A SHORT INTRODUCTION TO VALUED FIELDS

MARTIN WEIMANN AND JOAQUIM ROÉ

Contents

Introduction

Absolute values of a field - like the p-adic absolute value on $\mathbb{Q}$ - played an important role in the development of number theory in the beginning of the 20th century. In the 1930's, Krull generalized the notion of an absolute value to that of a valuation with values in an arbitrary ordered abelian group, generalizing the value group $\mathbb{Z}$ of the usual p-adic valuation on $\mathbb{Q}$. This generalization made possible new applications in other branches of mathematics, such as algebraic or arithmetic geometry, in particular the celebrated problem of resolution of singularities.

These notes intend to give a short introduction to valued fields focusing on the first steps towards the main problem of valuation theory : given a field extension L/K and a valuation v of K, describe all possible extensions of v to L. We mainly follow the book *Valued Fields* by Engler and Prestel, and some lecture notes of Franziska Jahnke. We warmly thank the authors.

1. Valuations

1.1. **Ordered abelian groups.** An ordered abelian group $(\Gamma, +, \leq)$ is an abelian group $(\Gamma, +)$ endowed with a total order $\leq$ which satisfies : for all $a, b, c \in \Gamma$,

$$a \leq b \implies a + c \leq b + c.$$

If $a \neq 0$, we have either

$$0 < a < 2a < 3a < \cdots \qquad \text{or} \qquad \cdots < 3a < 2a < a < 0$$

from which it follows that a non trivial ordered abelian group Γ is infinite and torsion free.

We say that Γ is *discrete* if it admits a minimal positive element.

A subgroup $\Delta \subset \Gamma$ is *convex* in Γ if for $a \in \Gamma$, we have

$$0 \leq a \leq b \in \Delta \implies a \in \Delta.$$

The *rank* of Γ is the number of proper convex subgroups of Γ.

If Γ and Δ are two ordered abelian groups, the direct product $\Gamma \oplus \Delta$ with the lexicographic order

$$(a, b) < (c, d) \iff a < c \quad \text{or} \quad (a = c \text{ and } b < d)$$

is again an ordered abelian group.

Example 1.1.

(1) *The group $\mathbb{Z} \oplus \mathbb{Z}$ with the lexicographic order $\preceq$ is discrete of rank 2. Namely, it has only two proper convex subgroups $\{0\}$ and $\{0\} \oplus \mathbb{Z}$ and admits $(0, 1)$ as a minimal strictly positive element. Notice that the ordered subgroup $\mathbb{Z} \oplus \{0\}$ is not convex in $\mathbb{Z} \oplus \mathbb{Z}$.*

(2) *The isomorphism $(\mathbb{Z} \oplus \mathbb{Z}, +) \simeq (\mathbb{Z} + \sqrt{2}\mathbb{Z}, +) \subset (\mathbb{R}, +)$ gives another ordering $\leq$ on $\mathbb{Z} \oplus \mathbb{Z}$ which is induced by that of $\mathbb{R}$. The ordered group $(\mathbb{Z} \oplus \mathbb{Z}, \leq)$ is now non-discrete of rank one.*

Rank 1 abelian ordered groups are characterized by the following result:

Proposition 1.2. *An ordered abelian group Γ has rank 1 if and only if it is order-isomorphic to a non-trivial subgroup of $(\mathbb{R}, +)$ with the canonical ordering induced from $\mathbb{R}$.*

1.2. **Valuations and valuation rings.** Given an ordered abelian group Γ, we extend the addition and the order to $\Gamma \cup \{\infty\}$ by setting $a + \infty = a$ and $a < \infty$ for all $a \in \Gamma$.

Definition 1.3. *A* valuation *on a field K is a surjective map $v : K \to \Gamma \cup \{\infty\}$ with Γ an ordered abelian group and such that for all $x, y \in K$,*

(1) $v(x) = \infty \iff x = 0$
(2) $v(xy) = v(x) + v(y)$
(3) $v(x + y) \geq \min(v(x), v(y))$

We say that (K, v) is a valued field *with* value group *Γ. The* rank *of v is the rank of Γ. v is said to be* discrete *if Γ is discrete.*

We deduce immediately the following properties. For all $x, y \in K$:

- $v(1) = 0$
- $v(x) = v(-x)$
- $v(x^{-1}) = -v(x)$
- If $v(x) < v(y)$ then $v(x+y) = v(x)$.

Definition 1.4. *A* valuation ring *of a field K is a subring $\mathcal{O} \subset K$ such that for all $x \in K^*$, one has $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$.*

It follows straightforwardly from the above properties that we can associate to a valuation v on K a valuation ring of K :

Proposition 1.5. *Let (K, v) be a valued field.*

- *The set*
$$\mathcal{O}_v := \{x \in K,\ v(x) \geq 0\}$$
is a valuation ring *of K.*
- *Its group of units is*
$$\mathcal{O}_v^\times = \{x \in K,\ v(x) = 0\}.$$
- *The complementary set*
$$\mathfrak{m}_v := \{x \in K,\ v(x) > 0\}$$
is the unique maximal ideal of $\mathcal{O}_v$. In particular $\mathcal{O}_v$ is a local ring.

The quotient field $k_v := \mathcal{O}_v / \mathfrak{m}_v$ is called the *residue field* of (K, v). Given $x \in \mathcal{O}_v$, we denote by $\overline{x} \in k_v$ its residue class.

Conversely we can associate to any valuation ring of K a valuation on K :

Proposition 1.6. *Let $\mathcal{O} \subset K$ be a valuation ring. Then there exists a valuation v on K such that $\mathcal{O} = \mathcal{O}_v$.*

Proof. Let $\mathcal{O}^\times$ stand for the group of units and consider the quotient group
$$\Gamma := K^\times / \mathcal{O}^\times$$
with the additive law $x\mathcal{O}^\times + y\mathcal{O}^\times := xy\mathcal{O}^\times$. Consider the relation
$$x\mathcal{O}^\times \leq y\mathcal{O}^\times \iff \frac{y}{x} \in \mathcal{O}.$$
Using that $\mathcal{O}$ is a valuation ring, we can check that $(\Gamma, +, \leq)$ is an ordered abelian group. Let us then define $v : K \to \Gamma \cup \{\infty\}$ by
$$v(x) := x\mathcal{O}^\times$$
if $x \in K^\times$ and $v(0) = \infty$. We obviously have $v(xy) = v(x) + v(y)$. Also, if $v(x) \leq v(y)$, then $y/x \in \mathcal{O}$. Thus $(x+y)/x = 1 + y/x \in \mathcal{O}$ from which it follows that $v(x+y) \geq v(x) = \min(v(x), v(y))$. Hence v is defines a valuation on K.

Using that $v(1) = 0$, we get
$$\mathcal{O}_v := \{x \in K, v(x) \geq 0\} = \left\{x \in K, \frac{x}{1} \in \mathcal{O}\right\} = \mathcal{O},$$

as required. □

Corollary 1.7. *Any valuation ring $\mathcal{O}$ is a local ring.*

For a counter-example to the converse assertion, consider $R = K[x,y]_{(x,y)}$. This is a local ring for which neither x/y nor y/x belong to R.

Definition 1.8. *We say that two valuations v and w on a field K are* equivalent *if there exists a ordered isomorphism $\gamma : \Gamma_v \to \Gamma_w$ such that $w = \gamma \circ v$.*

Proposition 1.9. *Two valuations on a field K are equivalent if and only if they have they have same valuation ring.*

Proof. If an ordered isomorphism exists, then obviously $\mathcal{O}_v = \mathcal{O}_w$. Conversely, since $v : K^\times \to \Gamma_v$ is a surjective morphism with kernel $\mathcal{O}_v^\times$, one gets an ordered isomorphism $\gamma_v : K^\times/\mathcal{O}_v^\times \simeq \Gamma_v$ defined by $x\mathcal{O}_v^\times \mapsto v(x)$. We get in the same way $\gamma_w : K^\times/\mathcal{O}_w^\times \simeq \Gamma_w$. As $\mathcal{O}_v = \mathcal{O}_w$ implies $K^\times/\mathcal{O}_v^\times = K^\times/\mathcal{O}_w^\times$, one gets the desired isomorphism $\gamma = \gamma_w \circ \gamma_v^{-1}$. □

With regards to Proposition 1.6 and Proposition 1.9 we may say that there is a one-to-one correspondence between the valuation rings of K and the valuations on K up to equivalence. Note that valuation rings of a field K are also uniquely determined by their maximal ideals :

Lemma 1.10. *Let $\mathcal{O}$ and $\mathcal{O}'$ be two valuation rings of a field K with respective maximal ideals $\mathfrak{m}$ and $\mathfrak{m}'$. Then $\mathcal{O} = \mathcal{O}'$ if and only if $\mathfrak{m} = \mathfrak{m}'$.*

Proof. This follows from the fact that $x \notin \mathcal{O}$ if and only if $x^{-1} \in \mathfrak{m}$. □

1.3. **Classical examples.**

- Any field K admits the *trivial valuation* $v : K \to \{0\} \cup \{\infty\}$. The residue field is $k_v = K$.
- For any prime p, the field $\mathbb{Q}$ admits the p-adic valuation
$$v_p(a/b) = \mathrm{ord}_p(a) - \mathrm{ord}_p(b)$$
where for $a \in \mathbb{Z}$, $\mathrm{ord}_p(a)$ stands for the highest power of p dividing a. It is discrete of rank one, with value group $\mathbb{Z}$. The valuation ring is the local ring $\mathbb{Z}_{(p)}$ and the residue field is
$$\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \simeq \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p.$$
- Consider the rational function field $K = k(t)$ over a field k. Given $p \in k[t]$ irreducible, we may define as above the p-adic valuation v_p on $k(t)$. The residue field is isomorphic to the splitting field $k[t]/pk[t]$ of p, finite extension of k of degree $\deg(p)$. The field $k(t)$ admits also the *degree valuation* v_∞
$$v_\infty(g/h) := \deg(h) - \deg(g).$$
The value group is again $\mathbb{Z}$ and the residue field is k.

- If v is a discrete valuation with $v(\pi)$ minimal, then $\mathfrak{m} = \pi\mathcal{O}$. However $\mathcal{O}$ is Noetherian if and only if $\operatorname{rank} v = 1$ [?]; in that case π is called an *uniformizer* of v.

Proposition 1.11. (1) *Any non trivial valuation on $\mathbb{Q}$ is (equivalent to) a p-adic valuation for some prime $p \in \mathbb{N}$. In other words, the proper valuation rings of $\mathbb{Q}$ are the $\mathbb{Z}_{(p)}$ for p a prime.*

(2) *Any non trivial valuation on $k(t)$ which is trivial on k is either a p-adic valuation for some irreducible $p \in k[t]$ or the degree valuation v_∞.*

Proof. (1) Let v be a valuation on $\mathbb{Q}$ and let $\mathcal{O} = \mathcal{O}_v$. As $v(1) = v(1/1) = 0$, we get $1 \in \mathcal{O}$ and thus $\mathbb{Z} \subset \mathcal{O}$. Since v is non trivial, there exists $p \in \mathbb{N}^\times$ minimal such that $v(p) > 0$ and p must be a prime by minimality. If $p \nmid n$, there exists a Bezout relation $ap + bn = 1$ with $a, b \in \mathbb{Z}$. Since $v(ap) > 0$, this forces $v(bn) = 0$ and so $v(b) = v(n) = 0$. Thus the only non-invertible elements in $\mathcal{O}$ are multiples of p, and $\mathcal{O} = \mathbb{Z}_{(p)}$ as required.

