ON THE GENERAL THEORY OF VALUATIONS AND CLASS FIELD THEORY (DRAFT VERSION)

A Dissertation Submitted
in Partial Fulfilment of the Requirements
for the Degree of

MASTER OF SCIENCE (BY RESEARCH)

in

MATHEMATICS

by

Daksh Dheer
(Roll No. 23050)

to

SCHOOL OF MATHEMATICS
INDIAN INSTITUTE OF SCIENCE EDUCATION AND RESEARCH
THIRUVANANTHAPURAM - 695551, INDIA

DECLARATION

I, **Daksh Dheer (Roll No: 23050)**, hereby declare that, this report entitled **"On the General Theory of Valuations and Class Field Theory"** submitted to Indian Institute of Science Education and Research Thiruvananthapuram towards the partial requirement of **Master of Science** in **Mathematics**, is an original work carried out by me under the supervision of **Prof Viji Z. Thomas** and has not formed the basis for the award of any degree or diploma, in this or any other institution or university. I have sincerely tried to uphold academic ethics and honesty. Whenever a piece of external information or statement or result is used then, that has been duly acknowledged and cited.

Thiruvananthapuram - 695551 **Daksh Dheer**

CERTIFICATE

This is to certify that the work contained in this project report entitled **"On the General Theory of Valuations and Class Field Theory"** submitted by **Daksh Dheer** (**Roll No: IPHD23050**) to the Indian Institute of Science Education and Research, Thiruvananthapuram towards the partial requirement of **Master of Science (Research)** in **Mathematics** has been carried out by him under my supervision and that it has not been submitted elsewhere for the award of any degree.

Thiruvananthapuram - 695551 | Prof. Viji Z. Thomas

ACKNOWLEDGEMENT

I thank everyone who has assisted me in seeing this project through to its completion.

I would like to express my deepest gratitude to my supervisor Prof. Viji Thomas for his constant support and guidance throughout the last two years. His insightful feedback and rigorous approach have consistently challenged me to improve, particularly his meticulous attention to detail in proofs, which has taught me the skillful art of writing mathematics.

I also wish to express my sincere appreciation to all the members of the School of Mathematics at IISER Thiruvananthapuram, especially my MSc and IPhD batchmates, for cultivating a stimulating and supportive academic environment, and for the depth of knowledge and guidance shared during my coursework and interactions. I am also deeply grateful to all my friends who have continued to support me, especially Shakshi, who has been my harshest critic as well as my strongest supporter in all matters academic or otherwise.

I would also like to acknowledge the covert privileges afforded to me by my caste, gender, and religion, which have granted me access to exclusive spaces, opportunities, and other forms of support.

Lastly, I am grateful to my family for their unwavering support; this project could never have been made possible without them. My parents without whom I would have never pursued my passion, as well as my brother Lakshay and my sister-in-law Ananya, who have always been guiding lights and pillars of support in my life.

Thiruvananthapuram - 695551 **Daksh Dheer**
December 01, 2025

ABSTRACT

Name of the student: **Daksh Dheer** Roll No: **23050**
Degree: **M.S. (by Research)** Department: **School of Mathematics**
Thesis title: *On the General Theory of Valuations and Class Field Theory*
Thesis supervisor: **Prof. Viji Thomas** Date of thesis submission: ________

In this thesis, we independently develop the theory of valuations in more generality than is traditionally required for algebraic number theory. We begin by defining absolute values (which can be seen as valuations of rank one) before introducing valuations proper and discussing their properties such as the equivalence between valuations and valuation rings. After this, we construct some valuations and move on to discuss their topology – this notion closely relates to dependence of valuations and we make this precise. In the same section, we also show the correspondence among overrings, primes and a class of convex groups, and conclude by proving a general approximation theorem. The remainder of the chapter deals with extensions of valuations and results concering them.

The second half of the thesis will deal with developing abstract class field theory, followed by local class field theory, including the general reciprocity law and generalized cyclotomic theory.

Contents

Contents **vi**

1 Valuation Theory **1**

1.1 Absolute Values 1
1.2 General Valuations 23
1.3 Constructing valuations 30
1.4 Dependence and Topology of Valuations 34
1.5 Extensions of Valuations 42

2 Class Field Theory **58**

2.1 Local Fields 58

Chapter 1

Valuation Theory

We base this report mainly on the first three chapters of [**EP2005**], with a few excursions into [**Neukirch1999**]. In this chapter, we prove theorems in the theory of valuations in more generality than required in standard algebraic number theory.

In accordance with the views of Alfréd Rényi, we denote the completion of a proof with .

1.1 Absolute Values

Definition 1.1.1. Let K be a field. An ***absolute value*** on K is a map

$$|\cdot| : K \longrightarrow \mathbb{R}$$

satisfying, for all $x, y \in K$:

1. $|x| > 0$ for all $x \neq 0$, and $|0| = 0$,
2. $|xy| = |x||y|$,
3. $|x + y| \leq |x| + |y|$.

Note that from the above axioms, we have $|1|^2 = |1^2| = |1|$, giving $|1| = 1$. Similarly, $|-1|^2 = |(-1)(-1)| = |1| = 1$ implies $|-1| = 1$, whence it follows that $|-x| = |x|$ for all $x \in K$. Since $|\cdot|$ is a homomorphism on $K^\times$, it follows that $|x^{-1}| = |x|^{-1}$ for $x \neq 0$.

Proposition 1.1.1. *The set $S = \{|n \cdot 1| : n \in \mathbb{Z}\}$ is bounded if and only if $|\cdot|$ satisfies the ultrametric triangle inequality: $|x+y| \leq \max\{|x|, |y|\}$ for all $x, y \in K$.*

Proof. If $|\cdot|$ satisfies the ultrametric triangle inequality, then for any element $|m \cdot 1| \in S$, we have $|m \cdot 1| = |1 + 1 + \cdots + 1| \leq \max\{|1|, \ldots, |1|\} = 1$.
Conversely, if S is bounded by some constant M, then we have, for any $n \in \mathbb{Z}$

$$|x+y|^n = |(x+y)^n| = \left|\sum_{\nu=0}^{n} \binom{n}{\nu} x^\nu y^{n-\nu}\right| \leq \sum_{\nu=0}^{n} \left|\binom{n}{\nu}\right| |x|^\nu |y|^{n-\nu} \leq M(n+1) \cdot \max\{|x|, |y|\}^n$$

since $|x|^\nu |y|^{n-\nu} \leq \max\{|x|, |y|\}^n$ and $\left|\binom{n}{\nu}\right| \leq M$. Therefore, on taking n-th roots, we get $|x + y| \leq M^{1/n}(n + 1)^{1/n} \cdot \max\{|x|, |y|\}$ and thus, as $n \to \infty$, we conclude $|x + y| \leq \max\{|x|, |y|\}$.

Definition 1.1.2. An absolute value satisfying the ultrametric triangle inequality $|x + y| \leq \max\{|x|, |y|\}$ for all $x, y \in K$ is said to be ***non-Archimedean***. If not, it is said to be ***Archimedean***.

Remark 1. The usual absolute value on $\mathbb{R}$, denoted by $|\cdot|_0$ is Archimedean.

We next consider some important non-Archimedean absolute values.

Example 1.1. For every rational prime p, define the p-adic absolute value $|\cdot|_p$ on $\mathbb{Q}$ by setting $|0|_p := 0$ and $\left|p^\nu \dfrac{m}{n}\right|_p := \dfrac{1}{e^\nu}$, where $m, n \in \mathbb{Z} \setminus \{0\}$ are not divisible by p. Here, $S = \{|n \cdot 1| : n \in \mathbb{Z}\} = \{e^{-\nu} : \nu \in \mathbb{N}\}$.

Example 1.2. Let k be a field and $q \in k[x]$ be an irreducible polynomial. We define $|\cdot|_q$ on the rational function field $k(x)$ as $|0|_q := 0$ and $\left|q^\nu \dfrac{f}{g}\right|_q := \dfrac{1}{e^\nu}$, where $f, g \in k[x] \setminus \{0\}$ are not divisible by q. This is known as the q-adic absolute value on $k[x]$.

An absolute value $|\cdot|$ on K defines a metric as $d(x, y) = |x - y|$, for all $x, y \in K$ and thus induces a topology on K.

Definition 1.1.3. Two absolute values are ***dependent*** if they induce the same topology on K. If not, they are ***independent***.

Proposition 1.1.2. *Let $|\cdot|_1$ and $|\cdot|_2$ be two nontrivial absolute values on K. The following are equivalent:*

1. *$|\cdot|_1$ and $|\cdot|_2$ are dependent.*
2. *$|x|_1 < 1$ implies $|x|_2 < 1$.*
3. *There exists $s > 0$ such that $|x|_1 = (|x|_2)^s$ for all $x \in K$.*

Proof. (1) $\implies$ (2): Suppose $|\cdot|_1$ and $|\cdot|_2$ are dependent, i.e., they induce the same topology on K. Let $x \in K$ be such that $|x|_1 < 1$, i.e., $x \in B_1(0,1)$ — the open unit ball around 0 in the topology induced by $|\cdot|_1$. By hypothesis, there exists $\varepsilon > 0$ such that $B_1(0,\varepsilon) \subset B_2(0,1)$. Since $|x|_1 < 1$, we may choose some positive integer $m \geq 1$ such that $|x^m|_1 = (|x|_1)^m < \varepsilon$, whence $x^m \in B_1(0,\varepsilon) \subset B_2(0,1)$. Thus, $|x^m|_2 = (|x|_2)^m < 1$ and so $|x|_2 < 1$, since m is a positive integer.

(2) $\implies$ (3): Suppose $|x|_1 < 1$ implies $|x|_2 < 1$. Let $y \in K$ be a fixed element satisfying $|y|_1 > 1$. Let $x \in K, x \neq 0$. Then, $\exists \alpha \in \mathbb{R}$ such that $|x|_1 = |y|_1^\alpha$. Let m_i/n_i be a rational sequence converging to α from above; assume that $n_i > 0$. Now, $|x|_1 = |y|_1^\alpha < |y|_1^{m_i/n_i}$, and so $\left|\dfrac{x^{n_i}}{y^{m_i}}\right|_1 < 1$. By hypothesis, we get $\left|\dfrac{x^{n_i}}{y^{m_i}}\right|_2 < 1$, whence $|x|_2 \leq |y|_2^{m_i/n_i}$, and therefore $|x|_2 \leq |y|_2^\alpha$. We now use a rational sequence m_i/n_i converging to α from below and proceed similarly to obtain $|x|_2 \geq |y|_2^\alpha$. Thus, we have $|x|_2 = |y|_2^\alpha$. Moreover, we started with $|x|_1 = |y|_1^\alpha$.

Using these two equations, we get, for all nonzero $x \in K$,

$$\alpha = \frac{\log|x|_1}{\log|y|_1} = \frac{\log|x|_2}{\log|y|_2} \implies \frac{\log|x|_1}{\log|x|_2} = \frac{\log|y|_1}{\log|y|_2} =: s,$$

hence, $|x|_1 = |x|_2^s$ and $|y|_1 > 1 \implies |y|_2 > 1$, i.e., $s > 0$.

(3) $\implies$ (1): Suppose $\exists s > 0$ such that $|x|_1 = (|x|_2)^s$ for all $x \in K$.

It suffices to show that every open ball in the topology induced by $|x|_1$ is contained in an open ball in the topology induced by $|x|_2$, and vice versa. Consider $B_1(\alpha, r) = \{x \in K : |x-\alpha|_1 < r\}$. For any $x \in B_1(\alpha, r)$, we have, by hypothesis, $(|x-\alpha|_2)^s < r$, i.e., $|x-\alpha|_2 < r^{1/s}$, i.e., $x \in B_2(\alpha, r^{1/s})$.

Hence, $B_1(\alpha, r) \subset B_2(\alpha, r^{1/s})$. Analogously, it follows that $B_2(\alpha, r) \subset B_1(\alpha, r^s)$ and thus the topologies are the same. ☕

Lemma 1.1.1. $|\cdot|$ *is a uniformly continuous map from K, with the topology given by $|\cdot|$, to $\mathbb{R}$ with the usual topology defined by $|\cdot|_0$*

Proof. We have $|x| = |x-y+y| \leq |x-y|+|y|$. Thus, $|x|-|y| \leq |x-y|$. Exchanging x and y, and using $|y-x| = |x-y|$, it follows that $||x|-|y||_0 \leq |x-y|$, where $|\cdot|_0$ is again the usual absolute value on the real numbers. ☕

The following theorem is an analogue of the Chinese Remainder Theorem in the case of absolute values.

Theorem 1.1.1 (Artin-Whaples Approximation)**.** *Let $|\cdot|_1, |\cdot|_2, \ldots, |\cdot|_n$ be pairwise-independent nontrivial absolute values on a field K. Let $x_1, x_2, \ldots, x_n \in K$ and $\varepsilon > 0$ be given. Then, there exists $x \in K$ such that $|x - x_i|_i < \varepsilon$ for all i.*

Proof. We will prove this in three steps.

Step 1. We shall prove that for every $1 \leq i \leq n$ there exists $a_i \in K$ such that $|a_i|_i > 1$ and $|a_i|_j < 1$ for all $j \neq i$. We show it for $i = 1$ and write $a = a_1$. The argument for every other i follows by replacing 1 with i.

We induct on n: for $n = 2$, the hypothesis states that $|\cdot|_1$ and $|\cdot|_2$ are independent. Hence, we use the earlier proposition to conclude that there exist $b, c \in K$ such that $|b|_1 < 1$ and $|b|_2 \geq 1$, $|c|_1 \geq 1$ and $|c|_2 < 1$. Now, take $a = b^{-1}c$, then $|a|_1 = |b^{-1}c|_1 = |b^{-1}|_1|c|_1 > 1$ since $|b|_1 < 1$ and $|c|_1 \geq 1$.

Similarly, $|a|_2 = |b^{-1}c|_2 = |b^{-1}|_2|c|_2 < 1$ since $|b|_2 \geq 1$ and $|c|_2 < 1$. Hence, the claim is true for $n = 2$.

Induction hypothesis: $\exists y \in K$ such that $|y|_1 > 1$ and $|y|_j < 1$ for all $j = 2, \ldots, n-1$.

