1'$ has a unique prolongation to $L$. Thus, there is some $\mathcal{O}_j'$ with $\mathcal{O}_j' \neq \mathcal{O}_1'$.

Consider $R := \bigcap_{1 \leq i \leq n} \mathcal{O}_i' \subseteq L$. By the (proof of the) Weak Approximation Theorem (Theorem 2.12), we can choose $\beta \in R$ with $\beta - 1 \in \mathfrak{m}_1'$ and $\beta \in \mathfrak{m}_i'$ for $1 < i \leq n$. Since $\mathcal{O}_1' \neq O_j'$, we get $\beta \notin K$ (since an element of $K$ is in one maximal ideal if and only if it is in all of the maximal ideals). Consider the minimal polynomial $f$ of $\beta$ over $K$, say

$$f(X) = X^k + a_{k-1}X^{k-1} + \ldots + a_0$$

for some $a_m \in K$ and $0 \leq m < k$.

**Claim:** We have $a_{k-1} \in 1 + \mathfrak{m}_v$ and $a_{k-2}, \ldots, a_0 \in \mathfrak{m}_v$.

*Proof of claim:* Let $\beta = \beta_1, \ldots, \beta_k$ be the conjugates of $\beta$ in $N$. Note that for $\sigma \in G \setminus D$ we have $\beta \in \sigma(\mathfrak{m}_1)$, so $\sigma(\beta) \in \mathfrak{m}_1$ holds for all $\sigma \in G \setminus D$. Since each $\beta_i$ occurs as $\sigma(\beta_1)$ for some $\sigma \in G \setminus D$, we have $\beta_i \in \mathfrak{m}_1$ for all $i > 1$. Now

$$f = \prod_{1 \leq i \leq k} (X - \beta_i)$$

and so $a_{k-1} = -(\beta_1 + \ldots + \beta_k) \in (1 + \mathfrak{m}_1) \cap K = 1 + \mathfrak{m}_v$ holds (since we have $\beta_1 \in 1 + \mathfrak{m}_1$ and $\beta_i \in \mathfrak{m}_1$ for $i > 1$). For $i \neq k-1$, we get that $a_i$ is a sum of products of at least two (distinct) $\beta_j$, and so $a_i \in \mathfrak{m}_1 \cap K = \mathfrak{m}_v$ holds for each $i < k-1$.

Now consider the polynomial

$$g := \frac{f(a_{k-1}X)}{(a_{k-1})^k} = X^k + X^{k-1} + \widetilde{a}_{k-2}X^{k-2} + \ldots + \widetilde{a}_0$$

over $\mathcal{O}_v$. As we have $a_{k-1} \in 1 + m_v \subseteq O_v^\times$, the claim implies that $\widetilde{a}_i \in \mathfrak{m}_v$ holds for each $0 \leq i < k-1$, and hence $g$ satisfies the assumptions of (4). But $g$ cannot have a zero, since $f$ is irreducible and $k > 1$. Thus, $\neg(4)$ holds. Taking the contrapositive, we conclude that $(4) \Rightarrow (1)$ holds. □

**Examples 3.12.**

- *Let $K$ be any field with the trivial valuation $v$. Then $(K, v)$ satisfies condition* (3) *from Theorem 3.10, so is henselian.*
- *Let $K = \mathbb{Q}_p$ (respectively $k = k((t))$) and $v = v_p$ (resp. $v = v_t$). Then, by Theorem 3.6, $(K, v)$ satisfies condition* (2) *in Theorem 3.10, so is henselian.*
- *Let $K = \mathbb{Q}$, $v = v_p$ for some prime $p$. For $q \neq p$ prime, let*

  $$f(x) = X^n + qX^{n-1} + pqX^{n-2} + \ldots + pq.$$

  *By the Eisenstein criterion, $f$ is irreducible. But*

  $$\overline{f}(X) = X^n + qX^{n-1} = (X - q)X^{n-1}$$

  *has a simple root, so condition* (3) *from Theorem 3.10 fails, and hence $(K, v)$ is not henselian. Alternatively, $f(qX)/q^n$ satisfies the assumption of condition* (4) *in Theorem 3.10, but fails the conclusion.*
- *Let $K = k(t)$ and $v = v_t$. Assume* $\mathrm{char}(k) \neq 2$. *Then $f(X) = X^2 - (t+1)$ is clearly irreducible, but $\overline{f}(X) = X^2 - 1$ has a simple zero, and hence condition* (3) *from Theorem 3.10 fails. For* $\mathrm{char}(k) = 2$, *use $f(X) = X^2 + X - (t+1)$ instead. Hence, $(k(t), v_t)$ is not henselian.*