(2) Let v be a non-trivial valuation on $k(t)$ which is trivial on k and let $\mathcal{O} = \mathcal{O}_v$. If $t \in \mathcal{O}$, then $k[t] \subset \mathcal{O}$ and as for point (1), we deduce that v is a p-adic valuation for some prime $p \in k[t]$. If $t \notin \mathcal{O}$, then $v(t) < 0$. Hence $t^{-1} \in \mathfrak{m}$ and $v(t^n) > v(t^m)$ whenever $0 < m < n$. Since v is trivial on k, it follows that

$$v(c_0 + \cdots + c_n t^n) = nv(t)$$

whenever $c_n \neq 0$. Hence $v(a/b) = (\deg(b) - \deg(a))v(t)$, with value group $\Gamma := \mathbb{Z}v(t)$. By sending $v(t)$ to -1, we get an ordered isomorphism $\Gamma \simeq \mathbb{Z}$ from which it follows that v is equivalent to the degree valuation v_∞. □

2. Extension of valuations

We adress the question to know if valuation v on a field K can be extended to a given field extension L of K, that is if there exists a valuation w on L such that $w_{|K} = v$. Let us start by an easy lemma :

Lemma 2.1. *Let $K \subset L$ be a field extension. Let v be a valuation on K and w be a valuation on L. The following statements are equivalent :*

(1) $w_{|K} = v$
(2) $\mathcal{O}_w \cap K = \mathcal{O}_v$.
(3) $\mathfrak{m}_w \cap K = \mathfrak{m}_v$.

Proof. It's clear that $w_{|K}$ is a valuation on K with valuation ring $\mathcal{O}_w \cap K$ and maximal ideal $\mathfrak{m}_w \cap K$. Thus, (1) ⇔ (2) follows from Proposition 1.9 and (2) ⇔ (3) follows from Lemma 1.10. □

With regards to Lemma 2.1, looking for w such that $w_{|K} = v$ amounts to look for valuation rings of L whose restrictions to K are $\mathcal{O}_v$.

2.1. **Chevalley's extension theorem.**

Theorem 2.2 (Chevalley). *Let L be a field, $R \subset L$ a subring, and $\mathfrak{p} \subset R$ a prime ideal of R. Then there is a valuation ring $\mathcal{O}$ of L with $R \subset \mathcal{O}$ and $\mathfrak{m} \cap R = \mathfrak{p}$.*

Proof. Denote by $R_\mathfrak{p}$ the localization of R at $\mathfrak{p}$. This is a local ring with unique maximal ideal $\mathfrak{p}R_\mathfrak{p}$. Consider the set

$$\Sigma = \{(A, I),\ A \subset L\,\text{subring},\ I \subset A \text{ proper ideal},\ R_\mathfrak{p} \subset A,\ \mathfrak{p}R_\mathfrak{p} \subset I\}.$$

This set is non empty as it contains $(R_\mathfrak{p}, \mathfrak{p}R_\mathfrak{p})$ and can be given a partial order by

$$(A, I) < (A', I') \iff A \subset A' \text{ and } I \subset I'.$$

As Σ is closed under chain, it possesses a maximal element $(\mathcal{O}, \mathfrak{m})$ by Zorn's lemma. We have $\mathfrak{p}R_\mathfrak{p} = \mathfrak{m} \cap R_\mathfrak{p}$ (the inclusion $\subset$ by construction and the reverse inclusion since $\mathfrak{p}R_\mathfrak{p}$ is the unique maximal ideal of $R_\mathfrak{p}$) from which it follows that $\mathfrak{p}R = \mathfrak{m} \cap R$ as required.

There remains to show that $\mathcal{O}$ is a valuation ring. 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 pair $(\mathcal{O}_\mathfrak{m}, \mathfrak{m}\mathcal{O}_\mathfrak{m})$ would be an element of Σ strictly bigger that $(\mathcal{O}, \mathfrak{m})$. Hence, $(\mathcal{O}, \mathfrak{m})$ is a local ring. In particular, $\mathcal{O}^\times = \mathcal{O} \setminus \mathfrak{m}$.

If $\mathcal{O}$ is not a valuation ring, there exists $x \in L^\times$ such that $x, x^{-1} \notin \mathcal{O}$. Then $\mathcal{O}$ is a proper subring of $\mathcal{O}[x]$ and $\mathcal{O}[x^{-1}]$. Since $(\mathcal{O}, \mathfrak{m})$ is maximal in Σ, we must have $\mathfrak{m}\mathcal{O}[x] = \mathcal{O}[x]$ and $\mathfrak{m}\mathcal{O}[x^{-1}] = \mathcal{O}[x^{-1}]$. Therefore, there exist $a_0, \ldots, a_n, b_0, \ldots, b_m \in \mathfrak{m}$ such that

$$1 = \sum_{i=0}^{n} a_i x^i \quad \text{and} \quad 1 = \sum_{i=0}^{m} b_i x^{-i} \tag{2.1}$$

with n, m minimal. Suppose that $m \leq n$. As $b_0 \in \mathfrak{m}$, we get that

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

Multiplying by $x^n/(1 - b_0)$, we get

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

where $c_i = b_i/(1 - b_0) \in \mathfrak{m}$. Plugging this into (2.1) gives

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

contradicting the minimality of n. By symmetry, we get also a contradiction if we assume that $n \leq m$. Hence $\mathcal{O}$ is a valuation ring. □

Remark 2.3. *The proof of the above theorem shows that the valuation rings of a field K are precisely the maximal elements in the set of local rings of K partially ordered by dominance : $(A, \mathfrak{m}_A) \leq (B, \mathfrak{m}_B)$ iff $A \subset B$ and $\mathfrak{m}_A = \mathfrak{m}_B \cap A$. In particular, any local ring is dominated by a valuation ring.*

For instance, the local ring $R = \mathbb{C}[x, y]_{(x,y)}$ is not a valuation ring since $a := y/x$ satisfies $a \notin R$ and $a^{-1} \notin R$. We check that

$$\mathcal{O} := \mathbb{C}[x, yx^{-1}]_{(x)} = \mathbb{C}[x, y, yx^{-1}]_{(x,y)} \supset \mathbb{C}[x, y]_{(x,y)}$$

is a valuation ring dominating R (blow-up of the maximal ideal (x, y)).

Corollary 2.4. *Let L/K be a field extension. Any valuation v on K admits at least one extension to the field L.*

Proof. By applying Chevalley's theorem with $R = \mathcal{O}_v$, we get a valuation ring of L (say $\mathcal{O} = \mathcal{O}_w$ by Proposition 1.6) containing $\mathcal{O}_v$ and such that $\mathfrak{m}_w \cap \mathcal{O}_v = \mathfrak{m}_v$. We get $w_{|K} = v$ thanks to Lemma 1.10. □

Terminology. If w extends v from K to L, we say that $(K, v) \subset (L, w)$ is a *valued field extension*. We say that $\mathcal{O}_w$ *lies above* $\mathcal{O}_v$, or *dominates* $\mathcal{O}_v$, or *extends* $\mathcal{O}_v$.

2.2. **Integral closure of a ring.**

Chevalley's theorem admits another important consequence for the integral closure of a ring in a field. Let us first remark :

Proposition 2.5. *Any valuation ring $\mathcal{O}$ of a field K is integrally closed in K.*

Proof. Let $x \in K$ such that $a_0 + \cdots + a_{n-1}x^{n-1} + x^n = 0$ for some $a_i \in \mathcal{O}$. We need to show that $x \in \mathcal{O}$. If $K = \mathcal{O}$ this is obvious. Otherwise, $\mathfrak{m} \neq 0$. Suppose that $x \notin \mathcal{O}$. Then $x^{-1} \in \mathfrak{m}$ and multiplying the original equation by x^{-n}, we get

$$a_0x^{-n} + \cdots + a_{n-1}x^{-1} = -1.$$

The left hand side belongs to $\mathfrak{m}$ while $-1 \in \mathcal{O}^\times$, a contradition. □

Theorem 2.6. *Let $R \subset K$ be a subring of a field K. Then, the integral closure $\overline{R}$ of R in K equals*

$$\overline{R} = \bigcap_{\mathcal{O} \in V} \mathcal{O},$$

where $\mathcal{O}$ ranges over of all valuation rings $\mathcal{O}$ of K containing R and whose maximal ideal $\mathfrak{m}$ is such that $\mathfrak{m} \cap R$ is a maximal ideal of R.

Proof. The inclusion $\overline{R} \subset \bigcap_{\mathcal{O}\in V} \mathcal{O}$ is clear from the above proposition. If now $x \notin \overline{R}$, then $x \notin R[x^{-1}]$. So $x^{-1} \in \mathfrak{m}'$ for some maximal ideal $\mathfrak{m}'$ of $R[x^{-1}]$. By Chevalley's theorem, there exists $(\mathcal{O}, \mathfrak{m})$ a valuation ring of L such that $R[x^{-1}] \subset \mathcal{O}$ and $\mathfrak{m} \cap R[x^{-1}] = \mathfrak{m}'$. This forces $x^{-1} \in \mathfrak{m}$ so $x \notin \mathcal{O}$. There only remains to show that $\mathcal{O} \in V$, *i.e.* that the ideal $\mathfrak{m} \cap R$ if a maximal ideal of R. Since $x^{-1} \in \mathfrak{m}'$, the natural map

$$R \longrightarrow R[x^{-1}]/\mathfrak{m}'$$

is surjective with kernel $\mathfrak{m}' \cap R = \mathfrak{m} \cap R$ (use $\sum c_i(x^{-1})^i + \mathfrak{m}' = c_0 + \mathfrak{m}'$). Hence $R/\mathfrak{m} \cap R \simeq R[x^{-1}]/\mathfrak{m}'$. The later ring being a field, the claim follows. □

Remark 2.7. *This theorem is of particular importance with regards to the resolution of singularities of algebraic varieties : if R is an integral finitely generated k-algebra, then the inclusion $R \subset \bar{R}$ leads to a birational morphism*

$$\bar{X} = \mathrm{Spec}(\bar{R}) \longrightarrow X = \mathrm{Spec}(R)$$

of irreducible k-varieties. We say that $\bar{X}$ is the normalization *of X. An important theorem of Zariski asserts that the normalization resolves the singularities of X in codimension one. In other words, the singular locus of $\bar{X}$ has codimension at least two. In particular, if X is a curve, then $\bar{X} \to X$ is a resolution of singularities (in arbitrary characteristic). After Zariski, the existence of the resolution of singularitites has been proved for arbitrary dimension in characteristic zero by the celebrated theorem of Hironaka, but it remains an open problem in positive characersistic for* $\dim X \geq 4$ *(as well as its "local" version known as the problem of local uniformization). Valuations play an important role in this story.*

Corollary 2.8. *Let L/K be any field extension, and let $\mathcal{O}$ be a valuation ring of K. Denote $\overline{\mathcal{O}}$ the integral closure of $\mathcal{O}$ in L. We have*

$$\overline{\mathcal{O}} = \bigcap \mathcal{O}'$$

where $\mathcal{O}'$ ranges over the set of all valuation rings of L lying above $\mathcal{O}$.