Applying the $n = 2$ case to $|\cdot|_1$ and $|\cdot|_n$, we get $|z|_1 > 1$ and $|z|_n < 1$ for some $z \in K$. Therefore, if $|y|_n \leq 1$, then $|zy^\nu|_1 > 1$ and $|zy^\nu|_n < 1$ for every integer $\nu \geq 1$. Now, we choose an integer $\nu \geq 1$ such that $|zy^\nu|_j < 1$; this exists because $|y|_j < 1$ for all $j = 2, \ldots, n-1$. For example, we may take any $\nu < \min\limits_{2 \leq j \leq n-1} \left(\dfrac{-\log|z|_j}{\log|y|_j} \right)$. setting $a = zy^\nu$. We have $|a|_1 = |zy^\nu|_1 > 1$ and $|a|_j = |zy^\nu|_j < 1$ for all $j \neq 1$. Hence we are done, under the assumption that $|y|_n \leq 1$.

Suppose now that $|y|_n > 1$. Consider the sequence $w_\nu = \dfrac{y^\nu}{1 + y^\nu}, \nu \in \mathbb{N}.$.

We then have

$$\lim_{\nu \to \infty} |w_\nu|_j = \lim_{\nu \to \infty} \frac{|y^\nu|_j}{|1 + y^\nu|_j} = 0 \text{ for } j = 2, \ldots, n-1,$$

because $|y|_j < 1 \implies |y|_j^\nu < 1$ and $1 + |y^\nu|_j > |1 + y^\nu|_j > 1 - |y^\nu|_j$, i.e., the denominator is bounded by 1 (by aplying the Sandwich theorem) meanwhile the numerator tends to zero.

Similarly,

$$\lim_{\nu \to \infty} |w_\nu - 1|_j = \lim_{\nu \to \infty} \left| \frac{y^\nu}{1 + y^\nu} - 1 \right|_j = \lim_{\nu \to \infty} \left| \frac{1}{1 + y^\nu} \right|_j \geq \lim_{\nu \to \infty} \frac{1}{1 - |y^\nu|_j} = 0 \text{ for } j = 1 \text{ and } n,$$

since $|y|_n > 1$ and $|y|_1 > 1$. Hence,

$$\lim_{\nu \to \infty} |w_\nu|_j = 0 \text{ for } j = 2, \ldots, n-1,$$

and

$$\lim_{\nu \to \infty} |w_\nu - 1|_j = 0 \text{ i.e., } \lim_{\nu \to \infty} |w_\nu|_j = 1 \text{ for } j = 1, n$$

As a result,

$$\lim_{\nu\to\infty}|zw_\nu|_j = |z|_j \lim_{\nu\to\infty}|w_\nu|_j = 0 \text{ for } j = 2,\dots,n-1,$$

and

$$\lim_{\nu\to\infty}|zw_\nu|_j = |z|_j \lim_{\nu\to\infty}|w_\nu|_j = |z|_j \text{ for } j = 1, n.$$

Hence, for sufficiently large ν, $a = zw_\nu$ is a valid choice since $|a|_1 = |zw_\nu|_1 = |z|_1|w_\nu|_1 > 1$, as $\lim_{\nu\to\infty}|zw_\nu|_1 = |z|_1 > 1$, and $|a|_j = |zw_\nu|_j < 1$, as $\lim_{\nu\to\infty}|zw_\nu|_n = |z|_n < 1$, for all $j \neq 1$.

Step 2. Now we show that for any real $\varepsilon > 0$ and every $1 \leq i \leq n$, there exists $c_i \in K$ with $|c_i - 1|_i < \varepsilon$ and $|c_i|_j < \varepsilon$ for all $j \neq i$. We again only consider the case $i = 1$ in detail. Let $a \in K$ be as in Step 1. Then the sequence $\left|\frac{a^\nu}{1+a^\nu}\right|_j$ converges to 1 for $j = 1$, and converges to 0 if $j > 1$. This follows by observing that $|a^\nu|_1 > 1$ and $|a^\nu|_j < 1$ for $j > 1$; we then apply the same argument as for w_v above. Thus, for sufficiently large ν, $c_1 = \frac{a^\nu}{1+a^\nu}$ has the required property.

Step 3. Proceeding inductively with step 2, there exist elements $c_1, \dots, c_n \in K$ such that c_i is close to 1 at $|\cdot|_i$, and for every $j \neq i$, c_i is close to 0 at $|\cdot|_j$. The element $x = c_1x_1 + \cdots + c_nx_n$ is then arbitrarily close to x_i at $|\cdot|_i$ for every $i = 1, \dots, n$, since

$$|x|_i = |c_1x_1 + \cdots + c_nx_n|_i \leq |c_1|_i|x_1|_i + \dots |c_n|_i|x_n|_i \longrightarrow |c_i|_i|x_i|_i \longrightarrow |x_i|_i$$

This proves the theorem.

Definition 1.1.4. A sequence $(x_n)_{n\in\mathbb{N}} \subset K$ is ***Cauchy*** if for every $\varepsilon > 0, \exists N \in \mathbb{N}$ such that $|x_n - x_m| < \varepsilon$ for all $n, m \geq N$.

K is called ***complete*** if every Cauchy sequence converges in K.

Note that K is always complete with respect to the trivial absolute value.

Lemma 1.1.2. *Let X be a metric space and $Y \subseteq X$ be a dense subset. Assume every Cauchy sequence in Y converges to a point in X. Then, X is complete.*

Proof. Let $(a_n)_n$ be a Cauchy sequence in X. Since Y is dense, $B(a_n, \varepsilon) \cap Y \neq \emptyset$, $\forall\varepsilon > 0$. Pick $y_n \in B(a_n, \varepsilon) \cap Y$, for each n.Then, $|y_n - a_n| < \varepsilon$ and so $|y_n - y_m| \leq |y_n - a_n| + |a_n - y_m| < 2\varepsilon$, i.e., $(y_n)_n$ is also Cauchy. Since $(y_n)_n \subseteq Y$, we have $y_n \to x \in X$, by hypothesis. Hence, given $\varepsilon > 0$, $|y_n - x| < \varepsilon$, $\forall n \geq M$.

Consider $|a_n - x| \leq |a_n - y_n| + |y_n - x| < 2\varepsilon$, $\forall n$ large enough. Hence, $(a_n)_n \to x$, i.e., X is complete.

Theorem 1.1.2. *Given a field K with an absolute value $|\cdot|$, there exists a field $\widehat{K}$, complete with respect to $|\cdot|$, and an embedding $i : K \to \widehat{K}$ such that $|i(x)| = |x|$ for all $x \in K$.*

The image $i(K)$ is dense in $\widehat{K}$. If $(\widehat{K}', i')$ is another such pair, then there exists a unique continuous isomorphism $\varphi : \widehat{K} \to \widehat{K}'$, preserving the absolute value, such that the following diagram commutes:

$$\begin{tikzcd}
\widehat{K} \arrow[rr, "\varphi"] & & \widehat{K}' \\
& K \arrow[ul, "i"] \arrow[ur, "i'"'] \arrow[u, phantom, "\circ"] &
\end{tikzcd}$$

Proof. **Existence of $\widehat{K}$:** Let $\mathcal{C}$ be the set of Cauchy sequences of elements in K. Clearly, $\mathcal{C}$ is a commutative ring with unity.

Consider the set of null sequences $\mathcal{N} = \{(x_n)_{n\in\mathbb{N}} : \lim_{n\to\infty} x_n = 0\} \subset \mathcal{C}$.

$\mathcal{N}$ is an ideal of $\mathcal{C}$: take any $(a_n)_n \in \mathcal{N}$. Then, $\exists n_0 \in \mathbb{N}$ such that

$$|a_m - a_{n_0+1}| < 1 \;\forall m > n_0.$$

Thus, $|a_m| = |a_m - a_{n_0+1} + a_{n_0+1}| < |a_m - a_{n_0+1}| + |a_{n_0+1}| < 1 + |a_{n_0+1}| \;\forall m > n_0$, i.e., $(a_n)_n$ is bounded above. Now, let $(b_n)_n \in \mathcal{N}$ and $\varepsilon > 0$. Then, $\exists n_1' \in \mathbb{N}$ such that $|b_n| < \dfrac{\varepsilon}{1 + |a_{n_0+1}|}$, $\forall n > n_1'$. Thus, if $n > \max\{n_0, n_1'\}$, then $|a_n b_n| < \varepsilon$, i.e., $(a_n b_n)_n \in \mathcal{N}$.

Claim: Every sequence from $\mathcal{C} \setminus \mathcal{N}$ also admits a lower bound.

Suppose not: let $(a_n)_n \in \mathcal{C} \setminus \mathcal{N}$ be such that for all $\eta > 0$ and every $n_0 \in \mathbb{N}$, $|a_m| < \eta$ for some $m > n_1'$. Now, since $(a_n)_n$ is Cauchy, given $\varepsilon > 0$, we can pick $n_1' \in \mathbb{N}$ such that $|a_p - a_q| < \varepsilon/2$, $\forall\; p, q > n_1'$.

Choosing $\eta = \varepsilon/2$, we get $m > n_1'$ be such that $|a_m| < \varepsilon/2$. Then, for all $p > n_1'$, $|a_p| \le |a_p - a_m| + |a_m| < \varepsilon$, which contradicts the fact that $(a_n)_n \notin \mathcal{N}$. This proves the claim.

Claim: $\mathcal{N}$ is a maximal ideal.

Fix an arbitrary sequence $(a_n)_n \in \mathcal{C} \setminus \mathcal{N}$. Then, there exist some $m_0 \in \mathbb{N}$ and $\eta > 0$ such that $|a_n| > \eta$ for all $n > m_0$.Define a sequence $(c_n)_n$ by $c_n := 1$ for $1 \le n \le M$, and $c_n := a_n^{-1}$ for $n > M$, where M will be chosen later. Let $\varepsilon > 0$ be given. Since $(a_n)_n$ is Cauchy, there exists $n_0 \in \mathbb{N}$ such that $|a_p - a_q| < \varepsilon\eta^2$ for all $p, q > n_0$. Set $M = \max\{n_0, m_0\}$. Then, for all $p, q > M$, we have

$$|c_p - c_q| = |a_p^{-1} - a_q^{-1}| = \left|\frac{a_q - a_p}{a_p a_q}\right| = |a_p - a_q| \cdot |a_p^{-1}|^{-1} \cdot |a_q|^{-1} \le \varepsilon\eta^2 \cdot \frac{1}{\eta} \cdot \frac{1}{\eta} = \varepsilon.$$

This shows that $(c_n)_n$ is Cauchy, hence $(c_n)_n \in \mathcal{C}$. Consider now $(a_n c_n)_n$. We have $|a_n c_n| = 1$ for all $n > m_0$, i.e., $(a_n c_n)_n \to 1$, i.e., $(a_n c_n)_n - 1 \in \mathcal{N}$. Thus, if we take $\mathcal{N}' = \mathcal{N} + \langle (c_n)_n \rangle$, then $\mathcal{N}' = \mathcal{C}$. Since $(a_n)_n$ was arbitrary, this means $\mathcal{N}$ is maximal. Hence, $\widehat{K} \coloneqq \mathcal{C}/\mathcal{N}$ is a field. This concludes the proof of existence of $\widehat{K}$.

Existence and density of the embedding: We have an embedding $K \hookrightarrow \widehat{K}$ defined by $x \mapsto (x, x, x, \dots)$. From the previously seen uniform continuity of $|\cdot|$, we have $||x| - |y||_0 \le |x - y|$, where $|\cdot|_0$ denotes the usual absolute value. By definition, for all $(a_n)_n \in \mathcal{N}$, we have $\lim_{n\to\infty}|a_n| = 0$. Hence, for $\xi = (a_n)_n + \mathcal{N}$, the value $\lim_{n\to\infty}|a_n|$ does not depend on the representative $(a_n)_n$ of ξ. This follows from the observation that if $\xi = (a_n)_n + \mathcal{N} = (b_n)_n + \mathcal{N}$ then $(a_n - b_n)_n$ is a nullsequence, hence $\lim_{n\to\infty}|a_n - b_n| = 0$, hence $\lim_{n\to\infty}|a_n| = \lim_{n\to\infty}|b_n|$. We thus define $\widehat{|\xi|} \coloneqq \lim_{n\to\infty}|a_n|$. By the properties of limits and $|\cdot|$, it follows that this is an absolute value on $\widehat{K}$ that induces $|\cdot|$ on K.

Claim: $i(K)$ is dense in $\widehat{K}$ with respect to $|\cdot|$.

Recall that a subspace Y of a metric space X is *dense* if $\forall \varepsilon > 0, x \in X,$ there exists $y \in Y$ such that $d(x, y) < \varepsilon$, i.e., $B(x, \varepsilon) \cap Y \neq \emptyset$. Fix $(x_n)_n \in \mathcal{C}$. Let $\varepsilon > 0$ be arbitrary. Choose $N \in \mathbb{N}$ such that $|x_n - x_m| < \varepsilon \ \forall n, m \ge N$. In particular, $|x_n - x_N| < \varepsilon \ \forall n \ge N$. Therefore,

$$\lim_{n\to\infty}|x_n - x_m| \le \varepsilon \implies |\widehat{(x_n)_n - (x_N)_n + \mathcal{N}}| = |\widehat{(x_n)_n - i(x_N) + \mathcal{N}}| \le \varepsilon.$$

Hence, given any $(x_n)_n + \mathcal{N} \in \widehat{K}$, we have a corresponding element $i(x_N) \in i(K)$ such that $|\widehat{(x_n)_n + \mathcal{N} - i(x_N)}| \le \varepsilon$.

Therefore, $i(K)$ is dense in $\widehat{K}$ with respect to $\widehat{|\cdot|}$.

We now prove the completeness of $\widehat{K}$.