The proof of the following corollary to Theorem 3.10 is left as an (easy) exercise.

**Corollary 3.13.** *If $(K, v)$ is henselian and* $\gcd(\mathrm{char}(Kv), n) = 1$ *holds, then we have $1 + \mathfrak{m}_v \subseteq K^n$.*

The final example of a henselian valued field treated in this section is left as an ambitious exercise. Help can be found in [EP05, Exercises 3.5.5 and 3.5.6 and Remark 4.1.8].

**Exercise 3.14.** *Suppose $k$ is a field and $\Gamma$ an ordered abelian group. We define*

$$k((\Gamma)) = \left\{ \sum_{\gamma\in\Gamma} a_\gamma t^\gamma : a_\gamma \in k \text{ for all } \gamma \in \Gamma \text{ and } \{\gamma : a_\gamma \neq 0\} \text{ is well-ordered} \right\}$$

*and call $k((\Gamma))$ the* generalized power series field *or* Hahn field over $k$ with exponents in $\Gamma$. *We define a valuation $v$ on $k((\Gamma))$ by setting*

$$v(\sum_{\gamma\in\Gamma} a_\gamma t^\gamma) = \min\{\gamma : a_\gamma \neq 0\}$$

*for $\sum_{\gamma\in\Gamma} a_\gamma t^\gamma \in k((\Gamma))$. Check that $(k((\Gamma)), v)$ is a henselian valued field.*

## 4. Galois Theory of Valued Fields

4.1. **Infinite Galois Theory.** *Assumption* Throughout this subsection, let $K$ be a field and $K^{\text{sep}}$ a fixed separable closure of $K$. Moreover, all finite Galois extensions of $K$ which occur are embedded as subfields into $K^{\text{sep}}$.

**Definition 4.1.** *The* absolute Galois group *of $K$ is defined as*

$$G_K := \text{Aut}(K^{sep}/K).$$

We now treat some infinite Galois Theory which is needed for the construction of the henselization of a valued field. A more comprehensive introduction to infinite Galois Theory can be found in [FJ08, Chapter 1]. We start by discussing the structure of Galois groups as inverse limits.

**Proposition 4.2.** *There is a canonical isomorphism*

$$G_K \cong \{(\sigma_i)_{i\in I} \in (\text{Gal}(L_i/K))_{i\in I} : L_i/K \text{ is finite Galois and if } L_i \subseteq L_j \text{ then } \sigma_j|_{L_i} = \sigma_i\}.$$

*In other words, $G_K = \varprojlim \text{Gal}(L/K)$, where $L$ ranges over all finite Galois extensions of $K$, with connecting homomorphisms for $M \supseteq L \supseteq K$ given by the canonical restriction maps*

$$\text{res}_L : \text{Gal}(M/K) \twoheadrightarrow \text{Gal}(L/K).$$

*Proof.* If $\sigma \in G_K$ then we have $\sigma(L) = L$ (setwise) for all $L/K$ finite Galois: any $\sigma \in G_K$ maps any element $a \in K^{\text{sep}}$ onto some element which has the same minimal polynomial as $a$ over $K$. Thus, $\sigma$ induces a compatible sequence of $(\sigma_i)_{i\in I}$ as described above.