Proof. If $\mathcal{O}'$ is a valuation ring of L containing $\mathcal{O}$, then $\mathcal{O}'$ lies above $\mathcal{O}$ if and only if $\mathfrak{m}' \cap \mathcal{O} = \mathfrak{m}$. The claim thus follows from Theorem 2.6. □

Remark 2.9. *This Corollary is of particular importance in computational number theory as it gives a way to compute a $\mathbb{Z}$-basis of the ring of integers $\mathcal{O}_L$ of a number field $L/\mathbb{Q}$. Very roughly speaking : compute the valuations rings of L lying above $\mathbb{Z}_{(p)}$ for all prime $p \in \mathbb{Z}$ (this task is not trivial only for a finite number of primes) and use a variant of the Chinese Remainder Theorem (see below) to compute the intersection of these valuation rings.*

2.3. **The approximation theorem.** The last result of this section is a very helpful analoguous of the Chinese Remainder Theorem for valuation rings.

Theorem 2.10. *Let $\mathcal{O}_1, \dots, \mathcal{O}_r$ be valuation rings of a field K with maximal ideals $\mathfrak{m}_1, \dots, \mathfrak{m}_r$. If $\mathcal{O}_i \not\subseteq \mathcal{O}_j$ for all $i \neq j$, then the multi-residue map*

$$R := \mathcal{O}_1 \cap \cdots \cap \mathcal{O}_r \ \to \ \mathcal{O}_1/\mathfrak{m}_1 \times \cdots \times \mathcal{O}_r/\mathfrak{m}_r$$

is surjective: given $x_i \in \mathcal{O}_i$ for all i, there exists $x \in R$ with $x - x_i \in \mathfrak{m}_i$ for all i.

Proof. Denote $\mathfrak{p}_i = R \cap \mathfrak{m}_i$. It is a prime ideal of R and we denote by $R_{\mathfrak{p}_i}$ the localisation of R at $\mathfrak{p}_i$.

- **Claim 1.** We have $R_{\mathfrak{p}_i} = \mathcal{O}_i$.

Proof of claim 1. Clearly $R_{\mathfrak{p}_i} \subset \mathcal{O}_i$ since $R \setminus \mathfrak{p}_i \subset \mathcal{O}_i^\times$. Now, take $a \in \mathcal{O}_i$. For all j such that $a \in \mathcal{O}_j$, denote α_j the residue class of a in $k_j = \mathcal{O}_j/\mathfrak{m}_j$. Let p be a prime such that $p > \mathrm{char}(k_j)$ and α_j not a primitive p^{th}-root of unity in k_j for all such j. Define $b = 1 + a + \cdots + a^{p-1}$. Let us show that $b^{-1}, ab^{-1} \in \mathcal{O}_j$ for all j:

○ If $a \in \mathcal{O}_j$ and $\alpha_j = 1$, then $\bar{b} = \bar{p} \neq 0 \in k_j$ so $b \in \mathcal{O}_j^\times$ and $b^{-1}, ab^{-1} \in \mathcal{O}_j$.

○ If $a \in \mathcal{O}_j$ and $\alpha_j \neq 1$, then $\bar{b} = (1-\alpha_j^p)/(1-\alpha_j) \neq 0$ and again $b^{-1}, ab^{-1} \in \mathcal{O}_j$.

○ If $a \notin \mathcal{O}_j$, then $a^{-1} \in \mathfrak{m}_j$ and $c := 1 + a^{-1} + \cdots + a^{-(p-1)} \in \mathcal{O}_j^\times$. From the equality $b^{-1} = a^{-(p-1)}c^{-1}$, we deduce again $b^{-1}, ab^{-1} \in \mathcal{O}_j$.

Finally, it follows that $b^{-1}, ab^{-1} \in R$. As $b \in \mathcal{O}_i$, we have $b^{-1} \notin \mathfrak{m}_i \cap R = \mathfrak{p}_i$ and we get $a = ab^{-1}/b^{-1} \in R_{\mathfrak{p}_i}$ as required.

- **Claim 2.** The prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ are exactly the maximal ideals of R.

Proof of claim 2. Note first that all $\mathfrak{p}_i$'s are maximal ideals of R. Indeed, let $\mathfrak{p}_i \subset \mathfrak{b}$ with $\mathfrak{b} \subset R$ maximal. Since $\mathfrak{m}_i$ is the unique maximal ideal of $\mathcal{O}_i$, we must have $\mathfrak{b} \subset \mathfrak{m}_i$, hence $\mathfrak{b} = R \cap \mathfrak{m}_i = \mathfrak{p}_i$. Now let $\mathfrak{m}$ be a maximal ideal of R and assume for a contradiction that $\mathfrak{m} \neq \mathfrak{p}_i$ for all i. Then for all i, there exists $m_i \in \mathfrak{m}$ and $p_i \in \mathfrak{p}_i$ such that $m_i + p_i = 1$. We get

$$\prod p_i = \prod (1 - m_i) = 1 - m \tag{2.2}$$

for some $m \in \mathfrak{m}$. Now, observe that

$$R^\times = \bigcup \mathcal{O}_i^\times = R \setminus \{\mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_r\}$$

As $\mathfrak{m} \subset R \setminus R^\times$, we get $m \in \mathfrak{p}_i$ for some i. Together with (2.2), this gives $1 \in \mathfrak{p}_i$, a contradiction.

We can now finish the proof of the approximation theorem. Note first that $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$ for all $i \neq j$ since otherwise $\mathcal{O}_j = R_{\mathfrak{p}_j}$ would be contained in $\mathcal{O}_i = R_{\mathfrak{p}_i}$. By maximality, we get $\mathfrak{p}_i + \mathfrak{p}_j = R$ for all $i \neq j$. Thus, the Chinese Remainder Theorem ensures that the map

$$R \ \to \ R/\mathfrak{p}_1 \times \cdots R/\mathfrak{p}_r$$

is surjective. We conclude thanks to the isomorphisms $R/\mathfrak{p}_i \simeq R_{\mathfrak{p}_i}/\mathfrak{p}_i R_{\mathfrak{p}_i} \simeq \mathcal{O}_i/\mathfrak{m}_i$. □

3. The fundamental inequality

Let v be a valuation on a field K and L/K some field extension. We would like to have a control on the number of extensions of v to L.

Recall first that if w extends v from K to L, then $\mathcal{O}_v = \mathcal{O}_w \cap K$ and $\mathfrak{m}_v = \mathfrak{m}_w \cap K$. In particular :

- There is an embedding of residue fields $k_v \subset k_w$.
- There is an embedding of ordered abelian groups $\Gamma_v \subset \Gamma_w$.

Definition 3.1. *Let $(K, v) \subset (L, w)$ be an extension of valued fields. The integer*

$$e = e(w/v) := [\Gamma_w : \Gamma_v]$$

is the ramification index *of the extension. The integer*

$$f = f(w/v) := [k_w : k_v]$$

is the residue degree *or* inertia degree *of the extension. If $e = f = 1$, we say that the extension is immediate.*

We allow e and f to be infinite. Notice that the ramification index and residual degree are multiplicative: if $(K_1, v_1) \subset (K_2, v_2) \subset (K_3, v_3)$ are valued fields extension, then we have

$$e(v_3/v_1) = e(v_3/v_2)e(v_2/v_1) \quad \text{and} \quad f(v_3/v_1) = f(v_3/v_2)f(v_2/v_1).$$

This section is dedicated to give the main lines of the proof of the following result.

Theorem 3.2 (Fundamental inequality)**.** *Let L/K be a finite extension. Any valuation v on K admits a finite number of extensions $w_1, \dots, w_r$ to L and we have*

$$\sum_{i=1}^{r} e(w_i/v)f(w_i/v) \leq [L : K].$$

The proof in the separable discrete rank one case is elementary and will be given in Section 3.3. The inequality in the general case is a deeper result whose proof requires more sophisticated Galois theory. We will only sketch the main steps of the proofs.

Let us first have a look at a simple example which already illustrates various situations.

3.1. An example.

We will compute all extensions w of the p-adic valuation v_p from $\mathbb{Q}$ to the quadratic extension $\mathbb{Q}(\sqrt{2})$. Denote $\alpha = \sqrt{2}$.

• Suppose $p = 2$. Then $w(\alpha^2) = v_2(2) = 1$ which forces $w(\alpha) = 1/2$. For $a, b \in \mathbb{Q}$, this forces

$$w(a + b\alpha) = \min\left(v_3(a), v_3(b) + \frac{1}{2}\right),$$

which determines w uniquely. We get $\Gamma_w = \frac{1}{2}\mathbb{Z}$ and $f(w/v_2) = 1$. Since $w(\alpha) > 0$, one has $\bar{\alpha} = 0$. Thus $k_w = \mathbb{F}_2$ and $e(w/v_2) = 2$.

• Suppose $p = 3$. Then $w(\alpha^2) = v_3(2) = 0$ so that $w(\alpha) = 0$ and $e(w/v_3) = 1$. We have $\bar{\alpha}^2 = \bar{2} \in \mathbb{F}_3$. Since 2 is not a square mod 3, we get $f(w/v_3) = [\mathbb{F}_3[\bar{\alpha}] : \mathbb{F}_3] = 2$. Again, the extension w is unique. For $a, b \in \mathbb{Q}$, it is given by

$$w(a + b\alpha) = \min(v_3(a), v_3(b)).$$

Indeed we have $w(a + b\alpha) \geq \min(w(a), w(b\alpha)) = \min(v_3(a), v_3(b))$. Suppose that strict inequality holds. Then $v_3(a) = v_3(b)$ and

$$w(a + b\alpha) > w(a) \quad \Longrightarrow \quad w\,(1 + c\alpha) > 0$$

where $c := b/a \in \mathcal{O}_{v_3} = \mathbb{Z}_{(3)}$ by assumption. This would lead to $\bar{1} + \bar{c}\bar{\alpha} = 0$, hence $\bar{\alpha} \in \mathbb{F}_3$, a contradiction.

• Suppose $p = 7$. Then again $w(\alpha) = 0$ and $e(w/v_p) = 1$. However, $\bar{\alpha}^2 - \bar{2} = 0$ has now two solutions $\bar{3}, \bar{4} \in \mathbb{F}_7$ leading to two distinct extensions w_1, w_2 of v. Namely, the choice $\bar{\alpha} = \bar{3}$ imposes $w_1(\alpha - 3) > 0$ and $w_1(\alpha - 4) = 0$ from which it follows that

$$w_1(\alpha - 3) = w_1((\alpha - 3)(\alpha - 4)) = w_1(7(\alpha + 2)) = 1 + w_1(\alpha + 2).$$

Since $\alpha + 2 = \alpha - 3 + 5$ and $w_1(\alpha - 3) > w_1(5) = v_7(5) = 0$, we get $w_1(\alpha + 2) = 0$. Hence, $w_1(\alpha - 3) = 1$. For $a, b \in \mathbb{Q}$, we may write $a + b\alpha = a + 3b + b(\alpha - 3)$ and we get finally

$$w_1(a + b\alpha) = \min(v_7(a + 3b), v_7(b) + 1).$$

(we can exclude strict inequality $>$ by a similar argument as above). In the same way, we get

$$w_2(a + b\alpha) = \min(v_7(a + 4b), v_7(b) + 1)$$

Hence there are exactly two extensions of v_7 to $\mathbb{Q}(\alpha)$, and they both satisfy $e(w_i/v_7) = 1$ and $f(w_i/v_7) = 1$. We check moreover that

$$w_1(a - b\alpha) = \min(v_7(a - 3b), v_7(b) + 1) = \min(v_7(a + 4b), v_7(b) + 1) = w_2(a + b\alpha)$$

from which it follows that the valuation rings $\mathcal{O}_{w_1}$ and $\mathcal{O}_{w_2}$ are conjugated under the Galois group of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$.