We have shown that $i(K)$ is dense in $\widehat{K}$. Hence, if we show that every Cauchy sequence in $i(K)$ converges to a point in $\widehat{K}$, then we are done (by lemma 1.1.1). Consider a Cauchy sequence $(\mathcal{Z}_n)_n \subseteq i(K)$, i.e., $\mathcal{Z}_n = (z_n, z_n, \dots, z_n) + \mathcal{N}$. We have $\widehat{|\mathcal{Z}_n - \mathcal{Z}_m|} = |z_n - z_m|$, by definition. Since $(\mathcal{Z}_n)_n$ is Cauchy, $\widehat{|\mathcal{Z}_n - \mathcal{Z}_m|} = |z_n - z_m| < \varepsilon$ for $n, m \ge M$. Hence, $(z_n)_n = (z_1, z_2, z_3, \dots)$ is a Cauchy sequence in K. Consider $(z_n)_n + \mathcal{N} \coloneqq \mathcal{Z}^*$. We will show $(\mathcal{Z}_n) \to \mathcal{Z}^*$. Given $\varepsilon > 0$, $\exists N \in \mathbb{N}$ such that $|z_k - z_n| < \varepsilon/2 \ \forall \ k, n \ge N$. Fixing $k \ge N$, we get $|z_k - z_n| < \varepsilon/2 \ \forall n \ge N \implies \lim_{n\to\infty}|z_k - z_n| \le \varepsilon/2$.

Now,

$$
\begin{aligned}
\widehat{|\mathcal{Z}_k - \mathcal{Z}^*|} &= \widehat{|(z_k, z_k, \dots) - (z_1, z_2, \dots) + \mathcal{N}|} \\
&= \widehat{|(z_k - z_1, z_k - z_2, \dots) + \mathcal{N}|} \\
&= \lim_{n\to\infty} |z_k - z_n| \le \varepsilon/2 < \varepsilon
\end{aligned}
$$

Hence, $(\mathcal{Z}_n) \to \mathcal{Z}^*$.

Uniqueness of $(\widehat{K}, i)$**:** let $(\widehat{K'}, i')$ be another pair with the same properties.

For every $\xi = (a_n)_n + \mathcal{N} \in \widehat{K}$, we have a sequence $(i'(a_n))_n$ in $\widehat{K'}$. Since $(a_n)_n$ is Cauchy in K, $(i'(a_n))_n$ is Cauchy in $\widehat{K'}$. Let its limit be $\xi' \in \widehat{K'}$.

Define $\varphi : \widehat{K} \to \widehat{K'} : \xi \mapsto \xi'$. φ is well-defined, by uniqueness of limits. Given $\eta' \in \widehat{K'}$, there exists a sequence $(i'(b_n))_n \subset i'(K)$ which converges to η'. Consider $(b_n)_n \subset K$ and let $\lim_{n\to\infty} i(b_n) = \eta \in \widehat{K}$. Then, $\varphi(\eta) = \eta'$ by definition. Hence, φ is surjective. Now, let $\xi_1, \xi_2 \in \widehat{K}$ with associated sequences $(i'(a'_n))_n$ and $(i'(b'_n))_n$. Then, $\xi_1 + \xi_2$ is associated to $(i'(a'_n) + i'(b'_n))_n = (i'(a'_n + b'_n))_n$, since i' is a homomorphism. Similarly, $\xi_1\xi_2$ is associated to $(i'(a'_n))_n(i'(b'_n))_n = (i'(a'_n b'_n))_n$.

Thus,

$$
\varphi(\xi_1 + \xi_2) = \lim(i'(a'_n + b'_n)) = \lim i'(a'_n) + \lim i'(b'_n) = \varphi(\xi_1) + \varphi(\xi_2).
$$

Similarly, $\varphi(\xi_1\xi_2) = \varphi(\xi_1)\varphi(\xi_2)$. Thus, φ is a homomorphism.

Since it is a nontrivial field homomorphism, φ must be injective. Therefore, φ is an isomorphism, and by its very definition, φ makes the diagram below commute.

$$
\begin{tikzcd}
\widehat{K} \arrow[rr, "\varphi"] & & \widehat{K'} \\
& K \arrow[ul, "i"] \arrow[ur, "i'"'] \arrow[u, phantom, "\circ"] &
\end{tikzcd}
$$

Remark 1.1. The pair $(\widehat{K}, \widehat{|\cdot|})$ is called a ***completion*** of $(K, |\cdot|)$.

Proposition 1.1.3. *Every Archimedean absolute value on* $\mathbb{Q}$ *is dependent on the usual one.*

Proof. Let $|\cdot|$ be an Archimedean absolute value on $\mathbb{Q}$. Let $|\cdot|_0$ denote the usual absolute value on $\mathbb{Q}$. Let $m, n \ge 2$ be arbitrary integers and let $t \ge 1$. Expand m^t in powers of n: $m^t = \sum_{i=0}^{s} c_i n^i$, where $0 \le c_i < n$, $c_s \ne 0$.

Now, $|c_i| = |1 + 1 + \cdots + 1| \le c_i|1| = c_i \le n$ ($\because |1|^2 = |1^2| = |1| \implies |1| = 1$).

Hence, for each $0 \le i \le s$, depending on whether $|n| \ge 1$ or $|n| < 1$, we have

$$|m|^t \le \sum_{i=0}^{s} |c_i||n|^i \le n \sum_{i=0}^{s} |n|^i \le n(s+1)\max\{1, |n|^s\}.$$

Since $n^s \le m^t$, we have $s\ln(n) \le t\ln(m) \implies s \le t\dfrac{\ln(m)}{\ln(n)}$.

Hence,

$$|m|^t \le n\left(\frac{t\ln(m)}{\ln(n)} + 1\right)\max\{1, |n|^{\frac{t\ln(m)}{\ln(n)}}\}$$
$$\implies |m| \le n^{1/t}\left(\frac{t\ln(m)}{\ln(n)} + 1\right)^{1/t}\max\left\{1, |n|^{\frac{\ln(m)}{\ln(n)}}\right\}.$$

As $t \to \infty$, we get $|m| \le \max\left\{1, |n|^{\frac{\ln(m)}{\ln(n)}}\right\}$. Note that we can take t-th root on both sides in the step above since all the quantities above are positive and real.

Suppose $|n| < 1$ for some n. Then by the above inequality, $|m| \le 1$ for all $m \ge 2$. This contradicts Archimedeanness. Hence, $\forall n \ge 2$ we must have $|n| \ge 1$. Thus, $|m| \le |n|^{\frac{\ln(m)}{\ln(n)}}$. Interchanging m, n above gives $|n| \le |m|^{\frac{\ln(n)}{\ln(m)}}$, hence we get $|n| = |m|^{\frac{\ln(n)}{\ln(m)}}$. Hence, if $m > n \ge 2$, then $\frac{\ln(m)}{\ln(n)} > 1$, so $|m| > |n|$. By definition, $|-m| = |m|$. Therefore, $|mb| > |nb| \implies |m| > |n|$. Consequently, if $m/n \in \mathbb{Q}$ satisfies $|m/n|_0 < 1$, then $|m/n| < 1$. Thus, we have shown $|x|_0 < 1 \implies |x| < 1\ \forall x \in \mathbb{Q}$, i.e., $|\cdot|$ and $|\cdot|_0$ are dependent.

☕

Up till now, we have restricted ourselves to Archimedean absolute values. Let us now consider nontrivial, non-Archimedean absolute values on a field K. For future convenience, we use the additive presentation of the absolute value: we define

$$v : K \to \mathbb{R} \cup \{\infty\} \text{ with } v(x) := -\ln|x|.$$

Then, the axioms read as follows, for all $x, y \in K$:

1. $v(x) \in \mathbb{R}$ for all $x \neq 0$, and $v(0) = \infty$
2. $v(xy) = v(x) + v(y)$
3. $v(x + y) \ge \min\{v(x), v(y)\}$

Remark 1.2. Note that we only use the additive structure of $\mathbb{R}$ and its ordering, hence we can (and will) generalize this definition later by requiring the target of v to just be an ordered abelian group unioned with a formal symbol ∞.

Now assuming that v is a non-Archimedean absolute value on K, the set $\mathcal{O}_v \coloneqq \{x \in K \mid v(x) \geq 0\}$ is a subring of K. This is easy to check: for any $x, y \in \mathcal{O}_v$, we have $v(x \pm y) \geq \min\{v(x), v(\pm y)\} \geq 0$ and $v(xy) = v(x) + v(y) \geq 0$. Hence $x \pm y, xy \in \mathcal{O}_v$. In fact, it is an integral domain: if $xy = 0$, then $\infty = v(xy) = v(x) + v(y) \implies v(x) = \infty$ or $v(y) = \infty$, whence $x = 0$ or $y = 0$ From $v(x^{-1}) = -v(x)$ (recall $|x^{-1}| = |x|^{-1}$), we find that x is a unit in $\mathcal{O}_v$ if and only if $v(x) = 0$, and that for every $x \in K$, either x or x^{-1} or both lie in $\mathcal{O}_v$.

Definition 1.1.5. An integral domain $\mathcal{O}$ of K satisfying $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$ for all $x \in K^\times$ is called a ***valuation ring*** of K. Thus $\mathcal{O}_v$ is a valuation ring of K.

Moreover, $\mathcal{M}_v \coloneqq \{x \in K \mid v(x) > 0\} \lhd \mathcal{O}_v$, because for any $x \in \mathcal{O}_v, t \in \mathcal{M}_v$, we have $v(xt) = v(x) + v(t) \geq v(t) > 0$, i.e., the product $xt \in \mathcal{M}_v$. Now, notice that x is a unit in $\mathcal{O}_v$ if and only if $x, x^{-1} \in \mathcal{O}_v \iff v(x) \geq 0$ and $v(x^{-1}) \geq 0 \iff v(x) \geq 0$ and $-v(x) \geq 0 \iff v(x) = 0$ (since $v(x^{-1}) = -v(x)$).

Moreover, $\mathcal{M}_v$ is the unique maximal ideal because if $\mathfrak{m} \supsetneqq \mathcal{M}_v$ was another, then it must contain a unit, and so $\mathfrak{m} = \mathcal{O}_v$. In summary, $\mathcal{M}_v$ is the unique maximal ideal consisting exactly of the non-units of $\mathcal{O}_v$. Therefore, $\mathcal{O}_v$ is a local ring.

Definition 1.1.6. $\overline{\mathcal{K}}_v \coloneqq \mathcal{O}_v/\mathcal{M}_v$ is called the ***residue class field*** of v. The residue class of $a \in \mathcal{O}_v$ is denoted by $\overline{a}$. Note that v is trivial if and only if $\mathcal{O}_v = K$, and hence also $\overline{\mathcal{K}}_v = K$. The group $v(K^\times)$ is called the ***value group*** of v.

Example 1.3. Consider $K = \mathbb{Q}$ and $v = v_p$, the p-adic valuation. Recall that $v_p(p^\nu \frac{m}{n}) = \nu$. We then have:

$$\mathcal{O}_{v_p} = \{x \in \mathbb{Q} \mid v_p(x) \geq 0\} = \left\{ \frac{a}{b} \in \mathbb{Q} \,\middle|\, a, b \in \mathbb{Z},\ p \nmid b \right\} \text{ and}$$

$$\mathcal{M}_{v_p} = \{x \in \mathbb{Q} \mid v_p(x) > 0\} = \left\{ \frac{ap}{b} \in \mathbb{Q} \,\middle|\, a, b \in \mathbb{Z},\ p \nmid b,\ p \mid a \right\}.$$

Note that $\mathcal{O}_v = \mathbb{Z}_{(p)}$, the localisation of $\mathbb{Z}$ at $p\mathbb{Z}$ and $\mathcal{M}_v = p\mathcal{O}_v = p\mathbb{Z}_{(p)}$. Hence, $\overline{\mathcal{K}}_v = \mathcal{O}_v/\mathcal{M}_v = \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \mathbb{Z}/p\mathbb{Z} \equiv \mathbb{F}_p$.

Example 1.4. Take $k[x]$, where k is a field, and the absolute value is given by
$|p^\nu f/g|_p = 1/e^\nu$, where $\nu \in \mathbb{Z}$, and $f, g \in k[x] \setminus \{0\}$ are not divisible by p.

Now, $v\left(p^\nu f/g\right) = -\ln \left|p^\nu f/g\right|_p = -\ln\left(1/e^\nu\right) = \nu$. Similar to above, we get $\mathcal{O}_v = k[x]_{(p)}$, the localisation of $k[x]$ at the prime ideal $(p) = pk[x]$. The maximal ideal is $pk[x]_{(p)}$, and $\overline{\mathcal{K}}_v = k[x]_{(p)}/pk[x]_{(p)} = k[x]/pk[x]$.

Proposition 1.1.4. *For any $x, y \in K$ with $v(x) < v(y)$, we have $v(x+y) = v(x)$.*

Proof. Suppose not, i.e., there exist some $x, y \in K$ with $v(x) < v(y)$ such that $v(x+y) \neq v(x)$. Now, since $v(x+y) \geq \min\{v(x), v(y)\}$, we must have $v(x+y) > v(x)$. Then, since $v(y) > v(x)$ and $v(x+y) > v(x)$, we get

$$\begin{aligned} v(x) = v((x+y)+(-y)) &\geq \min\{v(x+y), v(-y)\} \\ &= \min\{v(x+y), v(y)\} > v(x). \end{aligned}$$

This is a contradiction. ☕

Remark 1.3. $b \in \mathcal{O}_v$, $\overline{b} = 0$ in $\overline{\mathcal{K}}_v$ if and only if $b \in \mathcal{M}_v$, i.e., $v(b) > 0$, and $\overline{b} \neq 0$ in $\overline{\mathcal{K}}_v$ if and only if $b \in \mathcal{O}_v$ but $b \notin \mathcal{M}_v$, i.e., $v(b) = 0$.