Conversely, given a compatible sequence $(\sigma_i)_{i\in I}$, since each $x \in K^{\text{sep}}$ is contained in some finite Galois extension $L_i/K$, we can define $\sigma(x) = \sigma_i(x)$. The compatibility condition ensures that this definition does not depend on the choice of $L_i$ containing $x$. □

The canonical isomorphism in Proposition 4.2 above defines a topology on $G_K$: consider every finite $\text{Gal}(L/K)$ with the discrete topology and their product $\prod_{i\in I} \text{Gal}(L_i/K)$ with the product topology, then we can endow $G_K \leq \prod \text{Gal}(L_i/K)$ with the subspace topology (in fact, $G_K$ is a closed subset and hence compact see [FJ08, Lemma 1.1.2]).

Like any profinite group, $G_K$ is actually Hausdorff, compact, and totally disconnected as a topological group ([RZ00, Theorem 2.1.3]).

**Example 4.3.** *Fix any prime $p$; we want to describe $G_{\mathbb{F}_p}$. For every $n \in \mathbb{N}$, there exists a unique extension of $\mathbb{F}_p$ of degree $n$, namely $\mathbb{F}_{p^n}$. Because finite fields are perfect, these extensions are all separable, and in fact they are all normal. These are percisely the finite Galois extensions of $\mathbb{F}_p$. As we have*

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$$

*for each $n \in \mathbb{N}$ and $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}$ just in case $n$ divides $m$, we get*

$$G_{\mathbb{F}_p} \cong \lim_{\leftarrow} \mathbb{Z}/n\mathbb{Z} =: \hat{\mathbb{Z}}.$$

Note that all of the above definitions and statements work for any $\mathrm{Gal}(L/K)$ with $L/K$ Galois, not just $G_K = \mathrm{Gal}(K^{\mathrm{sep}})$.

**Theorem 4.4** (Galois correspondence, [FJ08, Propostion 1.3.1])**.** *Suppose $L/K$ is Galois (not necessarily finite). There is a 1-1 correspondence*

$$\{\textit{closed subgroups of } \mathrm{Gal}(L/K)\} \overset{1:1}{\longleftrightarrow} \{\textit{intermediate fields } K \subseteq M \subseteq L\},$$

*given by*

$$H \longmapsto \mathrm{Fix}(H)$$
$$\mathrm{Gal}(L/M) \longmapsfrom M.$$

4.2. **Henselizations.** We are now approaching our final aim, namely to show that each valued field has a 'smallest' extension which is henselian. We fix the following notation: Let $(K, v)$ be a valued field, $K^{\mathrm{sep}}$ a separable closure of $K$, and let $w$ denote some fixed prolongation of $v$ to $K^{\mathrm{sep}}$.

**Definition 4.5.** *We define the* decomposition group of $w$ over $v$ *as*

$$D_{w/v} := \{\sigma \in G_K : \sigma(\mathcal{O}_w) = \mathcal{O}_w\}.$$

Again, this definition works for any Galois extension $L$ of $K$ with $L \subseteq K^{\mathrm{sep}}$. Recall that we already encountered a decomposition group in the proof of Hensel's Lemma (Theorem 3.10).

**Lemma 4.6.** *$D_{w/v}$ is a closed subgroup of $G_K$. If $\widetilde{w}$ is another prolongation of $v$ to $K^{sep}$, then $D_{\widetilde{w}/v}$ and $D_{w/v}$ are conjugate in $G_K$.*

*Proof.* Given $\sigma \notin D_{w/v}$, take $\alpha \in \mathcal{O}_w$ with $\alpha \notin \sigma(\mathcal{O}_w)$. Let $K \subseteq N \subseteq K^{\mathrm{sep}}$ with $N/K$ finite Galois and $\alpha \in N$. Then, we have $\mathcal{O}_w \cap N \neq \sigma(\mathcal{O}_w) \cap N$. Thus, for any $\tau \in G_K$ with $\tau|_N = \sigma|_N$, we have $\tau \notin D_{w/v}$. Note that the singleton subset $\{\sigma|_N\} \subseteq \mathrm{Gal}(N/K)$ is open. As $G_K$ is equipped with the product topology, the canonical projection $G_K \to \mathrm{Gal}(N/K)$ is continuous. In particular, the preimage

$$A_\sigma := \{\tau \in G_K : \tau|_N = \sigma|_N\}$$

is open in $G_K$. Hence, we have shown that for any $\sigma \notin D_{w/v}$ there is some open $A_\sigma \subseteq G_K$ with $\sigma \in A_\sigma$ and $A_\sigma \cap D_{w/v} = \emptyset$. Thus, $D_{w/v}$ is closed.