• For a general $p \neq 2$, the situation will be either analoguous to $p = 3$ (this is when 2 is not a square mod p, that is $2 \neq \pm 1 \mod 8$), or to $p = 7$ (this is when 2 is a square mod p, that is $2 = \pm 1 \mod 8$).

3.2. **The weak inequality.**

Theorem 3.3 (Fundamental inequality - weak form)**.** *Let $(K, v) \subset (L, w)$ be a valued field extension of finite degree. Then*

$$e(w/v)f(w/v) \leq [L : K].$$

Proof. Let $\bar{\alpha}_1, \dots, \bar{\alpha}_f \in k_w$ be k_v-linearly independent and let $w(\pi_1), \dots, w(\pi_e)$ be representatives of distinct cosets of Γ_w/Γ_v. We need to show that the elements $\alpha_i\pi_j \in L$ are K-linearly independent. Suppose on the contrary that there exists $c_{ij} \in K$ not all zero such that

$$z := \sum_{i,j} c_{ij}\alpha_i\pi_j = 0.$$

Note that $w(\alpha_i) = 0$ by hypothesis. Let (I, J) such that $w(c_{IJ}\pi_J) = \min_{i,j} w(c_{ij}\pi_j)$. If $j \neq J$, then $w(c_{IJ}\pi_J) < w(c_{ij}\pi_j)$ since equality would lead to $w(\pi_J) - w(\pi_j) \in \Gamma_v$ contradicting our assumption. Hence, dividing z by $c_{IJ}\pi_J$, we get a sum $\sum_{i,j} u_{ij}\alpha_i$ where $u_{ij} \in \mathfrak{m}_w$ if $j \neq J$ while $u_{iJ} \in \mathcal{O}_w$ and $u_{IJ} \in \mathcal{O}_w^\times$. Reducing modulo $\mathfrak{m}_w$, we get a non trivial relation $\sum_i \bar{u}_{i,J}\bar{\alpha}_i = 0$, a contradiction. □

Corollary 3.4. *Let $(K, v) \subset (L, w)$ be an algebraic extension of valued fields. Then:*

- *k_w is an algebraic extension of k_v.*
- *Γ_w/Γ_v is torsion. In particular* $\mathrm{rk}(\Gamma_v) = \mathrm{rk}(\Gamma_w)$.

Proof. Let $\alpha \in L$ and let $L' = K(\alpha)$ and $w' = w_{|L'}$. As L'/K is finite, Theorem 3.3 ensures that $\bar{\alpha} \in k_{w'}$ is algebraic over k_v and that $\Gamma_{w'}/\Gamma_v$ is finite. Hence, $w'(\alpha) + \Gamma_v$ is torsion. For the rank equality, the group Γ_w/Γ_v being torsion, the map $\Delta \mapsto \Delta \cap \Gamma_v$ is a bijection between the set of convex subgroups of Γ_w and of Γ_v. □

Corollary 3.5. *Suppose that L/K is a purely inseparable extension of fields. Then any valuation on K admits a unique extension to L.*

Proof. Recall that L/K is purely inseparable if $\mathrm{char}(K) = p > 0$ and if for all $x \in L$, there exists some $n \in \mathbb{N}$ such that $x^{p^n} \in K$. Let v be a valuation on K and let w be an extension of v to L (which exists by Corollary 2.4). Since Γ_w/Γ_v is torsion by Corollary 3.4, we have an embedding $\phi : \Gamma_w \hookrightarrow \Gamma_v \otimes_{\mathbb{Z}} \mathbb{Q}$ of torsion-free groups. Let $x \in L$ and $n \in \mathbb{N}$ such that $x^{p^n} \in K$. We get $p^n w(x) = v(x^{p^n}) \in \Gamma_v$ and $\phi(w(x)) = v(x) \otimes 1/p^n$ determines $w(x)$ uniquely. □

3.3. The separable discrete rank one case.

In such a case, we have a stronger result: the fundamental inequality is in fact an equality. The proof is elementary, mainly based on the Approximation Theorem.

Theorem 3.6. *Let $\mathcal{O} \subset K$ be a valuation ring with value group $\Gamma \simeq \mathbb{Z}$ and let L/K a finite separable extension. Then there exists a finite number $\mathcal{O}_1, \ldots, \mathcal{O}_r$ of extensions of $\mathcal{O}$ to L and we have*

$$\sum_{i=1}^{r} e_i f_i = [L : K],$$

where $e_i = e(\mathcal{O}_i/\mathcal{O})$ and $f_i = f(\mathcal{O}_i/\mathcal{O})$.

Proof. Denote $\mathfrak{m}$ the maximal ideal of $\mathcal{O}$ and k its residue field. Let $\mathcal{O}_1, \ldots, \mathcal{O}_r$ be *some* extensions of $\mathcal{O}$, and define in the same way Γ_i, $\mathfrak{m}_i$ and k_i for the valuation ring $\mathcal{O}_i$. As we are in the discrete rank one case, there exists $\pi \in \mathcal{O}$ such that $\mathfrak{m} = \pi\mathcal{O}$. Denote $R = \mathcal{O}_1 \cap \cdots \cap \mathcal{O}_r$.

- **Claim** 1. The ring $\mathcal{O}_i/\pi\mathcal{O}_i$ is a k-vector space of dimension $e_i f_i$.

Proof. Since valuation groups are torsion free, Theorem 3.3 guarantees that $\Gamma_i \simeq \mathbb{Z}$ and Γ_i/Γ is cyclic of order e_i. Thus, there exists $\pi_i \in \mathcal{O}_i$ such that $\mathfrak{m}_i = \pi_i\mathcal{O}_i$. Moreover,

$$\pi_i\mathcal{O}_i \supsetneq \pi_i^2\mathcal{O}_i \supsetneq \cdots \supsetneq \pi_i^{e_i}\mathcal{O}_i = \pi\mathcal{O}_i.$$

For all $1 \leq j < e_i$, we have a group isomorphism

$$\pi_i^j\mathcal{O}_i/\pi_i^{j+1}\mathcal{O}_i \simeq \mathcal{O}_i/\pi_i\mathcal{O}_i = k_i.$$

Hence, $\mathcal{O}_i/\pi\mathcal{O}_i$ is a k_i-vector space of dimension e_i. As $[k_i : k] = f_i$ (which is finite by Theorem 3.3), the claim follows.

- **Claim** 2. We have $R/\pi R \simeq \prod_i \mathcal{O}_i/\pi\mathcal{O}_i$ as k-vector spaces.

Proof. Theorem 2.10 ensures that the multi-residue map $\phi : R \to \prod_i \mathcal{O}_i/\pi\mathcal{O}_i$ is surjective. We have $x \in \ker(\phi)$ if and only if $x \in \pi\mathcal{O}_i$ for all i. This means $\pi^{-1}x \in \mathcal{O}_1 \cap \cdots \cap \mathcal{O}_r = R$, that is $x \in \pi R$. The claim follows.

- **Claim** 3. We have $\dim_k R/\pi R \leq [L : K]$.

Proof. We know that $R/\pi R$ is a k-vector space of dimension $n := \sum e_i f_i$. Let $x_1, \ldots, x_n \in R$ such that $\bar{x}_1, \ldots, \bar{x}_n$ is a k-basis of $R/\pi R$. It's sufficient to show that $x_1, \ldots, x_n$ are K-linearly independent. Suppose on the contrary that $\sum c_i x_i = 0$ with $c_i \in K$ not all zero. Up to multiplying all c_i's by a suitable power of π, we may suppose that $c_i \in \mathcal{O}$ for all i, with moreover $c_i \in \mathcal{O}_i^\times$ for at least one index i. This would lead to a non trivial relation $\sum \bar{c}_i \bar{x}_i = 0$ in $R/\pi R$, a contradiction.

These three claims ensure that $n := \sum_{i=1}^r e_i f_i \leq [L : K]$ (notice that separability assumption has not been used yet). In particular, there exists a finite number of extensions of $\mathcal{O}$ to L. Assume that these extensions are $\mathcal{O}_1, \ldots, \mathcal{O}_r$. Then R is the integral closure of $\mathcal{O}$ in L by Corollary 2.8. As L/K is separable and $\mathcal{O}$ is a principal ideal domain, R is a thus a free $\mathcal{O}$-module of rank $[L : K]$ (see e.g. Zariski-Samuel, Corollary 2 p. 265). As moreover $\mathcal{O}$ is a local ring, Nakayama's Lemma ensures that $x_1, \ldots, x_n$ as defined above is an $\mathcal{O}$-basis of R. Hence, $n = [L : K]$. □

3.4. **Conjugation theorem and Galois extensions.**

The proof of the fundamental inequality for an arbitrary finite extension L/K is much more involved. A key step is to show that if L/K is normal, then two extensions of $\mathcal{O}$ are conjugated.

Theorem 3.7 (Conjugation theorem)**.** *Suppose that L/K is a normal extension of fields, $\mathcal{O}$ is a valuation ring of K and $\mathcal{O}', \mathcal{O}''$ are valuations rings of L lying above $\mathcal{O}$. Then there exists $\sigma \in \mathrm{Aut}(L/K)$ with $\sigma(\mathcal{O}') = \mathcal{O}''$. Moreover :*

- *The corresponding extensions w' and w'' of v to L satisfy $w'' = w' \circ \sigma$*
- *The residue fields $k_{w'}$ and $k_{w''}$ are k_v-isomorphic normal extensions of k_v.*
- *We have equality $e(w'/v) = e(w''/v)$ and $f(w'/v) = f(w''/v)$.*

In particular, if L/K is a finite extension, its normal closure N is a finite extension of K and the Conjugation theorem implies that any valuation v on K admits only a finite number of extensions $w_1, \ldots, w_r$ to L.

We now consider the case of a Galois extension, which is the next key step toward the proof of Theorem 3.2.

Theorem 3.8. *Suppose that L/K is a finite Galois extension and let v be a valuation on K. Then v admits only a finite number of extensions $w_1, \dots, w_r$ to L. All valuations w_i have same $e(w_i/v) = e$ and same $f(w_i/v) = f$. Moreover,*

$$[L : K] = refd$$

where $d = 1$ if $\mathrm{char}(k_v) = 0$ or $\mathrm{char}(k_v) = p > 0$ and $\{0 \leq a \leq v(p)\}$ is finite, or d is some power of p otherwise.