Lemma 1.1.3. *Given a polynomial $f(x) \in R[x]$, where R is a commutative ring with unity, there exists a polynomial $g(x, y) \in R[x, y]$ such that*

$$f(x+y) = f(x) + yf'(x) + y^2 g(x, y).$$

Proof. We have $f(x) = \sum_{i=0}^{n} a_i x^i$, thus $f(x+y) = \sum_{i=0}^{n} a_i (x+y)^i$. Hence,

$$\begin{aligned} f(x+y) &= a_0 + \sum_{i=1}^{n} a_i (x^i + ix^{i-1}y) + \sum_{i=1}^{n} g_i(x,y)y^2 \text{ for } g_i \in R[x,y], \\ &= \sum_{i=0}^{n} a_i x^i + \sum_{i=1}^{n} ia_i x^{i-1} y + g(x,y)y^2, \text{ where } \sum_{i=1}^{n} g_i(x,y) = g(x,y) \\ &= f(x) + yf'(x) + y^2 g(x,y). \end{aligned}$$

☕

Theorem 1.1.3 (Hensel's Lemma)**.** *Let K be a field complete with respect to a non-Archimedean absolute value v. Let $f \in \mathcal{O}_v[x]$ be a polynomial and $a_0 \in \mathcal{O}_v$ such that $v(f(a_0)) > 2v(f'(a_0))$. Then, there exists $a \in \mathcal{O}_v$ with $f(a) = 0$ and $v(a - a_0) > v(f'(a_0))$.*

Proof. Let $b_0 = f'(a_0)$ and choose $\varepsilon > 0$ such that $v(f(a_0)) \geq v(b_0^2) + \varepsilon$. This is possible because $v(f(a_0)) > 2v(f'(a_0)) = 2v(b_0) = v(b_0^2)$ Then, $f(a_0) = b_0^2 c_0$, where $c_0 = \frac{f(a_0)}{b_0^2} \in K$ and $v(c_0) \geq \varepsilon$. Set $a_1 \coloneqq a_0 - b_0 c_0$. By the lemma above, there exists $d_0 \in K$ such that $f(a_1) = f(a_0 - b_0 c_0) = f(a_0) - b_0 c_0 f'(a_1) + (b_0 c_0)^2 d_0 = b_0^2 c_0 d_0$. Since $c_0, b_0, c_0 \in \mathcal{O}_v$, $d_0 \in \mathcal{O}_v$. Therefore,

$$v(f(a_1)) = v(b_0^2 c_0^2 d_0) = v(b_0^2) + 2v(c_0 d_0) \geq v(b_0^2) + 2\varepsilon \tag{1}$$

Applying the same procedure to f', we get $f'(a_1) = f'(a_0 - b_0c_0) = f'(a_0) - b_0c_0b = b_0 - b_0c_0b = b_0(1 - c_0b) =: b_1$ for some $b \in \mathcal{O}_v$. Now, since $v(1 - c_0b) = v(1) = 0$, as $v(1) < v(c_0b)$, we have $v(b_1) = v(b_0) + v(1 - c_0b) = v(b_0)$. Hence, (1) implies $v(f(a_1)) \geq v(b_1^2) + 2\varepsilon$, i.e., $f(a_1) = b_1^2c_1$ where $v(c_1) > 2\varepsilon$.

We now repeat the above argument after replacing b_0 with b_1, a_1 with $a_2 \coloneqq a_1 - b_1c_1$, and ε with 2ε, to obtain a b_2 with $f'(a_2) = b_2$ such that $v(b_2) = v(b_0)$ and $f(a_2) = b_2^2c_2$ for some c_2 with $v(c_2) \geq 2^2\varepsilon$. This goes as follows:

We have $f(a_1) = b_1^2c_1$, where $v(c_1) > 2\varepsilon$, so by the lemma above, there exists $d_1 \in K$ with $f(a_2) = f(a_1 - b_1c_1) = f(a_1) - b_1c_1f'(a_2) + (b_1c_1)^2d_1 = b_1^2c_1d_1$. Since $c_1, b_1, c_1 \in \mathcal{O}_v$, we get $d_1 \in \mathcal{O}_v$. Therefore,

$$v(f(a_2)) = v(b_1^2c_1^2d_1) = v(b_1^2) + 2v(c_1d_1) \geq v(b_1^2) + 4\varepsilon \tag{2}$$

Applying the same procedure to f', we get $f'(a_2) = f'(a_1 - b_1c_1) = f'(a_1) - b_1c_1b = b_1 - b_1c_1b = b_1(1 - c_1b) =: b_2$ for some $b \in \mathcal{O}_v$. Now, $v(1 - c_1b) = v(1) = 0,$ as $v(1) < v(c_1b)$, hence we get $v(b_2) = v(b_1) + v(1 - c_1b) = v(b_1)$. Therefore, (2) implies $v(f(a_2)) \geq v(b_2^2) + 4\varepsilon$, i.e., $f(a_2) = b_2^2c_2$ where $v(c_2) > 4\varepsilon$. Iteratively continuing, we get a sequence $a_{n+1} = a_n - b_nc_n$, where $f'(a_{n+1}) = b_{n+1}, v(b_{n+1}) = v(b_0)$, $f(a_{n+1}) = b_{n+1}^2c_{n+1}$, and $v(c_{n+1}) \geq 2^{n+1}\varepsilon$.

Claim: $(a_n)_n$ is Cauchy: For $m < n$, we have:

$$\begin{aligned} v(a_n - a_m) &= v\left(\sum_{i=m}^{n-1}(a_{i+1} - a_i)\right) \\ &\geq \min_{m\leq i<n} v(a_{i+1} - a_i) \\ &= \min_{m\leq i<n} v(b_ic_i) \geq v(b_0) + 2^m\varepsilon. \end{aligned}$$

Hence, $\lim_{m\to\infty} v(a_n - a_m) = \infty$, i.e., $\lim_{m\to\infty} |a_n - a_m| = 0$, since $v(x) = -\ln|x| = \ln(1/|x|)$. Let $a = \lim_{n\to\infty} a_n$. Then, since the polynomial f is continuous, $f(a) = \lim_{n\to\infty} f(a_n)$.

Claim: $(b_n)_n \to f'(a)$: Since $a_n \to a$, we have $f'(a_n) \to f'(a)$, i.e., $b_n \to f'(a)$.

Now, $v(f(a_n)) = v(b_n^2) + v(c_n) \geq 2^n\varepsilon$ for all n. Hence, $\lim_{n\to\infty} v(f(a_n)) = \infty$, i.e., $\lim_{n\to\infty} f(a_n) = 0$, i.e., $f(a) = 0$. Furthermore, $v(f'(a_n)) = v(b_n) = v(b_0) \implies v(f'(a)) = v(b_0)$. From $v(a_n - a_m) \geq v(\sum_{i=m}^{n-1}(a_{i+1} - a_i))$, we get $(a_n - a_0) \geq v(b_0) + \varepsilon$. Hence, for n sufficiently large $v(a - a_0) = v((a - a_n) + (a_n - a_0)) \geq v(b_0) + \varepsilon > v(b_0) = v(f'(a_0))$. Therefore, our choice $a = \lim_{n\to\infty} a_n$ satisfies the assertions of the theorem.

Corollary 1.1.3.1. *Let K be a field complete with respect to a non-Archimedean absolute value v. Let $f \in \mathcal{O}_v[X]$ be a polynomial having a simple zero $\bar{a}_0$ in $\overline{\mathcal{K}_v}$, i.e., $\bar{f}(\bar{a}_0) = 0$ and $\bar{f}'(\bar{a}_0) \neq 0$. Then, f has a zero $a \in \mathcal{O}_v$ such that $\bar{a} = \bar{a}_0$ in $\overline{\mathcal{K}_v}$.*

Proof. Since $\bar{f}(\bar{a}_0) = 0$, we have $f(a_0) \in \mathcal{M}_v$, i.e., $v(f(a_0)) > 0$ and $f'(a_0) \notin \mathcal{M}_v$, i.e., $v(f'(a_0)) = 0$. Hence, by the theorem, $\exists a \in \mathcal{O}_v$ such that $f(a) = 0$ and $v(a - a_0) > v(f(a_0)) = 0$, i.e., $a - a_0 \in \mathcal{M}_v$, i.e., $\bar{a} = \bar{a}_0$.

Let $(\widehat{K}, \hat{v})$ denote the completion of (K, v).

Theorem 1.1.4. *Denote by $\mathcal{O}_{\hat{v}}$, $\overline{\mathcal{K}_{\hat{v}}}$ and $\mathcal{O}_v$, $\overline{\mathcal{K}_v}$ the valuation ring and residue class field of $\hat{v}$ and v, respectively. Then, $\overline{\mathcal{K}_v}$, $\overline{\mathcal{K}_{\hat{v}}}$ and $v(K^\times)$, $\hat{v}(\widehat{K}^\times)$ are canonically isomorphic.*

Proof. Consider $\mathcal{O}_{\hat{v}} = \{x \in \widehat{K} : \hat{v}(x) \geq 0\}$.

Thus, $\mathcal{O}_{\hat{v}} \cap K = \{x \in K : \hat{v}(x) \geq 0\} = \{x \in K : v(x) \geq 0\} = \mathcal{O}_v$ since $\hat{v}|_K = v$. Similarly, $\mathcal{M}_{\hat{v}} \cap K = \mathcal{M}_v$. Consider the map $\mathcal{O}_v \to \mathcal{O}_{\hat{v}}/\mathcal{M}_{\hat{v}} : a \mapsto \bar{a}$. It is well-defined since $a - b = 0$ in $\mathcal{O}_v \implies a - b \in \mathcal{M}_v \subseteq \mathcal{M}_{\hat{v}}$, thus $\bar{a} = \bar{b}$. It is clear that the map is a ring morphism as well.

We now show surjectivity: $\forall \bar{x} \in \mathcal{O}_{\hat{v}}/\mathcal{M}_{\hat{v}}$, $x + \mathcal{M}_{\hat{v}}$ is an open neighbourhood of x, since it consists of all z such that $\hat{v}(x - z) > 0$, i.e., $\widehat{|x - z|} < 1$. We know that K is dense in $\widehat{K}$, thus $(x + \mathcal{M}_{\hat{v}}) \cap K \neq \varnothing$. Consider $y \in (x + \mathcal{M}_{\hat{v}}) \cap K$, then $y \mapsto \bar{x}$. Hence, given any $\bar{x} \in \mathcal{O}_{\hat{v}}/\mathcal{M}_{\hat{v}}$, $\exists y \in K$ such that $y \mapsto \bar{x}$. Thus, by the first isomorphism theorem, we obtain $\mathcal{O}_v/\mathcal{M}_v \xrightarrow{\sim} \mathcal{O}_{\hat{v}}/\mathcal{M}_{\hat{v}}$; that is $\overline{\mathcal{K}_v} \cong \overline{\mathcal{K}_{\hat{v}}}$.

Consider $v(K^\times) \to \hat{v}(\widehat{K}^\times)$. This is a group monomorphism as $K^\times \subset \widehat{K}^\times$. To see its surjectivity, take $x \in \widehat{K}^\times$, then $\exists z \in K$ such that $\widehat{|z - x|} < |x|$, i.e.,

$$\hat{v}(z - x) > \hat{v}(x) = v(x) \implies \hat{v}(z) = \hat{v}(x), \text{ implying } \hat{v}(z) = v(x).$$

Therefore, as before, we get $v(K^\times) \xrightarrow{\sim} \hat{v}(\widehat{K}^\times)$.

Definition 1.1.7. An absolute value v is called ***discrete*** *(of rank 1)* if $v(K^\times) = (\mathbb{Z}, +)$. Any $\pi \in K$ with $v(\pi) = 1$ is called a ***uniformizer*** or a ***local parameter*** for v.

Now, if $v(x) = r$, then $v(x\pi^{-r}) = v(x) - rv(\pi) = v(x) - v(x) = 0$, i.e., $x\pi^{-r} = u$, where u is a unit of $\mathcal{O}_v$. Hence, every $x \in K^\times$ can be written as $x = \pi^r u$. In particular, any $x \in \mathcal{M}_v$ can be written as $x = u\pi^r$, and thus $\mathcal{M}_v = \langle \pi \rangle$. From this it immediately follows that $(\mathcal{M}_v)^n = \langle \pi^n \rangle$. Given any other ideal $\mathfrak{a} \triangleleft \mathcal{O}_v$, $\mathfrak{a} \subseteq \mathcal{M}_v$ (every ideal is contained in a maximal ideal and $\mathcal{M}_v$ is the unique maximal ideal of $\mathcal{O}_v$). Thus, $\mathfrak{a}$ is principal. Therefore, $\mathcal{O}_v$ is a principal ideal domain, hence factorial (i.e., a unique factorisation domain).

Proposition 1.1.5. *Let v be a discrete absolute value on K with uniformizer π. Then, every $x \in K^\times$ can be written uniquely as a convergent series*

$$x = r_\nu \pi^\nu + r_{\nu+1}\pi^{\nu+1} + r_{\nu+2}\pi^{\nu+2} + \cdots = \lim_{n\to\infty} \sum_{i=\nu}^{n} r_i \pi^i,$$

where $\nu = v(x)$, $r_\nu \neq 0$, and the coefficients r_i are taken from a set $R \subseteq \mathcal{O}_v$ of representatives of the residue classes in the field K_v (i.e., the canonical map $\mathcal{O}_v \to K_v$ induces a bijection of R onto K_v).

Proof. As before, $u = x\pi^{-\nu}$ is a unit in $\mathcal{O}_v$. Choose $r_\nu \in R$ such that $\overline{r_\nu} = \overline{u}$, i.e., $r_\nu - u \in \mathcal{M}_v$, i.e., $v(r_\nu - u) > 0$, and $v(r_\nu - x\pi^{-\nu}) > 0$. Thus,

$$\begin{aligned} v(x - r_\nu\pi^\nu) > 0 &\implies v(x - r_\nu\pi^\nu + \pi^\nu) > 0 \\ \implies v(x - r_\nu\pi^\nu) &> v(\pi^\nu) = \nu v(\pi) = \nu. \end{aligned}$$

Let $x_1 = x - r_\nu\pi^\nu$ and $\mu = v(x_1) > \nu$. By the same argument, we can choose $r_\mu \in R$ such that $\overline{r_j} = \overline{x_1}$, and get $v(x - (r_\nu\pi^\nu + r_\mu\pi^\mu)) = v(x_1 - r_\mu\pi^\mu) > -v(\pi^{-\mu}) = \mu$. Repeating the same and adding zero coefficients (i.e., $\overline{r_\alpha} = \overline{0}$) as necessary, we obtain a series:

$$r_\nu\pi^\nu + r_{\nu+1}\pi^{\nu+1} + \cdots = \sum_{i=0}^{\infty} r_\nu \pi^\nu.$$

Now, $v(x - r_\nu\pi^\nu) > \nu$, and $v(x - (r_\nu\pi^\nu + r_\mu\pi^\mu)) > \mu > \nu$. Hence, we have an increasing nonconstant sequence

$$y_n := v\left(x - \sum_{i=\nu}^{\nu+n} r_i\pi^{r_i}\right) \text{ i.e., } y_1 \leq y_2 \leq \cdots \to \infty.$$

Therefore, $v\left(x - \sum_{i=\nu}^{\infty} r_i\pi^{r_i}\right) = \infty$, i.e., $x - \sum_{i=0}^{\infty} r_i\pi^{r_i} = 0$.