By the Conjugation Theorem (Theorem 2.13), we have $\mathcal{O}_{\widetilde{w}} = \sigma(\mathcal{O}_w)$ for some $\sigma \in G_K$, and hence $D_{\widetilde{w}/v} = \sigma \circ D_{w/v} \circ \sigma^{-1}$ holds. □

Using the decomposition group, we can now define the henselization.

**Definition 4.7.** *Define $(K^h, v^h) = (\mathrm{Fix}(D_{w/v}), w|_{\mathrm{Fix}(D_{w/v})})$, and call it the* henselization *of $(K, v)$.*

Note that if $w$ and $\widetilde{w}$ are different prolongations of $v$ to $K^{\text{sep}}$, Lemma 4.6 implies that the corresponding henselizations are isormorphic. Thus, the henselization of a valued field is unique up to isomorphism.

We now show that the henselizsation indeed has the properties which make it the 'smallest henselian extension'.

**Theorem 4.8** (Universal Property of the Henselization)**.** *The henselization $(K^h, v^h)$ of $(K, v)$ has the following characterization:*

*(1) $(K^h, v^h)$ is henselian and*
*(2) if $(L, w)$ is a henselian valued extension of $(K, v)$, then there exists a unique $K$-embedding $i : (K^h, v^h) \hookrightarrow (L, w)$, i.e., $i : K^h \hookrightarrow L$ is an embedding of fields with $i(\mathcal{O}_{v^h}) = \mathcal{O}_w \cap i(K^h)$ and $i|_K = id_K$.*

*Proof.* We first show that $(K^h, v^h)$ satisfies both properties (1) and (2).

(1) By Galois correspondence (Theorem 4.4), we have

$$\text{Gal}(K^{\text{sep}}/K^h) = D_{w/v} = \{\sigma \in G_K : \sigma(\mathcal{O}_w) = \mathcal{O}_w\}.$$

Hence, applying the Conjugation Theorem (Theorem 2.13), we see that $v^h$ extends uniquely to $K^{\text{sep}}$.

(2) Assume that $(L, w) \supseteq (K, v)$ is henselian. Then, by Hensel's Lemma (use condition (4) of Theorem 3.10), the subfield $(K^{\text{alg}} \cap L, w|_{K^{\text{alg}} \cap L})$ is also henselian as it is relatively algebraically closed. Moreover, by Proposition 2.10, $(K^{\text{sep}} \cap L, w|_{K^{\text{sep}} \cap L})$ is again henselian. Thus, we may assume that $L/K$ is a separable algebraic extension.

Let $\widetilde{w}$ (respectively $\widetilde{v}$) be the (by henselianity) unique extension of $w$ (respectively $v^h$) to $K^{\text{sep}}$. As $w$ extends uniquely to $K^{\text{sep}}$, we have that $\text{Gal}(K^{\text{sep}}/L) \subseteq D_{\widetilde{w}/w}$ or, equivalently, $\text{Fix}(D_{\widetilde{w}/w}) \subseteq L$ holds. Note that $\widetilde{w}$ is also a prolongation of $v$ to $K^{\text{sep}}$. Thus, by the infinite version of the Conjugation Theorem (Fact 2.14), there is some $\sigma \in G_K$ with $\sigma(\mathcal{O}_{\widetilde{v}}) = \mathcal{O}_{\widetilde{w}}$ and hence $\sigma(K^h) = \text{Fix}(D_{\widetilde{w}/v})$.