The integer d is called the *defect* of the Galois extension L/K. If $d = 1$, the extension is said to be *defectless*.

Proof. (Main ideas.) Let $\mathcal{O}^* \subset L$ be a fixed extension of $\mathcal{O} = \mathcal{O}_v$ to L. Consider the subgroup

$$G = \{\sigma \in Gal(L/K)\, ,\, \sigma(\mathcal{O}^*) = \mathcal{O}^*\}.$$

Denote $K' \subset L$ the subfield fixed by G and denote $\mathcal{O}' = \mathcal{O}^* \cap K'$. Since L/K' is Galois with Galois group G, then $\mathcal{O}^*$ is the unique extension of $\mathcal{O}'$ to L by the Conjugation theorem. More importantly, it can be shown - and these are the key points, that we will not prove here - that :

(1) $(K', \mathcal{O}')$ is an immediate extension of $(K, \mathcal{O})$.
(2) $[L : K'] = d\, e(L/K')f(L/K')$ with d as in Theorem 3.8.

Theorem 3.8 then follows : we can write

$$Gal(L/K) = \bigcup_{i=1}^{r} \sigma_i G$$

where $r = [K' : K]$ and say $\sigma_1 = \mathrm{id}$. The Conjugation Theorem ensures that the extensions of $\mathcal{O}$ to L are precisely $\sigma_1(\mathcal{O}^*) = \mathcal{O}^*, \dots, \sigma_r(\mathcal{O}^*)$, all with same ramification index $e = e(L/K)$ and same residual degree $f = f(L/K)$. By multiplicativity of the ramification index and by (1), we get

$$e(L/K) = e(L/K')e(K'/K) = e(L/K')$$

and the same relation holds for $f(L/K)$. Using (2), we get finally

$$ref = [K' : K]e(L/K')f(L/K') = [K' : K][L : K']/d = [L : K]/d.$$

□

Remark 3.9. *The proof of point (1) uses mainly the approximation theorem. Point (2) is more tricky as it involves Henselian fields and more sophisticated Galois theory (inertia groups, ramification groups, etc).*

Example 3.10. *The following example intends to illustrate the subtility between the cases $d(w/v) = 1$ and $d(w/v) > 1$.*

- *Let $(K, v) = (\mathbb{F}_p(t), v_t)$ and let $g = x^p - x - t^{-1} \in K[x]$. Denote $\alpha \in \bar{K}$ a root of g and let $L = K(\alpha]$. Let w be some extension of v to L. Then $\alpha^p - \alpha = t^{-1}$ forces $w(\alpha) = -1/p$. Since $\Gamma_v = \mathbb{Z}$, we deduce easily that*

$$w\left(\sum_{i=0}^{p-1} c_i \alpha^i\right) = \min_i \left(v(c_i) - \frac{i}{p}\right), \tag{3.1}$$

so w is unique and $e(w/v)=p$. By Theorem 3.3, we get $f(w/v)=1$ and $[L:K]=p$ (in particular g is irreducible). The defect is $d(w/v)=1$ re is equality $\sum e_i f_i = [L:K]$ as predicted by Theorem 3.2 (separable discrete rank one case).

- *Take the same polynomial g, but now considered with coefficients in the the field of Puiseux series*

$$K = \bigcup_{n\geq 1} \overline{\mathbb{F}}_p((t^{1/n}))$$

(still with $v = v_t$). We claim that g is still irreducible. To see this, we remark that

$$\alpha = t^{-1/p} + t^{-1/p^2} + t^{-1/p^3} + \cdots$$

is a root of g such that $\alpha \notin K$. Moreover, the other roots of g are $\alpha+1, \dots, \alpha+p-1$. Thus, if $h \in K[x]$ is a divisor of g of degree $1 \leq d < p$, then

$$h = x^d - (d\alpha + c)x^{d-1} + \cdots$$

with $c \in K$ and $d \neq 0$. We would get $\alpha \in K$, a contradiction. Thus g is irreducible over K and L/K is Galois of degree p.

We still have $w(\alpha) = -1/p$, but as $\Gamma_v = \mathbb{Q}$ and k_v is algebraically closed, we have now $e(w/v)=1$, $f(w/v)=1$ (Corollary 3.4). Moreover, one can show that there is a unique extension w of v to L (this is not trivial since w is not anymore characterized by (3.1)*). This is an example for which the defect is $d(w/v) = p > 1$.*

3.5. **Proof of the fundamental inequality (sketch).** Let L/K be a finite extension. Let $\mathcal{O}$ be a valuation ring of K and let $\mathcal{O}_1, \dots, \mathcal{O}_r$ be the extensions of $\mathcal{O}$ to L. We want to show that

$$\sum_{i=1}^{r} e(\mathcal{O}_i/\mathcal{O}) f(\mathcal{O}_i/\mathcal{O}) \leq [L:K].$$

Up to replace L by the separable closure of K in L, we may assume L/K separable thanks to Corollary 3.5. Consider then the Galois closure N/K of L/K. Then $\mathcal{O}$ admits say s extensions to N and Theorem 3.8 gives

$$[N:K] = sefd \tag{3.2}$$

with the obvious notations. Let $\mathcal{O}_1, \dots, \mathcal{O}_r$ be the extensions of $\mathcal{O}$ to L and let $\mathcal{O}_{i1}, \dots, \mathcal{O}_{is_i}$ be the extensions of $\mathcal{O}_i$ to N. As N/L is also Galois, they have same ramification index e_i and residue degree f_i and Theorem 3.8 applied in L/N gives

$$[N:L] = s_i e_i f_i d_i \tag{3.3}$$

for all $i = 1, \dots, r$, for some defect d_i associated to the extension of $\mathcal{O}_i$ to N. It can be shown that d_i divides d for all i. Moreover, $s = \sum_{i=1}^{r} s_i$ while $e(\mathcal{O}_i/\mathcal{O}) = e/e_i$ and $f(\mathcal{O}_i/\mathcal{O}) = f/f_i$. Hence, (3.2) and (3.3) lead to

$$[N:K] = [N:L] \sum_{i=1}^{r} e(\mathcal{O}_i/\mathcal{O}) f(\mathcal{O}_i/\mathcal{O}) \frac{d}{d_i}.$$

Dividing both terms by $[N:L]$ and using that $d/d_i \geq 1$, we get the result. □

4. Transcendental extensions

Let us start by considering the simplest case of a purely transcendental extension of degree 1.

4.1. Extension to a rational function field.

Let us describe all possible extensions of a valuation v on a field K to the rational function field $K(t)$. Notice that we already solved the case where v is trivial on K, see Proposition 1.11.

Theorem 4.1. *Let (K, v) be a valued field with value group Γ and consider the rational function field $K(t)$. Let Λ be an ordered abelian group strictly containing Γ and let $a \in K$, $\delta \in \Lambda$. We define*

$$w\left(\sum_{i=0}^{n} c_i(t-a)^i\right) := \min\{v(c_i) + i\delta,\ i = 0, \dots, n\}$$

that we extend to $K(t)$ as $w(g/h) = w(g) - w(h)$. Then w defines a valuation on $K(t)$ with value group $\Gamma + \delta\mathbb{Z} \subset \Lambda$.

Proof. Consider first $f, g \in k[t]$. We easily check that $w(f + g) \geq \min\{w(f), w(g)\}$. Let us prove $w(fg) = w(f) + w(g)$. Write $f = \sum a_i(t-a)^i$ and $g = \sum b_j(t-a)^j$. Thus

$$fg = \sum c_k(t-a)^k, \qquad c_k = \sum_{i+j=k} a_i b_j$$

For $i + j = k$, we have

$$v(a_i b_j) + k\delta = v(a_i) + i\delta + v(a_j) + j\delta \geq w(f) + w(g).$$

Thus $v(c_k) + k\delta \geq w(f) + w(g)$ for all k and we get $w(fg) \geq w(f) + w(g)$. For the opposite inequality, let

$$i_0 = \min\{i \mid v(a_i) + i\delta = w(f)\} \quad \text{and} \quad j_0 = \min\{j \mid v(a_j) + j\delta = w(g)\}$$

and denote $k_0 = i_0 + j_0$. We may write

$$c_{k_0} = a_{i_0} b_{j_0} + \sum_{i+j=k_0,\, i<i_0} a_i b_j + \sum_{i+j=k_0,\, i>i_0} a_i b_j. \tag{4.1}$$

Let i, j be such that $i + j = k_0$.

- If $i < i_0$, we have $v(a_i) + i\delta > w(f)$ by definition of i_0. Since $v(b_j) + j\delta \geq w(g)$, we deduce

$$v(a_i b_j) + k_0\delta = v(a_i) + i\delta + v(b_j) + j\delta > w(f) + w(g). \tag{4.2}$$

- If $i > i_0$ then $j_0 < j$ and (4.2) still holds by symmetry.
- If $i = i_0$, then $j = j_0$ and

$$v(a_{i_0} b_{j_0}) + k_0\delta = v(a_{i_0}) + i_0\delta + v(b_{j_0}) + j_0\delta = w(f) + w(g). \tag{4.3}$$

Combining (4.1), (4.2) and (4.3) we get $v(c_{k_0}) + k_0\delta = w(f) + w(g)$. It follows that $w(fg) \geq w(f) + w(g)$ leading to the desired equality $w(fg) = w(f) + w(g)$ in $K[t]$.

Suppose now $f, g \in K(t)$. Note first that w is well-defined: if $f_1/f_2 = g_1/g_2$, then $f_1 g_2 = f_2 g_1$ so that $w(f_1) - w(g_1) = w(f_2) - w(g_2)$ by what we just proved. By reducing f and g to the same denominator, it's then straightforward to check that the relations $w(f+g) \geq \min\{w(f), w(g)\}$ and $w(fg) = w(f) + w(g)$ still hold in $K(t)$. □

If we let $a = 0$, $\delta = 0$ in the above theorem, then we get the so-called *Gauss valuation* defined on $K[t]$ by

$$w\left(\sum a_i t^i\right) := \min_i \{v(a_i)\}$$

and extended to $K(t)$ by $w(f/g) = w(f) - w(g)$.

Proposition 4.2. *The Gauss valuation is the unique extension of v to $K(t)$ for which $w(t) = 0$ and $\bar{t}$ is transcendental over k_v. It satisfies $\Gamma_w = \Gamma$ and $k_w = k_v(\bar{t})$.*

Proof. Uniqueness : Let $f = \sum a_i t^i$ non-zero. Let $v(a_k) = \min_i v(a_i)$ and write $f = a_k g$ with $g = \sum b_i t^i \in K[t]$, $b_i = a_i/a_k$. As $w(a_i/a_k) \geq 0$ and $w(t) = 0$, we deduce that $w(g) \geq 0$. Moreover, $\bar{g} = \sum \bar{b}_i \bar{t}^i$ is non zero since $\bar{t}$ is transcendental over k_v and $\bar{b}_k = \bar{1} \neq 0$. Thus $g \in \mathcal{O}_w^\times$, that is $w(g) = 0$. We get $w(f) = v(a_k) = \min v(a_i)$, as required.