For uniqueness, suppose $x = \sum_{i=0}^{\infty} r_i'\pi^i$, then we have $0 = x - x = \sum_{i=\nu}^{\infty}(r_i - r_i')\pi^i$ with $r_m \neq r_m' \in R$ i.e., $\overline{r_m - r_m'} \neq 0$ for some $m \in \mathbb{N}$. Thus, $v(0) = m$, which is a contradiction. ☕

Remark 1.4. It follows from above that any p-adic number $z \in \mathbb{Q}_p^\times$ has a unique representation of the form $z = \sum_{i=m}^{\infty} \alpha_i p^i$, where $m = v_p(z), \alpha_i \in \{0, 1, \ldots, p-1\}$. If $z \in \mathbb{Z}_p$, then $v(z) > 0$ and $z = \sum_{i=0}^{\infty} \alpha_i\pi^i = \lim_{n\to\infty} \sum_{i=0}^{n} \alpha_i\pi^i$, i.e., given any $z \in \mathbb{Z}_p$, we have a sequence $z_n := \sum_{i=0}^{n} \alpha_i p^i \in \mathbb{Z}_p$ such that $z_n \to z$. **Hence, $\mathbb{Z}$ is dense in $\mathbb{Z}_p$.**

We now briefly take a detour into [**Neukirch1999**]. Note that for the rest of this section, we use the term *valuation* in place of *absolute value*. First, we restate (and provide another, more algebraic, proof of Theorem 1.1.4.), with an extra result concerning discrete valuations. We then move on to some other crucial results, including another version of Hensel's Lemma and its corollaries as well as unqiue extension of a given valuation to an algebraic extension.

Proposition 1.1.6. *Suppose v a discrete valuation, and π is a uniformizer, then the nonzero ideals of $\mathcal{O}$ are given by $\mathfrak{p}^n = \pi^n\mathcal{O} = \{x \in K \mid v(x) \geq n\}, n \geq 0$. We further have $\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong \mathcal{O}/\mathfrak{p}$.*

Proof. Every $x \in K^\times$ can be written as $x = \pi^n u$. In particular, any $x \in \mathfrak{p}$ can be written as $x = u\pi^n$, and thus $\mathfrak{p} = \langle \pi \rangle = \pi\mathcal{O}$. Given any other ideal $\mathfrak{a}$, we have $\mathfrak{a} \subseteq \mathfrak{p}$ as every ideal is contained in some maximal ideal and $\mathfrak{p}$ is the unique maximal ideal. Let $x \in \mathfrak{a}$ with smallest possible value $v(x) = n$. Then, $x = \pi^n u, u \in \mathcal{O}^\times$. Thus, $\langle \pi^n \rangle = \pi\mathcal{O} \subseteq \mathfrak{a}$. Conversely, if $y = \pi^m e \in \mathfrak{a}$ is arbitrary with $e \in \mathcal{O}^\times$, then $v(y) = m \geq n$, hence $y = \pi^n(\pi^{m-n}e) \in \pi^n\mathcal{O}$. Therefore, $\mathfrak{a} = \pi^n\mathcal{O}$. Consider the map $\varphi : \mathfrak{p}^n/\mathfrak{p}^{n+1} \to \mathcal{O}/\mathfrak{p} : a\pi^n \mapsto a + \mathfrak{p}$. Then, $\ker\varphi = \{a\pi^n \mid a \in \mathcal{O}^\times, a + \mathfrak{p} = \mathfrak{p}\} = \{a\pi^n \mid a \in \mathcal{O}^\times, a \in \mathfrak{p}\}$. Now, $\mathfrak{p} = \pi\mathcal{O}$, hence $a \in \mathfrak{p} \implies a = b\pi$ for some $b \in \mathcal{O}^\times$. Thus, $\ker\varphi = \{(b\pi)\pi^n \mid b \in \mathcal{O}^\times\} = \{b\pi^{n+1} \mid b \in \mathcal{O}^\times\} = \mathfrak{p}^{n+1}$. Hence, $\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong \mathcal{O}/\mathfrak{p}$. ☕

In a discretely valued field K, the chain $\mathcal{O} \supseteq \mathfrak{p}^2 \supseteq \mathfrak{p}^3 \supseteq \dots$ forms a basis of neighborhoods of the zero element. Recall that $\mathfrak{p}^n = \{x \in K : v(x) \geq n\}$. Since K is a discretely valued field, $v(x) \in \mathbb{Z}$, hence $v(x) \geq n \iff v(x) > n-1$. Thus, $\mathfrak{p}^n = \{x \in K : v(x) \geq n\} = \{x \in K : |x| < 1/q^n\}$, and we clearly have $0 \in \mathfrak{p}^n$ and $\mathfrak{p}^n \cap \mathfrak{p}^m = \mathfrak{p}^{\max(n,m)}$. Similarly, $U^{(n)} = 1 + \mathfrak{p}^n$ forms a basis of neighborhoods of $1 \in K^\times$, and we have the chain $\mathcal{O}^\times \supseteq U^{(1)} \supseteq U^{(2)} \supseteq \dots$. Note that $U^{(n)} = \{x \in K^\times : |1-x| < 1/q^n\}, n > 0$.

Definition 1.1.8. We call $U^{(1)}$ the group of ***principal units*** and $U^{(n)}$ the n***-th higher unit group***.

Proposition 1.1.7. *$\mathcal{O}^\times/U^{(n)} \cong (\mathcal{O}/\mathfrak{p}^n)^\times$ and $U^{(n)}/U^{(n+1)} \cong \mathcal{O}/\mathfrak{p}$ for all $n \geq 1$.*

Proof. Consider the map $\varphi : \mathcal{O}^\times \to (\mathcal{O}/\mathfrak{p}^n)^\times : u \mapsto u \mod \mathfrak{p}^n$. Then $\ker\varphi = \{u \in \mathcal{O}^\times : u \equiv 1 \mod \mathfrak{p}^n\} = \{u \in \mathcal{O}^\times : u - 1 \in \mathfrak{p}^n\} = \{u \in \mathcal{O}^\times : u \in 1 + \mathfrak{p}^n\} = 1 + \mathfrak{p}^n = U^{(n)}$. To show surjectivity of φ, take an arbitrary $\overline{x} \in (\mathcal{O}/\mathfrak{p}^n)^\times$. Then, there exists $\overline{y} \in (\mathcal{O}/\mathfrak{p}^n)$ such that $xy \equiv 1 \mod \mathfrak{p}^n$, i.e., $xy - 1 \in \mathfrak{p}^n$. Therefore, $v(xy-1) \geq n$. Now, $v(xy) = v(xy - 1 + 1)$ and $0 = v(1) < v(xy) \implies v(xy) = v(1) = 0$. Hence, xy is a unit in $\mathcal{O}$. Therefore, $x^{-1} = (x^{-1}y^{-1})y \in \mathcal{O}$, therefore $x \in \mathcal{O}^\times$, thus giving a preimage of $\overline{x}$. By the first isomorphism theorem, $\mathcal{O}^\times/U^{(n)} \cong (\mathcal{O}/\mathfrak{p}^n)^\times$.

Choose a uniformizer π and write $U^{(n)} = 1 + \mathfrak{p}^n = 1 + \pi^n \mathcal{O}$. Consider the map $U^{(n)} \to \mathcal{O}/\mathfrak{p} : 1 + \pi^n a \mapsto a \mod \mathfrak{p}$. Then its kernel is $\{1 + \pi^n a \in U^{(n)} : a \in \mathfrak{p}\} = \{u \in U^{(n)} : u - 1 \in \pi^n \mathfrak{p}\} = \mathfrak{p}^{n+1}$, where we let $u = 1 + \pi^n a$. This map is surjective because given any $a \mod \mathfrak{p}$, we take $1 + \pi^n a \in U^{(n)}$ as its preimage. Hence, $U^{(n)}/U^{(n+1)} \cong \mathcal{O}/\mathfrak{p}$.

Theorem 1.1.5. *Let $\mathcal{O} \subset K$ and $\widehat{\mathcal{O}} \subset \widehat{K}$ be valuation rings corresponding to v and $\widehat{v}$ respectively, with maximal ideals $\mathfrak{p}$ and $\widehat{\mathfrak{p}}$. Then, we have $\mathcal{O}/\mathfrak{p} \cong \widehat{\mathcal{O}}/\widehat{\mathfrak{p}}$.*

If v is discrete then $\mathcal{O}/\mathfrak{p}^n \cong \widehat{\mathcal{O}}/\widehat{\mathfrak{p}^n}$ for all $n \geq 1$.

Proof. Consider the composite map $\varphi : \mathcal{O} \hookrightarrow \widehat{\mathcal{O}} \twoheadrightarrow \widehat{\mathcal{O}}/\widehat{\mathfrak{p}} : a \mapsto i(a) + \widehat{\mathfrak{p}}$. We first show its surjectivity: take arbitrary $\widehat{x} + \widehat{\mathfrak{p}} \in \widehat{\mathcal{O}}/\widehat{\mathfrak{p}}$ and take a representative sequence $(x_n)_n$ of $\widehat{x}$. Set $\eta := e^{-1}$. Since $i(K)$ is dense in $K, i(K) \cap B(x, \eta) \neq \emptyset$, i.e., there exists $a \in K$ such that $|\widehat{(x_n)_n - i(a)}| < \eta$, i.e., $\widehat{v}(\widehat{x} - i(a)) > -\ln(\eta) = 1 > 0$, i.e., $\widehat{x} - i(a) \in \widehat{\mathcal{O}}$. Note that $\widehat{x} - i(a) \in \widehat{\mathcal{O}}$ and $\widehat{x} \in \widehat{\mathcal{O}}$ imply $i(a) \in \widehat{\mathcal{O}}$. Thus, $v(a) = \widehat{v}(i(a)) \geq 0$, therefore, $a \in \mathcal{O}$. Now, we know that by definition that $\widehat{v}(\widehat{x} - i(a)) = \lim_{v \to \infty} v(x_n - a) > 0$, whence $\widehat{x} - i(a) \in \widehat{\mathfrak{p}}$, i.e., $\widehat{x} \equiv i(a) \mod \widehat{\mathfrak{p}}$, thus proving surjectivity. Consider now the kernel: $\ker \varphi = \{a \in \mathcal{O} : i(a) \in \widehat{\mathfrak{p}}\} = \{a \in \mathcal{O} : \widehat{v}(i(a)) = v(a) > 0\} = \mathfrak{p}$. Hence, we get an isomorphism $\mathcal{O}/\mathfrak{p} \xrightarrow{\sim} \widehat{\mathcal{O}}/\widehat{\mathfrak{p}}$. We have seen that in the case when v is discrete, $\mathfrak{p} = \langle \pi \rangle = \pi \mathcal{O}$, whence $\mathfrak{p}^n = \langle \pi^n \rangle = \pi^n \mathcal{O}$, where $v(\pi) = 1$.

Claim: In $\widehat{K}$, we have $\widehat{\mathfrak{p}^n} = \langle i(\pi^n) \rangle = i(\pi^n)\widehat{\mathcal{O}}$.

The inclusion $\widehat{\mathfrak{p}^n} \supset \langle i(\pi^n) \rangle$ follows by seeing that given any $i(\pi^n)\widehat{u}$, with $\widehat{u} \in \widehat{O}$, we have $\widehat{v}(i(\pi^n)\widehat{u}) = n + \widehat{v}(\widehat{u}) \geq n \implies i(\pi^n)\widehat{u} \in \widehat{\mathfrak{p}^n}$. For the converse, suppose $\widehat{u} \in \widehat{\mathfrak{p}^n}$, i.e., $\widehat{v}(\widehat{u}) = l \geq n$. Now, $\widehat{v}(i(\pi^n)) = v(\pi^n) = n$, thus

$$\widehat{v}(\widehat{u} i(\pi^{-l})) = \widehat{v}(\widehat{u}) - \widehat{v}(i(\pi^l) = l - l = 0.$$

Therefore, $\widehat{u} i(\pi^{-l}) \in \widehat{\mathcal{O}^\times}$ and so $\widehat{u} \in i(\pi^l)\widehat{\mathcal{O}} \subset i(\pi^n)\widehat{\mathcal{O}}$ since $l \geq n$. Hence, $\widehat{\mathfrak{p}^n} \subset \langle i(\pi^n) \rangle$, hence the claim is true. As before, consider the map $\varphi : \mathcal{O} \hookrightarrow \widehat{\mathcal{O}} \twoheadrightarrow \widehat{\mathcal{O}}/\widehat{\mathfrak{p}^n} : a \mapsto i(a) + \widehat{\mathfrak{p}^n}$. The proof of surjectivity follows mutatis mutandis as before by setting $\eta := e^{-n}$. For the kernel, we have

$$\begin{aligned} \ker \varphi &= \{a \in \mathcal{O} : i(a) \in \widehat{\mathfrak{p}^n} = \langle i(\pi^n) \rangle\} \\ &= \{a \in \mathcal{O} : i(a) = \hat{u}\, i(\pi^n), \hat{u} \in \widehat{\mathcal{O}}\} \\ &= \{a \in \mathcal{O} : i(a/\pi^n) = \hat{u} \in \widehat{\mathcal{O}}\} \\ &= \{a \in \mathcal{O} : a/\pi^n \in \mathcal{O}\} \\ &= \{a \in \mathcal{O} : a \in \pi^n \mathcal{O}\} = \mathfrak{p}^n. \end{aligned}$$

Therefore, we have $\mathcal{O}/\mathfrak{p}^n \xrightarrow{\sim} \widehat{\mathcal{O}}/\widehat{\mathfrak{p}^n}$.