**Claim:** The embedding $\sigma$ is uniquely determined.

*Proof of claim:* Suppose that $\rho : K^h \to L$ is a homomorphism with $\rho|_K = \text{id}_K$ and $\rho(\mathcal{O}_{v^h}) = \mathcal{O}_{\widetilde{w}} \cap \rho(K^h)$. Extend $\rho$ to any $K$-automorphism $\widetilde{\rho}$ of $K^{\text{sep}}$: clearly, there is an extension of $\rho$ to any finite separable extension $M$ of $K^h$. Using Zorn's lemma, there is a maximal homomorphism $\widetilde{\rho}$ extending $\rho$, it is straightforward to check that $\widetilde{\rho}$ is an automorphism of $K^{\text{sep}}$. Then, we have

$$\widetilde{\rho}(\mathcal{O}_{\widetilde{v}}) \cap \widetilde{\rho}(K^h) = \widetilde{\rho}(\mathcal{O}_{\widetilde{v}} \cap K^h) = \widetilde{\rho}(\mathcal{O}_{v^h}) = \mathcal{O}_{\widetilde{w}} \cap \widetilde{\rho}(K^h).$$

As $\widetilde{\rho}(\mathcal{O}_{v^h})$ is a henselian valuation ring on $\widetilde{\rho}(K^h)$, we get $\widetilde{\rho}(\mathcal{O}_{\widetilde{v}}) = \mathcal{O}_{\widetilde{w}}$. Thus, we have $\widetilde{\rho}^{-1} \circ \sigma(\mathcal{O}_{\widetilde{v}}) = \mathcal{O}_{\widetilde{v}}$ and hence $\widetilde{\rho}^{-1} \circ \sigma \in D_{\widetilde{v}/v}$. Therefore, we get $\widetilde{\rho}|_{K^h} = \sigma|_{K^h}$. This proves the claim.

By the claim, $(K^h, v^h)$ satisfies (2) as required.

Finally, if $(K^0, v^0)$ is another extension of $(K, v)$ satisfying (1) and (2), we immediately get embeddings $i_1 : (K^h, v^h) \hookrightarrow (K^0, v^0)$ and $i_2 : (K^0, v^0) \hookrightarrow (K^h, v^h)$ and hence an isomorphism $(K^h, v^h) \cong (K^0, v^0)$. □

As an immediate consequence, we get the following corollaries.

**Corollary 4.9.** *A field $(K, v)$ is henselian if and only if $(K, v) = (K^h, v^h)$.*

**Corollary 4.10.** *For any $K \subseteq L \subseteq K^{sep}$, we have $K^h = \mathrm{Fix}(D_{w/v}) \subseteq L$ if and only if $(L, w|_L)$ is henselian.*

We now show that decomposition groups behave well in towers.

**Proposition 4.11.** *Let $(K, v)$ be a valued field and $\widetilde{v}$ a prolongation of $v$ to some Galois extension $F \subseteq K^{sep}$. For any intermediate field $K \subseteq L \subseteq F$ with $L/K$ Galois and induced valuation ring $\mathcal{O}_w = \mathcal{O}_{\widetilde{v}} \cap L$, the restriction map induces a canonical surjection:*

$$D_{\widetilde{v}/v} = \{\widetilde{\sigma} \in \mathrm{Gal}(F/K) : \widetilde{\sigma}(\mathcal{O}_{\widetilde{v}}) = \mathcal{O}_{\widetilde{v}}\} \longrightarrow D_{w/v} = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\mathcal{O}_w) = \mathcal{O}_w\}$$
$$\widetilde{\sigma} \longmapsto \widetilde{\sigma}|_L$$

*Proof.* We first show that for any $\widetilde{\sigma} \in D_{\widetilde{v}/v}$, its restriction $\sigma := \widetilde{\sigma}_L$ to $L$ is indeed contained in $D_{w/v}$. Note that, as $F/K$ is Galois, we have $\sigma \in \mathrm{Gal}(L/K)$. Moerover, $\mathcal{O}_w = \mathcal{O}_{\widetilde{v}} \cap L$ implies

$$\sigma(\mathcal{O}_w) \subseteq \widetilde{\sigma}(\mathcal{O}_{\widetilde{v}}) \cap \widetilde{\sigma}(L) = \mathcal{O}_{\widetilde{v}} \cap L.$$

Now, using Proposition 2.10, we get $\mathcal{O}_w = \sigma(\mathcal{O}_w)$.