Existence : Let us show that $w(\sum a_i t^i) := \min_i\{v(a_i)\}$ satisfies the desired properties. We already know that it is a valuation, and equality $w(t) = 0$ and $\Gamma_w = \Gamma$ are clear. To show that $\bar{t} \in k_w$ is transcendental over k_v, consider a relation $\sum \bar{a}_i \bar{t}^i = 0$ for some $a_i \in \mathcal{O}_v$. Then $w(\sum a_i t^i) > 0$ which implies $v(a_i) > 0$ for all i, that is $\bar{a}_i = 0$ as required. There remains to show that $k_w = k_v(\bar{t})$. The inclusion $k_v(\bar{t}) \subset k_w$ is clear. Let $h = f_1/f_2 \in \mathcal{O}_w^\times$, with $f_i \in K[t]$. As above, we may write $f_i = c_i g_i$ for some $c_i \in K^\times$ and $g_i \in \mathcal{O}_w^\times$. Therefore, $h = cg_1/g_2$ with $c = c_1/c_2 \in K^\times$. As h, g_1, g_2 belong to $\mathcal{O}_w^\times$, so does c. It follows that $\bar{h} = \overline{cg_1}/\overline{g_2} \in k_v(\bar{t})$. □

Proposition 4.3. *Let (K, v) be a valued field with value group $\Gamma \subset \Lambda$. If $\delta \in \Lambda \setminus \{0\}$ and $\Gamma \cap \mathbb{Z}\delta = \{0\}$, then there exists a unique extension of v to $K(t)$ which satisfies $w(t) = \delta$. It satisfies $k_w = k_v$ and $\Gamma_w = \Gamma \oplus \mathbb{Z}\delta$ (with the ordering induced by Λ).*

Proof. Existence follows from Theorem 4.1. For uniqueness, let $f = \sum a_i t^i$. Then

$$w(f) = w(\sum a_i t^i) \geq \min\{w(a_i t^i)\} = \min\{v(a_i) + i\delta\}.$$

If equality does not hold, there would exist $i \neq j$ such that $a_i \neq 0$, $a_j \neq 0$ and $v(a_i) + i\delta = v(a_j) + j\delta$, contradicting that $\Gamma \cap \mathbb{Z}\delta = \{0\}$. Obviously, we have $\Gamma_w = \Gamma \oplus \mathbb{Z}\delta$. There remains to show that $k_v = k_w$. Since there is a unique index m such that $w(f) = w(a_m t^m)$, we deduce that $f = a_m t^m (1 + u)$ with $u \in \mathfrak{m}_w$. If $h = f/g \in K(t)$, there thus exists $c \in K^\times$, $r \in \mathbb{Z}$ and $u, u' \in \mathfrak{m}_w$ such that

$$h = ct^r \frac{1+u}{1+u'}.$$

Hence, if $h \in \mathcal{O}_w^\times$, we must have $w(cX^r) = 0$, that is $v(c) + r\delta = 0$. Since $\Gamma \cap \mathbb{Z}\delta = \{0\}$, this forces $v(c) = 0$ and $r = 0$. So $c \in \mathcal{O}_v^\times$. As $\bar{u} = \bar{u'} = 0$, we get $\bar{h} = \bar{c} \in k_v$. □

Example 4.4. *Consider $K = k(s)$ equipped with the s-adic valuation. Let $L = k(s, t)$ with two independent variables s, t. We have an isomorphism $L \simeq K(t)$. Previous results ensure that :*

- *There is a unique valuation w on L trivial on k which satisfies $w(s) = 1$ and $w(t) = \sqrt{2}$. It is defined on $k[s,t]$ by*

$$w(\sum a_{ij}s^it^j) = \min\{i + j\sqrt{2},\ a_{ij} \neq 0\}.$$

The value group is $\mathbb{Z} + \sqrt{2}\mathbb{Z} \subset (\mathbb{R}, +)$ and w is non-discrete of rank 1. The residue field is k.

- *There is a unique valuation w on L with value group $\mathbb{Z}^2_{lex}$ such that $w(s) = (1,0)$ and $w(t) = (0,1)$. It is defined on $k[s,t]$ by*

$$w(\sum a_{ij}s^it^j) = \min\{(i,j),\ a_{ij} \neq 0\}.$$

The residue field is again k, but v is now discrete of rank 2.

Notice that we could have provided similar examples by considering $L = \mathbb{Q}(t)$ with $\mathbb{Q}$ equipped with the p-adic valuation. Such a valuation would have residue field $\mathbb{F}_p$.

4.2. **The dimension inequality.** Let us now consider a field extension L/K of arbitrary transcendental degree.

Theorem 4.5. *Let $(K,v) \subset (L,w)$ be a valued field extension. Let $\bar{x}_1, \dots, \bar{x}_r \in k_w$ be algebraically independent over k_v and let $w(y_1), \dots, w(y_s) \in \Gamma_w$ with $\mathbb{Z}$-linearly independent classes in Γ_w/Γ_v. Then $x_1, \dots, x_r, y_1, \dots, y_s \in L$ are algebraically independent over K. Moreover, the restriction v' of w to $K(x_1, \dots, x_r, y_1, \dots, y_s)$ has residue field and value group*

$$k_{v'} = k_v(\bar{x}_1, \dots, \bar{x}_r) \qquad \text{and} \qquad \Gamma_{v'} = \Gamma_v \oplus w(y_1)\mathbb{Z} \oplus \cdots w(y_s)\mathbb{Z}.$$

Proof. (sketch) The case $r+s = 1$ is a consequence of Corollary 3.4 for the first point, together with Proposition 5.2 and 5.3 for the second point. Then, the proof proceeds by induction on $r+s$. □

Definition 4.6. *The* rational rank *of an abelian group Γ is the dimension of the $\mathbb{Q}$-vector space $\overline{\Gamma} := \Gamma \otimes_{\mathbb{Z}} \mathbb{Q}$. We denote it by* $\mathrm{rr}(\Gamma)$.

In other words, $\mathrm{rr}(\Gamma)$ is the maximal number (possibly infinite) of elements of Γ which are $\mathbb{Z}$-linearly independent. If $\Delta \subset \Gamma$ is a subgroup of an ordered abelian group Γ, then one can show by induction

$$\mathrm{rk}(\Gamma) \leq \mathrm{rk}(\Delta) + \mathrm{rr}(\Gamma/\Delta).$$

In particular, considering $\Delta = \{0\}$, we get the inequality $\mathrm{rk}(\Gamma) \leq \mathrm{rr}(\Gamma)$. For instance, $\Gamma = \mathbb{Z} + \sqrt{2}$ has rank 1 and rational rank 2.

By combining Theorem 4.5 together with Corollary 3.4, we get the following result :

Corollary 4.7 (Dimension inequality – Abhyankar). *Let $(K,v) \subset (L,w)$ be an extension of valued fields. Then,*

$$\mathrm{tr.deg}(k_w/k_v) + \mathrm{rr}(\Gamma_w/\Gamma_v) \leq \mathrm{tr.deg}(L/K)$$

Corollary 4.8. *Let L/K be a field extension and let $\mathcal{O}$ be a valuation ring of K. If there exists extensions $\mathcal{O}_1 \subsetneq \cdots \subsetneq \mathcal{O}_n$ of $\mathcal{O}$ to L, then tr.deg$(L/K) \geq n-1$.*

Proof. We have $\mathcal{O} = \mathcal{O}_v$ and $\mathcal{O}_1 = \mathcal{O}_w$ for some valuations v of K and w of L. Let $y_i \in \mathcal{O}_i \setminus \mathcal{O}_{i-1}$ for all $i = 2, \ldots, n$. By the previous corollary, it's sufficient to show that $w(y_2), \ldots, w(y_n)$ generate $\mathbb{Z}$-linearly independent cosets in Γ_w/Γ_v. Suppose on the contrary that there exist $c_i \in \mathbb{Z}$ not all zero and $a \in K^\times$ such that

$$c_2 w(y_2) + \cdots + c_n w(y_n) = w(a).$$

Thus $b = a^{-1} y_2^{c_2} \cdots y_n^{c_n} \in \mathcal{O}_1^\times \subset \mathcal{O}_n^\times$. Since $y_i \notin \mathcal{O}_{i-1}$, we get $y_i^{-1} \in \mathcal{O}_{i-1} \subset \mathcal{O}_i$ so that $y_i \in \mathcal{O}_i^\times \subset \mathcal{O}_n^\times$ for all i. Hence $a = b^{-1} y_2^{c_2} \cdots y_n^{c_n} \in \mathcal{O}_n^\times$. Since $a \in K$, we deduce that $a \in \mathcal{O}^\times$. Let m be the maximal index such that c_m is non zero. Then $y_m^{c_m} = bay_2^{-c_2} \cdots y_{m-1}^{-c_{m-1}} \in \mathcal{O}_{m-1}^\times$. Since $\mathcal{O}_{m-1}$ is integrally closed, this forces $y_m \in \mathcal{O}_{m-1}$, a contradiction.

□

5. Topology and completion

The main reference for this section is [10, Sections 2.3 and 2.4]

5.1. **Topology induced by a valuation.** To any valuation $v : K \to \Gamma \cup \{\infty\}$ with $\Gamma \subset \mathbb{R}$ (i.e., of rank 1) one may associate a non archimedean absolute value $|\cdot|_v : K \to \mathbb{R}$ defined by $|x|_v = \exp(-v(x))$.

Theorem 5.1. *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 $(\hat{K}_0, i_0)$ is another such pair, then there exists a unique continuous isomorphism $\varphi : \hat{K} \to \hat{K}_0$ preserving $|\cdot|$ such that $i_0 = i \circ \varphi$.*

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

Proof. The existence of a completion and the density of $i(K)$ in $\hat{K}$ can be proved by the standard constructive method of taking Cauchy sequences modulo the ideal of sequences converging to zero. Uniqueness is easily proved by topological arguments using the density of $i(K)$. □

Example 5.2 (Completions of $\mathbb{Q}$)**.** *The field $\mathbb{Q}$ admits a single archimedean absolute value (up to equivalence) namely the usual one: $|x| = \max\{x, -x\}$ (see* [10, 1.2]*). Of course, its completion with respect to the archimedean absolute value is $\mathbb{R}$.*

All other absolute values on $\mathbb{Q}$ are non-archimedean and derive from p-adic valuations where $p \in \mathbb{Z}$ is a prime. The completion of $\mathbb{Q}$ with respect to $|x|_p = \exp(-v_p(x))$ is called $\mathbb{Q}_p$. An element x of $\mathbb{Q}_p$ can be written uniquely as a convergent series

$$z = \sum_{i \geq m} a_i p^i = \lim_{n \to \infty} \sum_{i=m}^{n} a_i p^i$$

where $m \in v_p(z) \in \mathbb{Z}$, and $a_i \in \{0, 1, \ldots, p-1\}$ with $a_m \neq 0$.

Example 5.3 (Completions with respect to a discrete valuation)**.** *More generally, if v is a discrete valuation of rank 1, and π is a uniformizer, then every element $z \in \hat{K}^\times$*

can be written uniquely as a convergent series

$$z = \sum_{i \geq m} a_i \pi^i = \lim_{n \to \infty} \sum_{i=m}^{n} a_i \pi^i$$

where $m = v(x)$, $a_m \neq 0$, and all coefficients a_i are taken from a set $R \subseteq \mathcal{O}_v$ of representatives of the residue classes in the field k_v.