Proposition 1.1.8. *Let K be complete with respect to a discrete valuation. The canonical mapping $\varphi : \widehat{\mathcal{O}} = \mathcal{O} \to \varprojlim_n \mathcal{O}/\mathfrak{p}^n : x \to (x \mod \mathfrak{p}, x \mod \mathfrak{p}^2, \ldots)$ is an isomorphism and a homeomorphism (where each $\mathcal{O}/\mathfrak{p}^n$ has the discrete topology and $\lim \mathcal{O}/\mathfrak{p}^n$ has the subspace topology induced by the product topology on $\prod_{n=1}^{\infty} \mathcal{O}/\mathfrak{p}^n$).*

The same is true for the mapping $\mathcal{O}^\times \to \varprojlim_n \mathcal{O}^\times/U^{(n)}$, where $U^{(n)} = 1 + \mathfrak{p}^n$.

Proof. Consider $\ker \varphi = \{x \in \mathcal{O} \mid (x \mod \mathfrak{p}, x \mod \mathfrak{p}^2, \ldots) = 0\} = \{x \in \mathcal{O} \mid x \equiv \mod \mathfrak{p}^n \ \forall n\} = \bigcap_{n\in\mathbb{N}} \mathfrak{p}^n = \bigcap_{n\in\mathbb{N}} \pi^n\mathcal{O}$, hence if $x \in \ker\varphi$ then $x \in \pi^n\mathcal{O}$ for all n, i.e., $v(x) \geq n$ for all n, implying $v(x) = \infty \implies x = 0$. Thus, φ is injective. As an aside, the triviality of $\bigcap_{n\in\mathbb{N}} \mathfrak{p}^n$ also follows from Krull's Intersection Theorem, which states the following:

Theorem. *Let I be a ideal of commutative Noetherian ring R contained in the Jacobson radical and M be a finitely generated R-module. Then, $\bigcap_{n\in\mathbb{N}} I^n M = 0$.*

In our situation, we have a local ring $\mathcal{O}$, hence every ideal is contained in the Jacobson ideal (which is just $\mathfrak{p}$). We put $I = \mathfrak{p}$ and $M = \mathcal{O}$ to conclude $\bigcap_{n\in\mathbb{N}} I^n M = \bigcap_{n\in\mathbb{N}} \mathfrak{p}^n = 0$.

For surjectivity, let $\mathfrak{p} = \pi\mathcal{O}$ and $R \subset \mathcal{O}$ be a system of representatives for $\mathcal{O}/\mathfrak{p}$ such that $0 \in R$. Now, each $a \mod \mathfrak{p}^n \in \mathcal{O}/\mathfrak{p}^n$ can be written uniquely in the form $a = a_0 + a_1\pi + a_2\pi^2 + \ldots + a_{n-1}\pi^{n-1} \mod \mathfrak{p}^n$, $a_i \in R$. Hence, for any $s \in \lim \mathcal{O}/p^n$, we have $s = (s_1, s_2, \ldots)$ with $s_{n+1} \equiv s_n \mod \mathfrak{p}^n$, thus we can write $s_n = a_0 + a_1\pi + a_2\pi^2 + \ldots + a_{n-1}\pi^{n-1}$, $n = 1, 2, \ldots$. Consider $x = \sum_{n=1}^{\infty} a_n\pi^n \in \mathcal{O}$, then $x \equiv s_n \mod \mathfrak{p}^n \implies \varphi(x) = s$, and so φ is surjective. Hence, φ is an isomorphism. We now show that it is also a homeomorphism; it suffices to show that φ is an open continuous map. Consider the collection $P_n = \prod_{v>n} \mathcal{O}/\mathfrak{p}^v = \mathcal{O}/\mathfrak{p}^{n+1} \times \mathcal{O}/\mathfrak{p}^{n+2} \times \ldots$. We claim these form a basis of neighborhoods of the zero element in $\prod_{n=1}^{\infty} \mathcal{O}/\mathfrak{p}^n$. To prove this, we first observe that $0 = (0, 0, \ldots) \in \prod_{v>n} \mathcal{O}/\mathfrak{p}^v$ for any n. Next, suppose V is an arbitrary neighborhood of 0 in $\prod_{n=1}^{\infty} \mathcal{O}/\mathfrak{p}^n$. Then, $V = \prod_{n=1}^{\infty} V_n$ where only finitely many $V_n \neq \mathcal{O}/\mathfrak{p}^n$. Suppose $V_n = \mathcal{O}/\mathfrak{p}^n$ for all $n > t$, then the basic open set $\{0\} \times \{0\} \times \ldots \mathcal{O}/\mathfrak{p}^{n+1} \times \mathcal{O}/\mathfrak{p}^{n+2} \times \ldots \cong P_t$ is contained in V. Therefore, (P_n) form a basis of neighborhoods of 0 in $\prod_{n=1}^{\infty} \mathcal{O}/\mathfrak{p}^n$, which implies that $T_n := P_n \cap \varprojlim_n \mathcal{O}/\mathfrak{p}^n$ form a basis of neighborhoods of 0 in $\varprojlim_n \mathcal{O}/\mathfrak{p}^n$. Now, $\mathcal{O} \supset \mathfrak{p} \supset \mathfrak{p}^2 \supset \mathfrak{p}^3 \supset \ldots$ is a basis of neighborhoods in $\mathcal{O}$, as we saw before. Consider $\varphi(\mathfrak{p}^n) = \{(x \mod \mathfrak{p}, x \mod \mathfrak{p}^2, \ldots) : x \in \mathfrak{p}^n\} = \{(0, 0, \ldots, x \mod \mathfrak{p}^{n+1}, x \mod \mathfrak{p}^{n+2}, \ldots) : x \in \mathfrak{p}^n\} = T_n$, hence φ maps the basis of neighborhoods $\mathfrak{p}^n \in \mathcal{O}$ to the basis of neighborhoods $T_n \in \varprojlim_n \mathcal{O}/\mathfrak{p}^n$, which implies it is an open map. To check continuity, consider the inverse image $\varphi^{-1}(T_n) = \{x \in \mathcal{O} \mid (x \mod \mathfrak{p}, x \mod \mathfrak{p}^2, \ldots) \in \prod_{v>n} \mathcal{O}/\mathfrak{p}^v\} = \{x \in \mathcal{O} \mid x \equiv 0 \mod \mathfrak{p}^n\} = \mathfrak{p}^n$. Hence, φ is an open continuous bijection and therefore it is an isomorphism.

To prove the same for $\mathcal{O}^\times \to \varprojlim_n \mathcal{O}^\times/U^{(n)}$, we simply use the fact that $(\varprojlim_i R_i)^\times = \varprojlim_i R_i^\times$. We prove this below (Lemma 1.1.5). Putting $R_i = \mathcal{O}/\mathfrak{p}^i$ and using the fact $\mathcal{O}^\times/U^{(n)} \cong (\mathcal{O}/\mathfrak{p}^n)^\times$, we conclude the theorem.

Lemma 1.1.4. *Given local rings $(R, \mathfrak{m}_R)$ and $(S, \mathfrak{m}_S)$ with a surjective ring homomorphism $f : R \twoheadrightarrow S$, one obtains a surjective group homomorphism $f^\times : R^\times \twoheadrightarrow S^\times$ by restricting f to $R^\times$.*

Proof. Note that $f^\times$ is well-defined because a ring homomorphism maps units to units. For surjectivity, take an arbitrary $s \in S^\times$ and let its preimage under f be $r \in R$. Consider the inverse t of s in S, i.e., $st = 1$. Suppose the preimage of t under f is $r' \in R$, then we have $f(1) = 1 = st = f(r)f(r') = f(rr') \implies f(1 - rr') = 0 \implies 1 - rr' \in \ker f \subset \mathfrak{J}_R$, the Jacobson radical of R. Thus, r must be a unit, as desired. Hence, $f^\times = f\mid_{R^\times}$ is a surjection.

Lemma 1.1.5. *Given an inverse system of local rings R_i with surjective transition maps $\lambda_n : R_n \twoheadrightarrow R_{n-1}$, the units of the inverse limit are the inverse limit of the units, i.e., $(\varprojlim_i R_i)^\times = \varprojlim_i R_i^\times, i \in \mathbb{N}$, with respect to the transition maps $\lambda_n^\times = \lambda_n \mid_{R_n^\times} : R_n^\times \twoheadrightarrow R_{n-1}^\times$.*

Proof. First observe that the surjective map $\lambda_n : R_n \twoheadrightarrow R_{n-1}$ restricts to a surjective map $\lambda_n : R_n^\times \twoheadrightarrow R_{n-1}^\times$, by Lemma 1.1.4. Let $x = (x_1, x_2, \ldots) \in (\varprojlim_i R_i)^\times$, i.e., there exists $y = (y_1, y_2, \ldots) \in (\varprojlim_i R_i)^\times$ such that $xy = (x_1y_1, x_2y_2, \ldots) = (1, 1, \ldots) \in (\varprojlim_i R_i)^\times$. Therefore, we have $x_iy_i = 1 \in R_i^\times$. To show that $x \in \varprojlim_i R_i^\times$, we need to check that $\lambda_n(x_n) = x_{n-1}$ for all n, but this is clear by the definition of λ_n and the fact that $\lambda_n(R_n^\times) = R_{n-1}^\times$. Therefore, $(\varprojlim_i R_i)^\times \subseteq \varprojlim_i R_i^\times$. For the converse, suppose $x = (x_1, x_2, \ldots) \in \varprojlim_i R_i^\times$, i.e., for each $x_i \in R_i$, there exists a $y_i \in R_i$ such that $x_iy_i = 1$. We need to exhibit an inverse for x in $\varprojlim_i R_i$. Consider the element $y = (y_1, y_2, \ldots)$, then since $x_ny_n = 1$ for all n, we have $\lambda_n(x_ny_n) = 1 = x_{n-1}y_{n-1}$ for all n. Thus, $\lambda_n(x_ny_n) - x_{n-1}y_{n-1} = \lambda_n(x_n)\lambda_n(y_n) - \lambda_n(x_n)y_{n-1} = \lambda_n(x_n)[\lambda_n(y_n) - y_{n-1}] = 0$. Since $\lambda_n(x_n) = x_{n-1}$ is a unit in R_{n-1}, it follows that $\lambda_n(y_n) - y_{n-1} = 0$, i.e., $\lambda_n(y_n) = y_{n-1}$, yielding $y \in \varprojlim_i R_i$. Thus, y is an inverse for x, and so $x \in (\varprojlim_i R_i)^\times$, which gives $(\varprojlim_i R_i)^\times \supseteq \varprojlim_i R_i^\times$.

Definition 1.1.9. A polynomial $f \in \mathcal{O}[x]$ is called ***primitive*** if $|f| := \max |a_i| = 1$ (this absolute value is actually the Gauss valuation discussed in Corollary 1.3.1.1).

Theorem 1.1.6 (Hensel's Lemma, second version)**.** *Let $f \in \mathcal{O}[x]$ be a primitive polynomial which admits modulo the maximal ideal $\mathfrak{p}$ a factorisation $\overline{f(x)} = \overline{g(x)}\ \overline{h(x)}$ into relatively prime polynomials $\overline{g(x)}, \overline{h(x)} \in (\mathcal{O}/\mathfrak{p})[x]$. Then, f admits a factorisation $f(x) = g(x)h(x)$ where $g(x), h(x) \in \mathcal{O}[x]$ such that deg$(\overline{g})$ = deg(g) and $g \equiv \overline{g} \mod \mathfrak{p}$, $h \equiv \overline{h} \mod \mathfrak{p}$.*

Proof. Let $d = \deg(f), m = \deg(\overline{g})$. Then, $\deg(\overline{h}) \leq d - m$. Let g_0, h_0 be degree-preserving lifts of $\overline{g(x)}, \overline{h(x)}$ to $\mathcal{O}[x]$. Since $\overline{g(x)}, \overline{h(x)} \in (\mathcal{O}/\mathfrak{p})[x]$ are relatively prime, there exist polynomials $\overline{a}, \overline{b} \in (\mathcal{O}/\mathfrak{p})[x]$ such that $\overline{a(x)}\ \overline{g(x)} + \overline{b(x)}\ \overline{h(x)} = 1$, i.e., $ag_0 + bh_0 \equiv 1 \mod \mathfrak{p}$, where a, b are degree-preserving lifts of $\overline{a(x)}, \overline{b(x)}$ to $\mathcal{O}[x]$. Consider now the coefficients of $f - g_0h_0$ and $ag_0 + bh_0 - 1 \in \mathfrak{p}[x]$; pick one with maximum absolute value (minimum valuation) and call it π. Then, $\pi \in \mathfrak{p} \implies |\pi| < 1 \iff v(\pi) \geq 0$.