Conversely, take any $\sigma \in D_{w/v}$ and extend it to some $\widetilde{\sigma} \in \mathrm{Gal}(F/K)$. By the Conjugation Theorem (Theorem 2.14), there is some $\tau \in \mathrm{Gal}(F^{\mathrm{sep}}/F) = \mathrm{Gal}(K^{\mathrm{sep}}/F)$ with $\tau(\widetilde{\sigma}(\mathcal{O}_{\widetilde{v}})) = \mathcal{O}_{\widetilde{v}}$. Thus, we have $\tau \circ \widetilde{\sigma} \in D_{\widetilde{v}/v}$ and, as $(\tau \circ \widetilde{\sigma})|_L = \sigma$ holds, $\tau \circ \widetilde{\sigma}$ is indeed in the preimage of $\sigma$. □

Proposition 4.11 gives rise to the notion of a relative henselization, as it implies $\mathrm{Fix}(D_{w/v}) \subseteq \mathrm{Fix}(D_{\widetilde{v}/v})$ for any Galois extension $(K, v) \subseteq (L, w) \subseteq (K^{\mathrm{sep}}, \widetilde{v})$.

**Observation 4.12.** *Let $(K, v) \subseteq (L, w)$ be such that $L/K$ Galois and define $D_{w/v}$ as before. Consider the intermediate field given by*

$$(M, u) := (\mathrm{Fix}(D_{w/v}), w|_{\mathrm{Fix}(D_{w/v})}).$$

*Then, $(M, u)$ is the* relative henselization of $(K, v)$ with respect to $(L, w)$*, i.e., $u$ extends uniquely to $L$ and $(M, u)$ embeds into any intermediate valued field $(K, v) \subseteq (F, \nu) \subseteq (L, w)$ with this property.*

Finally, we show that the henselization of a valued field $(K, v)$ is not only 'small' in the sense that it embeds into any henselian extension, but also has the same value group and residue field as $(K, v)$.

**Theorem 4.13.** *The henselization $(K^h, v^h)$ is an immediate extension of $(K, v)$, i.e., we have $K^h v^h = Kv$ and $v^h K^h = vK$.*

*Proof.* Fix some prolongation $\widetilde{v}$ of $v$ to $K^{\mathrm{sep}}$. By Proposition 4.11, it suffices to show that for any finite Galois extension $K \subseteq N \subseteq K^{\mathrm{sep}}$ with valuation ring $\mathcal{O}_u = \mathcal{O}_{\widetilde{v}} \cap N$, we have that $L := \mathrm{Fix}(D_{u/v})$ with its induced valuation ring $\mathcal{O}_w := \mathcal{O}_u \cap L$ is an immediate extension of $K$. As any element in $K^h$ is contained in some finite Galois extension of $K$, this implies $K^h v^h = Kv$.

We first show $Lw = Kv$. Take any $x \in \mathcal{O}_w^\times$; we want to show that we have $\overline{x} \in Kv$. Let $w = w_1, \ldots, w_r$ be the prolongations of $v$ to $L$. Note that we may assume $r > 1$: Otherwise, $(K, v)$ is already relatively henselian in $(N, u)$, so we have $L = K$ and trivially $\overline{x} \in Kv$.

Consider the subring of $L$ given by $R := \bigcap_{i=1}^{r} O_{w_i}$. By the Weak Approximation Theorem (Theorem 2.12), we can choose some $y \in R$ with $y \in (x+\mathfrak{m}_{w_1}) \cap \bigcap_{i=2}^{r} \mathfrak{m}_{w_i}$. Let $y, \sigma_1(y), \ldots, \sigma_s(y)$ be the distinct conjugates of $y$ over $K$ in $N$. Since we have chosen $y \in L = \mathrm{Fix}(D_{w/v})$, we get $\sigma_1, \ldots, \sigma_s \notin D_{w/v}$. This implies for every $1 \leq j \leq s$ that $\sigma_j^{-1}(\mathfrak{m}_w) = \mathfrak{m}_{w_i}$ holds for some $i \neq 1$. We conclude $\sigma_j(y) \in \mathfrak{m}_w$ for every $1 \leq j \leq s$. Thus, we can write

$$\overline{x} = \overline{y + \sigma_1(y) + \ldots + \sigma_s(y)}.$$

But the sum of the conjugates of $y$ over $K$ (i.e., the right hand side without the bar) is a coefficient in the minimum polynomial of $y$ over $K$, and hence its residue is in $Kv$. Thus, we have $\overline{x} \in Kv$ and hence $Lw = Kv$.