The p-adic valuation of $\mathbb{Q}$ is a particular case of this; another example is given by the t-adic valuation on $k(t)$ where k is some field, $v_t(f) = \mathrm{ord}_t(f)$, with uniformizer t. Then the completion $\widehat{k(t)}$ is (isomorphic to) the field $k((t))$ of Laurent power series of the form

$$f = \sum_{i \geq m} a_i t^i$$

where $m \in v_t(f) \in \mathbb{Z}$, and $a_i \in k$.

In many aspects, in particular for local-to-global problems, the absolute value $|\cdot|_{v_\infty}$ on $k(t)$ attached to the valuation $-\deg$ plays an analoguous role to the archimedean absolute value on $\mathbb{Q}$.

Valuations of rank higher than 1, which do not define absolute values, can be used nevertheless to define a topology. Let $v : K \to \Gamma \cup \{\infty\}$ be an arbitrary valuation, and define, for each $\gamma \in \Gamma$ and each $x \in K$,

$$\mathcal{U}_\gamma(x) = \{y \in K | v(y - x) > \gamma\}.$$

The family of sets $\mathcal{U}_\gamma(x)$ for all γ and all x form the basis of a topology and the sets $\mathcal{U}_\gamma(x)$ for x fixed are then a basis of neighborhoods of x (called *open balls* centered at x) [10, Section 2.3]. Once a topology is given one may perform completions much in the same way as for absolute values.

Example 5.4. *Fix a prime $p \in \mathbb{Z}$ and consider the following rank 2 valuation on $K = \mathbb{Q}(t)$. For $f \in K \subset \mathbb{Q}((t))$ write $f = \sum a_i t^i$ and let $v(f) = (v_t(f), v_p(a_{v_t(f)})) \in \mathbb{Z}^2_{lex}$. It is not hard to see that v is indeed a valuation.*

A sequence f_n in K converges to 0 with respect to v if and only if for every $(a, b) \in \mathbb{Z}^2$ there exists n_0 such that $v(f_n) >_{lex} (a, b)$ for all $n > n_0$. This is equivalent to the statement that for every $a \in \mathbb{Z}$ there exists n_0 such that $v_t(f_n) > a$ for all $n > n_0$. So the topologies induced by v and by v_t are equal; the following section deals with this issue in general.

5.2. **Dependent or composite valuations.**

Definition 5.5. *Two valuations v_1, v_2 on a field K are* dependent *if their valuation rings $\mathcal{O}_{v_1}$, $\mathcal{O}_{v_2}$ are contained in a common proper subring of K, i.e., if $\mathcal{O}_{v_1}\mathcal{O}_{v_2} \neq K$. v_2 is called a* coarsening *of v_1 if $\mathcal{O}_{v_1} \subset \mathcal{O}_{v_2}$.*

Theorem 5.6. *Given a valuation v on a field K, let $O(v)$ be the set of overrings of $\mathcal{O}_v$, i.e.,*

$$O(v) = \{\mathcal{O}' \subseteq K \text{ subring} \mid \mathcal{O}_v \subseteq \mathcal{O}' \subseteq K\}.$$

Then:

1. *Every $\mathcal{O}' \in O(v)$ is a valuation ring with maximal ideal $\mathfrak{m}' \subseteq \mathfrak{m}_v$ and $\mathfrak{m}'$ is prime in $\mathcal{O}_v$.*

2. *The map $O(v) \to \operatorname{Spec} \mathcal{O}_v$ given by $\mathcal{O}' \mapsto \mathfrak{m}'$ is an order-reversing bijection, with inverse map given by localization $\mathfrak{m}' \mapsto (\mathcal{O}_v)_{\mathfrak{m}'}$.*
3. *Both $O(v)$ and $\operatorname{Spec} \mathcal{O}_v$ are totally ordered sets, in bijection with the set of convex subgroups of $v(K^\times)$.*

Proof. (1) Since

$$x \notin \mathcal{O}' \implies x \notin \mathcal{O}_v \iff x^{-1} \in \mathfrak{m} \subset \mathcal{O}',$$

$\mathcal{O}'$ is a valuation ring, and therefore

$$x \in \mathfrak{m}' \iff x^{-1} \notin \mathcal{O}' \implies x^{-1} \notin \mathcal{O}_v \iff x \in \mathfrak{m}_v.$$

The fact that $\mathfrak{m}'$ is prime in $\mathcal{O}_v$ also follows from $x \in \mathfrak{m}' \Leftrightarrow x^{-1} \notin \mathcal{O}'$.

(2) That the map is order-reversing is clear, and that localization at any prime $\mathfrak{m}'$ of $\mathcal{O}_v$ gives an overring whose maximal ideal is $\mathfrak{m}'$ is clear too. Using the property $x \in \mathfrak{m}' \Leftrightarrow x^{-1} \notin \mathcal{O}'$ again it is clear that $\mathcal{O}' = (\mathcal{O}_v)_{\mathfrak{m}'}$ is *the only* overring with maximal ideal $\mathfrak{m}'$, and bijectivity follows.

(3) The value group of every $\mathcal{O}' \in O(v)$ is by 1.6 equal to $K^\times/\mathcal{O}'^\times$, which is a quotient of $K^\times/\mathcal{O}_v^\times$. The kernel of this quotient is the convex subgroup that corresponds to $\mathcal{O}'$ by this bijection. Conversely, if Δ is a convex subgroup of $v(K^\times)$, the corresponding prime ideal is

$$\mathfrak{p}_\Delta = \{x \in K\,,\ v(x) > \delta,\ \forall\ \delta \in \Delta\}.$$

Since convex subgroups are totally ordered by inclusion, and all involved bijections preserve ordering, $O(v)$ and $\operatorname{Spec} \mathcal{O}_v$ are also totally ordered sets.

□

Note then that a valuation ring has rank 1 if and only if it is maximal, i.e. has no non-trivial overrings. In particular, any distinct valuation rings $\mathcal{O}_1$ and $\mathcal{O}_2$ of rank 1 are necessarily independent.

Whereas the value group of the larger valuation ring is a quotient by the corresponding convex subgroup, the convex subgroup itself corresponds to a valuation on its residue field. One says that v is *composite* with these two valuations.

Corollary 5.7. Dependence *of valuations is an equivalence relation.*

Proof. If v_1, v_2 are dependent and v_2, v_3 are dependent, then $\mathcal{O}_{v_1}\mathcal{O}_{v_2} \neq K$ and $\mathcal{O}_{v_2}\mathcal{O}_{v_3} \neq K$ are overrings of $\mathcal{O}_{v_2}$, so one must be included in the other, say $\mathcal{O}_{v_1}\mathcal{O}_{v_2} \subseteq \mathcal{O}_{v_2}\mathcal{O}_{v_3} \neq K$. But then $\mathcal{O}_{v_1}$ and $\mathcal{O}_{v_3}$ are contained in a common proper subring of K, namely $\mathcal{O}_{v_2}\mathcal{O}_{v_3}$.

□

Theorem 5.8. *Two nontrivial valuations are* dependent *if and only if they define the same topology on K.*

Proof. If $\mathcal{O}_{v'}$ is an overring of $\mathcal{O}_v$ then the value group of v' is a quotient $\Gamma_{v'} = \Gamma_v/\Delta$, and for every $x \in K$, $v'(x) = v(x) + \Delta \in \Gamma_v/\Delta$. Then, the key point is that for every $\gamma \in \Gamma$ there exist $\gamma' \in \Gamma$ such that $\gamma' + \Delta > \gamma + \Delta$, because this guarantees an inclusion of open balls $\mathcal{U}'_{\gamma'+\Delta}(a) \subset \mathcal{U}_\gamma(a)$ and also $\mathcal{U}_{\gamma'}(a) \subset \mathcal{U}'_{\gamma'+\Delta}(a)$. So the two bases of neighborhoods are cofinal.

For the converse, if the topologies induced by v and v' are equivalent one considers the ring $\mathcal{O} = \{x/y | x \in \mathcal{O}_{v_1}, y \in \mathcal{O}_{v_1} \setminus \mathfrak{m}_{v_2}\}$, which is easily seen to contain $\mathcal{O}_v$ and

$\mathcal{O}_{v'}$. Using the equivalence of the topologies, it follows that there exists $a \in K^\times$ such that $a\mathfrak{m}_v \subset \mathfrak{m}_{v'}$, which can be used to show that $\mathcal{O}$ is a proper subring of K. □

6. Henselian fields

6.1. **Hensel's lemma for complete valued fields.**

Theorem 6.1. *Let (K, v) be complete valued field with* $\operatorname{rank}(v) = 1$. *Given $a \in \mathcal{O}_v$ and $f \in \mathcal{O}_v[t]$ such that $v(f(a)) > 2v(f'(a))$ holds, there is some $b \in \mathcal{O}_v$ such that $f(b) = 0$ and $v(b - a) > v(f'(a))$.*

The idea is that if $f(a)$ is 'close' to zero then $f(a - f(a)/f'(a))$ is even closer.

Proof. (Sketch) First one remarks that for every polynomial $f(x) \in \mathcal{O}_v[t]$ there exists $g(t, \delta) \in \mathcal{O}_v[t, \delta]$ such that $f(t + \delta) = f(t) + f'(t)\delta + \delta^2 g(t, \delta)$. This is a simple computation which does not require either rank 1 or completeness.

Then one applies Newton's method.

Let $\varepsilon = v(f(a)) - 2v(f'(a))$, which is positive by hypothesis, and define $a_1 = a - f(a)/f'(a)$, noting that $f(a)/f'(a) \in \mathfrak{m}_v$. The remark we just made shows then that

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

for some $d \in \mathcal{O}_v$. This gives $v(f(a_1)) \geq 2v(f'(a)) + 2\varepsilon$ and $v(f'(a_1)) = v(f'(a))$. Then one proceeds iteratively defining $a_{n+1} = a_n - f(a_n)/f'(a_n)$, which is a Cauchy sequence because $v(a_{n+1} - a_n) \geq v(f'(a)) + (n + 1)\varepsilon$. Therefore $b = \lim a_n$ exists in K, and since the value of $f(a_n)$ grows indefinitely, the limit is a root of f. □

6.2. **The Henselian property.**

We saw before that the topology induced by a valuation depends only on its rank-1 coarsening, so the property of (K, v) being complete also depends only on the rank-1 coarsening of v. It turns out that the *conclusion* in Hensel's lemma is a more fundamental property, and more suitable for the study of valuations of rank greater than 1, than the *completeness hypothesis*.

Theorem 6.2 (Hensel's Lemma). *For a valued field (K, v), the following are equivalent:*

1. For all $f \in \mathcal{O}_v[t]$, $a \in \mathcal{O}_v$ with $v(f(a)) > 2v(f'(a))$, there exists some $b \in \mathcal{O}_v$ satisfying $f(b) = 0$ and $v(a - b) > v(f'(a))$.
2. Simple roots lift: For each $f \in \mathcal{O}_v[t]$ and $a \in \mathcal{O}_v$ with $\overline{f}(\overline{a}) = 0$ and $\overline{f'}(\overline{a}) \neq 0$ in the residue field, there exists some $b \in \mathcal{O}_v$ such that $f(b) = 0$ and $\overline{b} = \overline{a}$ holds.
3. Every polynomial of the form $t^n + t^{n-1} + a_{n-2}t^{n-2} + \cdots + a_0$ with $a_i \in \mathfrak{m}_v$ for $0 \leq i \leq n - 2$ has a zero in K.
4. v extends uniquely to every finite (algebraic) extension of K.