Construct sequences of polynomials $g_n(x)$ and $h_n(x)$ of the form $g_n(x) = g_0 + p_1\pi + \cdots + p_n\pi^n$ and $h_n(x) = h_0 + q_1\pi + \cdots + q_n\pi^n$ where $\deg(p_i) < m$ and $\deg(q_i) \leq d - m$, such that $f \equiv g_{n-1}h_{n-1} \mod \pi^n\mathcal{O}$ for all $n \in \mathbb{N}$. We do this by induction on n. For $n = 1$, we need to show $f \equiv g_0h_0 \mod \pi\mathcal{O}$, which is equivalent to $f - g_0h_0 \in \pi\mathcal{O} \iff |f - g_0h_0| \leq |\pi|$, which is true by the choice of π. We now assume the congruence for for some $n > 1$ and show it for $n+1$. Hence, $f \equiv g_{n-1}h_{n-1} \mod \pi^n\mathcal{O}$. Note that $g_n = g_{n-1} + p_n\pi^n$ and $h_n = h_{n-1} + q_n\pi^n$, therefore, $g_nh_n = g_{n-1}h_{n-1} + (p_nh_{n-1} + q_ng_{n-1})\pi^n + p_nq_n\pi^{2n} \equiv g_{n-1}h_{n-1} + (p_nh_{n-1} + q_ng_{n-1})\pi^n \mod \pi^{n+1}\mathcal{O}$. Hence, $f - g_nh_n \equiv f - (g_{n-1}h_{n-1} + (p_nh_{n-1} + q_ng_{n-1})\pi^n) \mod \pi^{n+1}\mathcal{O}$. We are done if we can show $f - g_{n-1}h_{n-1} \equiv (p_nh_{n-1} + q_ng_{n-1})\pi^n \mod \pi^{n+1}\mathcal{O}$, which is true if we have $\pi^{-n}(f - g_{n-1}h_{n-1}) := f_n \equiv p_nh_{n-1} + q_ng_{n-1} \mod \pi.\mathcal{O}$. We now focus our attention on finding p_n and q_n that satisfy the above congruence. It is clear that $g_{n-1} \equiv g_0 \mod \pi\mathcal{O}$ and $h_{n-1} \equiv h_0 \mod \pi\mathcal{O}$, therefore we have $f_n \equiv p_nh_{n-1} + q_ng_{n-1} \equiv p_nh_0 + q_ng_0 \mod \pi\mathcal{O}$. Since $a_0f_0 + b_0h_0 = 1 \mod \pi\mathcal{O}$, we have $a_0g_0f_n + b_0h_0f_n \equiv f_n \mod \pi\mathcal{O}$. We might try putting $p_n = bf_n$ and $q_n = af_n$, but the degrees of p_n and q_n might be larger than m and $d-m$, respectively. Therefore. we divide bf_n by g_0 and write $bf_n = qg_0 + p_n$, where $\deg(p_n) < \deg(g_0) = m$. Since $g_0 \equiv \overline{g} \mod p$ and $\deg(g_0) = \deg(\overline{g})$, the highest coefficient of g_0 is not in $\mathfrak{p}$ and hence is a unit. Therefore $|g_0| = \max\{|\text{coeffs of } g_0|\} \geq 1$, *i.e.*, $g_0 \in \mathcal{O}[x]$. Thus $a_0g_0f_n + b_0h_0f_n \equiv f_n \mod \pi\mathcal{O}$ gives us $f_n \equiv a_0g_0f_n + h_0q_n + h_0p_n = g_0(af_n + h_0q) + h_0p_n \mod \pi\mathcal{O}$. Let $q_n = af_n + h_0q \mod \pi\mathcal{O}$, then $f_n = g_0q_n + h_0p_n \mod \pi\mathcal{O}$. Since $\deg(f_n) \leq d$, $\deg(g_0) = m$ and $\deg(h_0p_n) < d - m + m = d$, we have $\deg(q_n) \leq d - m$. Hence, we have successfully constructed the sequences $g_n(x)$ and

$h_n(x)$ with $\deg(p_i) < m$ and $\deg(q_i) \leq d - m$, such that $f \equiv g_{n-1}h_{n-1} \mod \pi^n\mathcal{O}$ for all $n \in \mathbb{N}$.

Claim: A Cauchy sequence $(t_n(x))_n$ of bounded degree converges in $\mathcal{O}[x]$.

Let $t_n(x) = a_{n,0} + a_{n,1}x + \cdots + a_{n,l}x^l$, where $a_{n,l}$ can be zero. Fix any j and consider the sequence $(a_{n,j})_n \subset \mathcal{O}$. This is Cauchy because $|a_{n+1,j} - a_{n,j}| < |t_{n+1}(x) - t_n(x)| < \varepsilon$, since $(t_n(x))_n$ is Cauchy. The inequality above holds because $|f(x)| = \max\{|a_i|\}$ for any polynomial $f(x)$. Since K is complete, $(a_{n,j})_n$ converges to some $a_j \in K$. Therefore, $|a_{n,j} - a_j| < \varepsilon \ \forall n \geq n_0$. Moreover, $(a_{n,j})_n \subset \mathcal{O} \implies |a_{n,j}| \leq 1 \ \forall n \implies \lim_{n\to\infty} |a_{n,j}| \leq 1 \implies |a_j| \leq 1 \implies a_j \in \mathcal{O}$. We will show that $(t_n(x))_n \to t(x) := a_0 + a_1x + \cdots + a_lx^l \in \mathcal{O}[x]$. Consider $|t_n(x) - t(x)| =$

$$\left|(a_{n,0} + a_{n,1}x + \cdots + a_{n,l}x^l) - (a_0 + a_1x + \cdots + a_lx^l)\right| = \max_j\{|a_{n,j} - a_j|\} < \varepsilon$$

Thus, $t_n(x) \to t(x) \in \mathcal{O}[x]$.We will show $(g_n(x))_n$ and $(h_n(x))_n$ are Cauchy and of bounded degree, then apply the claim. Recall that $g_n = g_{n-1} + p_n\pi^n$ and $h_n = h_{n-1} + q_n\pi^n$. Thus $|g_n - g_{n-1}| = |p_n\pi^n| = |\pi|^n|p_n|$. Now, $\pi \in \mathfrak{p} \implies |\pi| < 1$, hence there exists $m_0 \in \mathbb{N}$ such that $\forall\, n \geq m_0$, $|g_n - g_{n-1}| = |\pi|^n|p_n| < \varepsilon$. Hence, $(g_n)_n$ is Cauchy. Similarly, $(h_n)_n$ is also Cauchy. Now, $\deg(g_n) = \deg(g_0 + p_1\pi + \cdots + p_n\pi^n)$, where $\deg(g_n) = m$, $\deg(p_i) < m \implies \deg(g_n) \leq m$. Similarly, $\deg(h_n) = \deg(h_0 + q_1\pi + \cdots + q_n\pi^n)$, where $\deg(h_n) \leq d - m$, and $\deg(q_i) \leq d - m \implies \deg(h_n) \leq d - m$. Therefore, $(g_n)_n$ and $(h_n)_n$ are Cauchy sequences of polynomials of bounded degree, hence they converge to say $g, h \in O[x]$.

Now, we had proven $f \equiv g_nh_n \mod \pi^nO \ \forall n$, i.e., $f - g_nh_n \in \pi^nO \implies |f - g_nh_n| \leq |\pi|^n \ \forall n$. Thus $\lim_{n\to\infty}|f - g_nh_n| \leq \lim|\pi|^n = 0$ and $|f - \lim g_nh_n| \leq 0 \implies |f - gh| \leq 0 \implies f = gh$. Therefore, we are done if we show that g, h reduce to $\overline{g}, \overline{h}$ mod $\mathfrak{p}$ respectively. Now, $g_n \equiv g_0 \mod \pi^n \ \forall n$, i.e., $|g_n - g_0| \leq |\pi|^n \ \forall n$. Thus $\lim|g_n - g_0| \leq \lim(|\pi|^n) = 0 \implies |g - g_0| \leq |\pi| < 1$, i.e., $g - g_0 \in \mathfrak{p} \implies g \equiv g_0 \equiv \overline{g}$ mod $\mathfrak{p}$. Similarly, $h \equiv h_0 \equiv \overline{h} \mod \mathfrak{p}$. This finishes the proof of Hensel's Lemma.

Corollary 1.1.6.1. *Let K be complete with a non-archimedean valuation $|\cdot|$. Then, for every irreducible polynomial $f(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$ with $a_n \neq 0$, we have $|f| = \max\{|a_0|, |a_n|\}$. In particular, $a_n = 1$ and $a_0 \in \mathcal{O} \implies f \in \mathcal{O}[x]$.*

Proof. We first assume $|f| = 1$ and prove the theorem. Now, if $\max\{|a_0|, |a_n|\} = 1$, then $|a_i| \leq 1 \ \forall i \in \mathbb{N}, a_i \in \mathcal{O}$ and $f \in \mathcal{O}[x]$. Let a_r be the first coefficient of f with $|a_r| = 1$. Then,

$$\begin{aligned} f(x) &= a_0 + a_1x + \cdots + a_rx^r + \cdots + a_nx^n \\ &\equiv a_rx^r + a_{r+1}x^{r+1} + \cdots + a_nx^n \pmod{\mathfrak{p}}. \end{aligned}$$

Now $|a_i| < 1 \implies a_i \in \mathfrak{p}$, and we have $a_0 + a_1x + \cdots + a_{r-1}x^{r-1} \equiv 0 \pmod{\mathfrak{p}}$. Thus, $f(x) = x^r(a_r + a_{r+1}x + \cdots + a_nx^{n-r}) \pmod{\mathfrak{p}}$. Note that we have $|f| = \max\{|a_i|\} = 1$. If $\max_i\{|a_0|, |a_n|\} = 1$, then we are done. Suppose not, i.e., $\max_i\{|a_0|, |a_n|\} < 1$, then $0 < r < n$ and f is reducible mod $p \implies f$ is reducible in $\mathcal{O}$ by Hensel's Lemma. This is a contradiction as f was chosen to be irreducible. Therefore, $\max\{|a_0|, |a_n|\} = 1$, i.e., $|f| = \max\{|a_0|, |a_n|\}$.

Now, for the general case, suppose $|f| = \alpha \in \mathbb{R}$, then $|\frac{1}{\alpha}f| = 1$ and so by the above argument we have $\frac{1}{\alpha}|f| = |\frac{1}{\alpha}f| = \max\{|\frac{1}{\alpha}a_0|, |\frac{1}{\alpha}a_n|\} = \frac{1}{\alpha}\max\{|a_0|, |a_n|\}$., whence it follows that $|f| = \max\{|a_0|, |a_n|\}$.

Lemma 1.1.6. *Let K be complete with respect to the non-Archimedean valuation $|\cdot|$ and L/K be an algebraic extension. Let $\mathcal{O}$ be the valuation ring and $\mathcal{O}_L$ be its integral closure in L. Then, we have $\mathcal{O}_L = \{\alpha \in L \mid N_{L/K}(\alpha) \in \mathcal{O}\}$.*

Proof. **Claim:** $\mathcal{O} = \mathcal{O}_L \cap K$: The containment $\mathcal{O} \subseteq \mathcal{O}_L \cap K$ is immediate. For the reverse containment, let $\alpha \in \mathcal{O}_L \cap K$, then α is integral over $\mathcal{O}$. But $\alpha \in K$ and $\mathcal{O}$ is integrally closed (in its field of fractions K), therefore $\alpha \in \mathcal{O}$. Take any $\alpha \in \mathcal{O}_L$, such that $a_0 + a_1\alpha^1 + \cdots + a_{n-1}\alpha^{n-1} + \alpha^n = 0$, where $a_i \in \mathcal{O}$. Now, $N_{L/K}(\alpha) = \prod_\sigma \sigma(\alpha)$, where σ varies over the distinct K–embeddings $L \hookrightarrow \overline{K}$. Since $\alpha \in \mathcal{O}_L$, $\sigma(\alpha) \in \mathcal{O}_L$ for all $\sigma L \hookrightarrow \overline{K}$. Therefore, $N_{L/K}(\alpha) \in \mathcal{O}_L$ and from definition, we know $N_{L/K}(\alpha) \in K$. Thus, by claim, $N_{L/K}(\alpha) \in \mathcal{O}$. This gives $\mathcal{O}_L \subseteq \{\alpha \in L \mid N_{L/K}(\alpha) \in \mathcal{O}\}$. Conversely, if $\alpha \in L^\times$ and $N_{L/K}(\alpha) \in \mathcal{O}$, consider the minimal polynomial of α over K, $m_K^\alpha(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0 \in K[x]$. Then, by transitivity of the norm, we have $N_{L/K}(\alpha) = N_{K(\alpha)/K} \circ N_{L/K(\alpha)}(\alpha) = N_{K(\alpha)/K}((-1)^d a_0) = ((-1)^d a_0)^m = (-1)^n a_0^m \in \mathcal{O}$, where $m = [L : K(\alpha)]$ and $md = n$. Now, $(-1)^n a_0^m \in \mathcal{O} \implies |a_0|^m \le 1 \implies |a_0| \le 1$, and so $\alpha \in \mathcal{O}$. By the previous corollary, this implies $f(\alpha) \in \mathcal{O}[x] \implies \alpha \in \mathcal{O}$, which gives $\{\alpha \in L \mid N_{L/K}(\alpha) \in \mathcal{O}\} \subseteq \mathcal{O}_L$. Hence, we have $\mathcal{O}_L = \{\alpha \in L \mid N_{L/K}(\alpha) \in \mathcal{O}\}$.

Corollary 1.1.6.2. *Let A be a complete DVR (discrete valuation ring) with field of fractions K and L/K be a finite extension. Any element $\alpha \in L$ is integral over A if and only if $N_{L/K}(\alpha) \in A$*

Proof. Suppose $\alpha \in L$ is integral over A, i.e., α is in the integral closure of A. Since A is a valuation ring of K, it follows from the above lemma that $N_{L/K}(\alpha) \in A$, as required. Conversely, if $N_{L/K}(\alpha) \in A$, then again by the above lemma, it follows that α is in the integral closure of A, which means $\alpha \in L$ is integral over A.

Theorem 1.1.7. *Let K be complete with respect to the valuation $|\cdot|$. Then, $|\cdot|$ may be extended uniquely to a valuation of any given algebraic extension L/K.*

If $[L:K]=n$, then it is given by $|\alpha|_L := |N_{L/K}(\alpha)|^{1/n}$, equivalently, in additive notation by $v_L(\alpha) := \dfrac{1}{n}v(N_{L/K}(\alpha))$.

Proof. We only prove this for non-Archimedean valuations. For Archimedean valuations, one uses Ostrowski's Theorem and classical analysis. Since every algebraic extension is the union of its finite subextensions, we first show the theorem for a finite extension L/K.

We have to verify that $|\alpha|_L := |N_{L/K}(\alpha)|^{1/n}$ does define a valuation on L:

1. $\underline{|\alpha|_L = 0 \iff \alpha = 0}$ follows from $|\alpha|_L = 0 \iff |N_{L/K}(\alpha)|^{1/n} = 0 \iff |N_{L/K}(\alpha)| = 0 \iff N_{L/K}(\alpha) = 0 \iff \prod_\sigma \sigma(\alpha) = 0 \implies \sigma(\alpha) = 0$ for some $\sigma \implies \alpha = 0$.

2. $\underline{|\alpha\beta|_L = |\alpha|_L|\beta|_L}$ follows since $N_{L/K}$ is multiplicative.