We now show that we have $wL = vK$. Choose any $x \in L$; we want to show that $w(x) \in vK$ holds. Once more, let $w = w_1, \ldots, w_r$ denote the prolongations of $v$ to $L$, we may assume $r > 1$ as before. Using the Weak Approximation Theorem (Theorem 2.12) once more, we can choose $y \in (1 + \mathfrak{m}_w) \cap \bigcap_{i=2}^{r} \mathfrak{m}_{w_2}$. Then, there is some $n \in \mathbb{N}$ such that we have

$$w(xy^n) = w(x) \neq w_i(xy^n)$$

for $i \geq 2$ (note that for every $i \geq 2$, $w(x) = w_i(xy^n)$ holds for at most one $n \in \mathbb{N}$). Let $xy^n, \sigma_1(xy^n), \ldots, \sigma_s(xy^n)$ be the dictinct conjugates of $xy^n$ over $K$.

As once more $\sigma_j \notin D_{w/v}$ holds for $1 \leq j \leq s$, we have $\sigma_j(xy^n) \in \mathfrak{m}_{w_1}$ as before. Consider the minimal polynomial $f$ of $xy^n$ over $K$ given by

$$f(X) = \prod_{j=0}^{s} X - \sigma_j(xy^n) = X^{s+1} + c_s X^s + \ldots + c_0$$

(setting $\sigma_0 = \mathrm{id}$). Then, $xy^n$ is the unique zero of $f$ with $w(xy^n) = w_1(x)$. Without loss of generality, the $\sigma_j$'s are ordered such that

$$w(\sigma_j(xy^n)) < w(x) \text{ for } 1 \leq j \leq k$$

and

$$w(\sigma_j(xy^n)) > w(x) \text{ for } j > k$$

holds; we cannot have equality of these valuations since $j = 0$ is the unique element with equality. Note that for each $j \geq 0$, if we set $l = s - j + 1$, we have

$$c_j = \pm \sum_{0 \leq j_1 < \ldots < j_l \leq r} \sigma_{j_1}(xy^n) \ldots \sigma_{j_l}(xy^n).$$

Now, by the choice of $k$, we have

$$w(c_{s-k+1}) = w\left( \sum_{0 \leq j_1 < \ldots < j_k \leq r} \sigma_{j_1}(xy^n) \ldots \sigma_{j_k}(xy^n) \right) = w\left( \prod_{j=1}^{k} \sigma_j(xy^n) \right) \in vK$$

and

$$w(c_{s-k}) = w\left( \prod_{j=0}^{k} \sigma_j(xy^n) \right) \in vK$$

and hence

$$w(xy^n) = w(c_{s-k+1}/c_{s-k}) = w(c_{s-k+1}) - w(c_{s-k}) \in vK.$$

Thus, we get $w(x) = w(xy^n) \in vK$, so $wL = vK$. □

Overall, we have shown that any valued field $(K, v)$ admits a henselization $(K^h, v^h)$ (which is unique up to isomorphism): this is an immediate and separably algebraic extension which embeds into any henselian extenion of $(K, v)$.

## References

[EP05] Antonio Engler and Alexander Prestel. *Valued Fields*. Springer Monographs in Mathematics. Springer, 2005.

[FJ08] Michael D. Fried and Moshe Jarden. *Field Arithmetic*. Ergebnisse der Mathematik III 11. 3rd edition, revised by M. Jarden. Springer, 2008.

[RZ00] Luis Ribes and Pavel Zalesskii. *Profinite Groups*. Springer, 2000.

Institut für Mathematische Logik und Grundlagenforschung, University of Münster, Einsteinstr. 62, 48149 Münster, Germany

*E-mail address*: franziska.jahnke@wwu.de