Definition 6.3. (K, v) *is called* Henselian *if it satisfies one (and hence any) of the properties of Hensel's lemma*

In order to prove Hensel's lemma in all generality, the following version of Gauss's Lemma will be useful:

Lemma 6.4. *Let (K, v) be any valued field and $f \in \mathcal{O}_v[t]$. Then there exitst $h_1, \dots, h_n \in \mathcal{O}_v[t]$ irreducible in $K[t]$ with*

$$f = h_1 \dots h_n.$$

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

$$\tilde{v}\left(\sum a_i t^i\right) = \min\{v(a_i)\}.$$

Let a be the coefficient of f of minimal valuation, so that $\tilde{v}(f) = v(a)$ and similarly let b_i be the coefficient of g_i of minimal valuation. Then $g_i/b_i \in \mathcal{O}_v[t]$ has null Gauss valuation, and one checks that $h_1 = ag_1/b_1$, $h_i = g_i/b_i$ for $i \geq 2$ gives a factorization of f as desired. □

Proof of Theorem 6.2. (1)⇒(2)**:** If $\overline{f}(\overline{a}) = 0$ and $\overline{f'}(\overline{a}) \neq 0$ then $v(f(a)) > 0 = 2v(f'(a))$, so by (1), there exists some $b \in \mathcal{O}_v$ satisfying $f(b) = 0$ and $v(a-b) > 0$, therefore (2) holds.

(2)⇒(3)**:** If $f = t^n + t^{n-1} + a_{n-2}t^{n-2} + \dots + a_0$ with $a_i \in \mathfrak{m}_v$, then $\overline{f}(t) = t^{n-1}(t+1)$ has the simple root -1, which by (2) means that f has a root in K.

(3)⇒(4)**, Sketch:** Suppose there is a Galois extension N/K such that v has more than one extension to N. Fix one of the extensions, w, and let $G = \{\sigma \in \mathrm{Gal}(N/K) | \sigma(\mathcal{O}_w) = \mathcal{O}_w\}$. By Theorem 3.7, G is a proper subgroup of the Galois group; let $L \subset N$ be the fixed field of G, and let $\mathcal{O}_1 = \mathcal{O}_w, \mathcal{O}_2, \dots, \mathcal{O}_n$ be the conjugates of $\mathcal{O}_1$ in N.

The idea is then to prove for any element $\beta \in \bigcap \mathcal{O}_i \cap L$ with $\beta - 1$ in the maximal ideal of $\mathcal{O}_1$ and β in the maximal ideal of $\mathcal{O}_i$ for all $i > 1$ (which exist by Weak Approximation), the minimal polynomial of β is of the form given in (3).

□

Example 6.5. *A complete field of rank greater than 1 need not be Henselian.*

Consider the field $L = k(s, t)$ equipped with the $\mathbb{Z}^2_{lex}$-valuation w from example 4.4 with $w(s) = (1, 0)$ and $w(t) = (0, 1)$. Its residue field is k and its completion is $\hat{L} = k(t)((s))$.

Let $f(x) = x^2 - (1 + t)$. 1 is obviously a root of $\bar{f}(x) = x^2 - 1$ over the residue field. However we claim that 1 cannot be lifted to a root in $\hat{L}$. To see this it is enough to show that $w(a^2 - (1 + t)) < (1, 0)$ for every $a \in L$, or equivalently, that $v_s(a^2 - (1 + t)) \leq 0$ for every $a \in L$, which is clear if $v_x(a) \neq 0$, and follows from the fact that $1 + t$ is not a square in $k(t)$ when $v_x(a) = 0$.-

References

[1] S.S. Abhyankar, Coverings of algebraic curves, Amer. J. Math. **79** (1957), 825–856.

[2] S.S. Abhyankar, Irreducibility criterion for germs of analytic functions of two complex variables, Adv. Math. **35** (1989), 190–257.

[3] S.S. Abhyankar, T. Moh, Newton-Puiseux Expansion and Generalized Tschirnhausen Transformation, J. Reine Angew. Math. **260** (1973), 47–83.

[4] M. Alberich-Carramiñana, J. Guàrdia, E. Nart, J. Roé, Valuative trees of valued fields, J. Algebra **614** (2023), 71–114.

[5] M. dos Santos Barnabé, J. Novacoski, Valuations on $K[x]$ approaching a fixed irreducible polynomial, J. Algebra **592** (2022), 100–117.

[6] J.-D. Bauch, Computation of integral bases, J. Number Theory **165** (2016), 382—407.

[7] J.-D. Bauch, E. Nart, H. Stainsby, Complexity of the OM factorizations of polynomials over local fields, LMS J. of Comp. and Math. **16** (2013), 139–171.

[8] D. Duval, Rational Puiseux expansions, Compositio Math. **70** (1989), no.2, 119–154.

[9] O. Endler, Valuation Theory, Universitex, Springer-Verlag, Berlin Heidelberg, 1972.

[10] A. J. Engler, A. Prestel, *Valued fields*, Springer, Berlin, 2005.

[11] J.v.z. Gathen, G. Jürgen, Modern Computer Algebra, Cambridge University Press, 2013.

[12] A. Jakhar, S. K. Khanduja, N. Sangwan, On factorization of polynomials in Henselian valued fields, Comm. Alg. **46-7** (2018), 3205–3221.

[13] J. Guàrdia, J. Montes, E. Nart, Okutsu invariants and Newton polygons, Acta Arith. **145** (2010), 83–108.

[14] J. Guàrdia, J. Montes, E. Nart, Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields, J. Théor. Nombres Bordeaux **23** (2011), no. 3, 667–696.

[15] J. Guàrdia, J. Montes, E. Nart, Newton polygons of higher order in algebraic number theory, Trans. Amer. Math. Soc. **364** (2012), no. 1, 361–416.

[16] J. Guàrdia, J. Montes, E. Nart, A new computational approach to ideal theory in number fields, Found. Comput. Math. **13** (2013), 729–762.

[17] J. Guàrdia, J. Montes, E. Nart, Higher Newton polygons and integral bases, J. Number Theory **147** (2015), 549-–589.

[18] J. Guàrdia, E. Nart, Genetics of polynomials over local fields, in *Arithmetic, geometry, and coding theory*, Contemp. Math. vol. 637 (2015), 207-241.

[19] F.J. Herrera Govantes, M.A. Olalla Acosta, M. Spivakovsky, Valuations in algebraic field extensions, J. Algebra **312** (2007), no. 2, 1033–1074.

[20] F.J. Herrera Govantes, W. Mahboub, M.A. Olalla Acosta, M. Spivakovsky, Key polynomials for simple extensions of valued fields, J. Singul. **25** (2022), 197–267.

[21] F.-V. Kuhlmann, Value groups, residue fields, and bad places of rational function fields, Trans. Amer. Math. Soc. **356** (2004), no. 11, 4559–4660.

[22] J. Mac Donald, Fiber polytopes and fractional power series, J. of Pure and App. Alg. **104** (1995), no. 2, 213–233.

[23] S. Mac Lane, A construction for absolute values in polynomial rings, Trans. Amer. Math. Soc. **40** (1936), 363–395.

[24] S. Mac Lane, A construction for prime ideals as absolute values of an algebraic field, Duke Math. J. **2** (1936), 492–510.

[25] J. Montes, Polígonos de Newton de orden superior y aplicaciones aritméticas, PhD Thesis, Universitat de Barcelona, 1999.

[26] N. Moraes de Oliveira, E. Nart, Defectless polynomials over Henselian fields and inductive valuations, J. Algebra, **541** (2020), 270–307.

[27] N. Moraes de Oliveira, E. Nart, Computation of residual polynomial operators of inductive valuations, J. Pure Appl. Algebra **225-9** (2021), 106668.

[28] E. Nart, Key polynomials over valued fields, Publ. Mat. **64** (2020), 195–232.

[29] E. Nart, Mac Lane-Vaquié chains of valuations on a polynomial ring, Pacific J. Math. **311-1** (2021), 165–195.

[30] E. Nart, Rigidity of valuative trees under Henselization, Pacific J. Math. **319** (2022), 189–211.

[31] E. Nart, J. Novacoski, The defect formula, Adv. Math. **428** (2023), 109153.

[32] J. Neukirch, Algebraische Zahlentheorie, Springer-Verlag Berlin Heidelberg 1992.

[33] J. Novacoski, On Mac Lane–Vaquié key polynomials, J. Pure Appl. Algebra **225** (2021), 106644.

[34] J. Novacoski and M. Spivakovsky, Reduction of local uniformization to the rank one case, Valuation Theory in Interaction, EMS Series of Congress Reports, Eur. Math. Soc. (2014) 404–431.

[35] J. Novacoski, M. Spivakovsky, On the local uniformization problem, Banach Center Publ. **108** (2016), 231–238.

[36] K. Okutsu, Construction of integral basis I, II, Proc. Japan Acad. Ser. A **58** (1982), 47–49, 87–89.

[37] Ø. Ore, Zur Theorie der algebraischen Körper, Acta Math. **44** (1923), 219–314.

[38] Ø. Ore, Newtonsche Polygone in der Theorie der algebraischen Körper, Math. Ann. **99** (1928), 84–117.

[39] P. Popescu-Pampu, Approximate roots, Fields Inst. Comm. **33** (2002), 1–37.

[40] A. Poteaux and M. Weimann, Computing Puiseux series : a fast divide and conquer algorithm, Ann. Henri Leb. **4** (2021), 1061–1102.

[41] A. Poteaux, M. Weimann, A quasi-linear irreducibility test in $\mathbb{K}[[x]][y]$, Comput. Complexity **31** (2022), no. 6, 1–52.

[42] A. Poteaux, M. Weimann, Local polynomial factorisation: improving the Montes algorithm, Proceedings of the 2022 ACM on International Symposium on Symbolic and Algebraic Computation ISSAC'22 (2022), 149–158.

[43] H. D. Stainsby, Triangular bases of integral closures, J. Symb. Comp. **87** (2018) 140–175.

[44] M. Vaquié, Famille admisse associée à une valuation de $K[x]$, Singularités Franco-Japonaises, Séminaires et Congrés 10, SMF, Paris (2005), Actes du colloque franco-japonais, juillet 2002, édité par Jean-Paul Brasselet et Tatsuo Suwa, 391–428.

[45] M. Vaquié, Extension d'une valuation, Trans. Amer. Math. Soc. **359** (2007), no. 7, 3439–3481.

[46] M. Vaquié, Famille essential de valuations et défaut d'une extension, J. Algebra **311** (2007), no. 2, 859–876.

LMNO, UMR 6139, Université de Caen-Normandie, F-14032 Caen, France
Email address: `martin.weimann@unicaen.fr`

Departament de Matemàtiques, Universitat Autònoma de Barcelona, Edifici C, E-08193 Bellaterra, Barcelona, Catalonia
Email address: `jroe@mat.uab.cat`