3. $\underline{|\alpha+\beta|_L \leq \max\{|\alpha|_L, |\beta|_L\}}$: we will use Lemma 1.1.4 to prove this. We first show that $|\gamma|_L \leq 1 \implies |\gamma+1|_L \leq 1$. Consider $|\gamma|_L = |N_{L/K}(\gamma)|^{1/n} \leq 1 \iff |N_{L/K}(\gamma)| \leq 1 \iff N_{L/K}(\gamma) \in \mathcal{O} \iff \gamma \in \mathcal{O}_L$ by Lemma 1.1.4. Therefore, since $\gamma \in \mathcal{O}_L$, we also have $\gamma + 1 \in \mathcal{O}_L$, which proves $|\gamma|_L \leq 1 \implies |\gamma+1|_L \leq 1$. This means that $|\gamma+1|_L \leq 1 = \max\{|\gamma|_L, 1\}$. Now, assume $|\alpha|_L \leq |\beta|_L$ without loss of generality and put $\gamma = \alpha/\beta$, then by multiplicativity of $|\cdot|_L$, we have $|\gamma|_L \leq 1$; in this case, we have $|\gamma+1|_L \leq 1 = \max\{|\gamma|_L, 1\}$, i.e., $|\alpha/\beta+1|_L \leq \max\{|\alpha/\beta|_L, 1\}$. Multiplying throughout by $|\beta|_L$ gives $|\alpha+\beta|_L \leq \max\{|\alpha|_L, |\beta|_L\}$, as desired.

   Moreover, the valuation ring associated to $|\cdot|_L$ is the set $\{x \in L : |x|_L = |N_{L/K}(x)|^{1/n} \leq 1\} = \{x \in L : |N_{L/K}(x)| \leq 1\} = \{x \in L : |N_{L/K}(x)| \in \mathcal{O}\} = \mathcal{O}_L$. For uniqueness, suppose there exists another valuation $|\cdot|'_L$ with valuation ring $\mathcal{O}'$. We need only show $\mathcal{O}' = \mathcal{O}_L$. Suppose not, i.e., there exists $\alpha \in \mathcal{O}_L \backslash \mathcal{O}'$. Let $f(x) = a_0 + a_1x + \cdots + x^d$ be the minimal polynomial of α over K, then each $a_i \in \mathcal{O}$. Note that $\alpha \notin \mathcal{O}'$ implies that $\alpha^{-1} \in \mathcal{O}'$, because $\mathcal{O}'$ is a valuation ring. Therefore, α^{-1} is a nonunit in $\mathcal{O}'$ and so belongs to the maximal ideal $\mathcal{M}'$. Now, $f(\alpha) = a_0 + a_1\alpha + \cdots + \alpha^d = 0 \implies \alpha^d = -(a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1}) \implies 1 = -\alpha^{-d}(a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1}) \in \mathcal{M}'$, which is a contradiction. Hence, no such $\alpha \in \mathcal{O}_L \setminus \mathcal{O}'$ exists, i.e., $\mathcal{O}_L \subseteq \mathcal{O}'$. This inclusion is equivalent to saying $|\alpha|_L \leq 1 \implies |\alpha|'_L \leq 1$, i.e., $|\cdot|'_L$ and $|\cdot|_L$ are equivalent.

For the general case, we write $L = \bigcup_n L_n$ where each $[L_n : K]$ is finite. To show the valuation is well-defined, we take $\alpha \in L_n \subset L_m$ (all extensions finite) and show that $|\alpha|_{L_n} = |\alpha|_{L_m}$. Let $[L_n : K] = d$ and $[L_m : L_n] = t$, then we have $[L_m : K] =$

dt. We then $|\alpha|_{L_m} = |N_{L_m/K}(\alpha)|^{1/dt} = |(N_{L_n/K}(\alpha))^t|^{1/dt} = |N_{L_n/K}(\alpha)|^{1/d} = |\alpha|_{L_n}$. Therefore, $|\cdot|_L$ is well-defined for any algebraic extension L/K. ☕

1.2 General Valuations

Definition 1.2.1. We define an ***ordered abelian group*** as an abelian group $(\Gamma, +, 0)$, with a binary relation $\leq$ on Γ such that, for any δ, γ and $\lambda \in \Gamma$, we have:

$$\begin{array}{ll} (1) & \gamma \leq \gamma \\ (2) & \gamma \leq \delta,\ \delta \leq \gamma \implies \gamma = \delta \\ (3) & \gamma \leq \delta,\ \delta \leq \lambda \implies \gamma \leq \lambda \\ (4) & \gamma \leq \delta \text{ or } \delta \leq \gamma \\ (5) & \gamma \leq \delta \implies \gamma + \lambda \leq \delta + \lambda. \end{array}$$

Definition 1.2.2. A subgroup $\Delta \subseteq \Gamma$ is ***convex*** if for any $\gamma \in \Gamma$ satisfying $0 \leq \gamma \leq \delta$ with $\delta \in \Delta$, we have $\gamma \in \Delta$.

Lemma 1.2.1. *The collection of all proper convex subgroups of Γ is linearly ordered by inclusion.*

Proof. Given convex subgroups $A, B \subseteq \Gamma$, if $A \subset B$ or $B \subset A$, we are done. Suppose not; pick $a \in A \setminus B$ and $b \in B \setminus A$ and assume without loss of generality that $0 \leq a, b$ (otherwise we work with $-a$ or $-b$). Now, either $a \leq b$ or $a \geq b$. If $a \leq b$, then by convexity $a \in B$, a contradiction. If $a \geq b$, then by convexity $b \in A$, again a contradiction. ☕

The order type of this collection is called the ***rank*** of Γ. Hence, if there are exactly n proper convex subgroups of Γ, then Γ is of rank n. In particular, if $\{0\}$ is the only proper convex subgroup of Γ, then Γ is of rank 1.

Definition 1.2.3. An ordering $\leq$ of an ordered abelian group Γ is ***Archimedean*** if $\forall \gamma, \varepsilon \in \Gamma$ with $\varepsilon > 0, \exists n \in \mathbb{N}$ such that $\gamma \leq n\varepsilon$.

Lemma 1.2.2. *An Archimedean ordered abelian group Γ has rank 1.*

Proof. We need only show that Γ admits no nontrivial proper convex subgroups. Proceeding by contradiction, suppose $\Delta \subset \Gamma$ is such a subgroup and let $\delta \in \Delta$. Given any $\gamma \in \Gamma, \exists n \in \mathbb{N}$ such that $\gamma \leq n\delta$, since Γ is Archimedean. Since $\delta \in \Delta$, we have $n\delta = \delta + \delta + \cdots + \delta \in \Delta$, by virtue of Δ being a subgroup. Then, by convexity of Δ, we have $\gamma \in \Delta$ i.e., $\Gamma \subseteq \Delta \implies \Gamma = \Delta$. This is the required contradiction, as Δ was assumed to be a proper subgroup. ☕

Lemma 1.2.3. *Every nontrivial subgroup Δ of $(\mathbb{R}, +, 0)$ is Archimedean with respect to the canonical ordering $\leq$ induced from $\mathbb{R}$.*

Proof. Let $\gamma, \varepsilon \in \Delta$, $\varepsilon > 0$. Then, $\gamma, \varepsilon \in \mathbb{R}$ and $\leq$ is Archimedean over $\mathbb{R}$, since $\gamma \leq n\varepsilon$ for $n = \lfloor \gamma/\varepsilon \rfloor + 1$. Now, since Δ is a subgroup and $\varepsilon \in \Delta$, we get $n\varepsilon \in \Delta$. Hence, $\gamma \leq n\varepsilon$ in Δ and so Δ is Archimedean. Therefore, Δ has rank 1, except for $\Delta = \{0\}$.

The converse is also true:

Lemma 1.2.4. *An ordered abelian group Γ of rank 1 is order-isomorphic to a nontrivial subgroup of $(\mathbb{R}, +, 0)$ with the canonical ordering $\leq$ induced from $\mathbb{R}$.*

Proof. We first show that a rank-one ordered group Γ is Archimedean.

Given $\varepsilon \in \Gamma$, $\varepsilon > 0$, consider $\Delta \coloneqq \{\gamma \in \Gamma : -n\varepsilon \leq \gamma \leq n\varepsilon$ for some $n \in \mathbb{N}\}$. Clearly, $0 \in \Delta$ and $-\delta \in \Delta$ whenever $\delta \in \Delta$. Suppose $\delta_1, \delta_2 \in \Delta$, then $\pm\delta_1 \leq n_1$ and $\pm\delta_2 \leq n_2$, implying $\pm(\delta_1 + \delta_2) \leq (n_1 + n_2)\varepsilon$, so $\delta_1 + \delta_2 \in \Delta$. Hence, Δ is a subgroup. Convexity follows because given any $\delta \in \Delta$ and $0 \leq \tau \leq \delta$, we have $\tau \leq \delta \leq n\varepsilon \implies \tau \in \Delta$. Now, $\varepsilon \in \Delta$ and $\varepsilon \neq 0$, but Γ has rank one, i.e., $\Gamma = \Delta$. Therefore, Γ is Archimedean since Δ is (by definition). Fix any positive $\varepsilon \in \Gamma$. For each $\alpha \in \Gamma$, let

$$L(\alpha) = \{m/n \in \mathbb{Q} \mid n > 0, m \leq n\alpha\} \text{ and } U(\alpha) = \{m/n \in \mathbb{Q} \mid n > 0, m \geq n\alpha\}.$$

Recall: A ***Dedekind cut*** is a subset X of $\mathbb{Q}$ such that:

a) $\emptyset \neq X \subseteq \mathbb{Q}$, b) $q \in X, r < q \implies r \in X$, c) X has no largest member.

The real number associated to a Dedekind cut X is given by $x \in \mathbb{R}$ such that $X = \{\gamma \in \mathbb{Q} \mid \gamma \leq x\} = \{m/n \in \mathbb{Q} \mid m \leq nx\}$. In the sequel, we fix any positive $\varepsilon \in \Gamma$. For each $\alpha \in \Gamma$, let $L(\alpha) = \{m/n \in \mathbb{N} \mid n > 0, m\varepsilon \leq n\alpha\}$ and $U(\alpha) = \{m/n \in \mathbb{N} \mid n > 0, m\varepsilon \geq n\alpha\}$.

Claim: For each $\alpha \in \Gamma$, $L(\alpha)$ and $U(\alpha)$ define a Dedekind cut.

Since Γ is ordered, either $m\varepsilon \leq n\alpha$ or $m\varepsilon \geq n\alpha$, i.e., every $m/n \in \mathbb{Q}$ lies in $L(\alpha)$ or $U(\alpha)$; i.e., $L(\alpha) \cup U(\alpha) = \mathbb{Q}$. Clearly, $L(\alpha) \neq \mathbb{Q}$, otherwise $U(\alpha) = \mathbb{Q}$ and $m\varepsilon \leq \alpha$ for all $m \in \mathbb{Z}$, which contradicts the Archimedean property. Similarly, $U(\alpha) \neq \emptyset$. Now, let $m/n \in L(\alpha)$ and $m'/n' \in U(\alpha)$, then $m\varepsilon \leq n\alpha$ and $m'\varepsilon \geq n'\alpha$, hence $mn'\varepsilon \leq n'n\varepsilon = nn'\alpha \leq nm'\varepsilon$, which gives $mn' \leq m'n \implies m/n \leq m'/n'$, i.e., for all $\beta \in L(\alpha)$ and $\beta' \in U(\alpha)$, we have $\beta \leq \beta'$. Consider $q \in L(\alpha)$, i.e., $q\varepsilon \leq \alpha$, hence for every $r < q$, we have $r\varepsilon \leq q\varepsilon \leq \alpha \implies r \in L(\alpha)$. Thus, $L(\alpha)$ is a Dedekind cut. Let its associated real number be $r(\alpha)$. Consider the map $\Gamma \to (\mathbb{R}, +, 0) : \alpha \mapsto r(\alpha)$. Clearly, $\alpha \leq \beta \implies L(\alpha) \subseteq L(\beta) \implies r(\alpha) \leq r(\beta)$.

Claim: This map is a group monomorphism.

For $\alpha, \beta \in \Gamma$, let $m/n \in L(\alpha)$ and $m'/n' \in L(\beta)$. Thus, $m/n \leq \alpha/\varepsilon$ and $m'/n' \leq \beta/\varepsilon$. Now, we have $m'/n' \leq \beta/\varepsilon$ if and only if $m'n/n' \leq \beta/\varepsilon$ and similarly, $m/n \leq \alpha/\varepsilon$ if and only if $mn'/nn' \leq \alpha/\varepsilon$. Thus, after replacing m by mn' and m' by $m'n$, we get the same denominators. Hence, we may assume $n = n'$ without loss of generality. Thus, $m\varepsilon \leq n\alpha$ and $m'\varepsilon \leq n\beta$, which implies $(m+m')\varepsilon \leq n(\alpha+\beta)$, i.e., $(m+m')/n \in L(\alpha+\beta)$. Hence, $r(\alpha+\beta) \geq r(\alpha)+r(\beta)$. Similarly, $U(\alpha)+U(\beta) \subseteq U(\alpha+\beta)$ implies $r(\alpha+\beta) \leq r(\alpha)+r(\beta)$, i.e., $r(U(\alpha+\beta)) = r(U(\alpha)) + r(U(\beta))$. Thus, r is a group homomorphism.

Now, take $\alpha \in \ker(r)$, i.e., $0 = r(\alpha) = \sup L(\alpha) = \inf U(\alpha)$. Hence, $-1/n \in L(\alpha)$ and $1/n \in U(\alpha)$ for all $n > 0$. Thus, $-\varepsilon \leq n\alpha \leq \varepsilon$ for all $n > 0$, which implies $\alpha = 0$, since Γ is Archimedean. Hence r has trivial kernel, and this proves the claim.

Since we have an order-preserving group monomorphism $\Gamma \hookrightarrow \mathbb{R}$, Γ is order-isomorphic to a nontrivial subgroup, namely its image, of $(\mathbb{R}, +, 0)$ with the canonical ordering $\leq$ induced from $\mathbb{R}$.

☕

Hence, combining the previous two lemmas, we obtain:

Proposition 1.2.1. *An ordered abelian group Γ has rank 1 if and only if it is order-isomorphic to a nontrivial subgroup of $(\mathbb{R}, +, 0)$ with the canonical ordering $\leq$ induced from $\mathbb{R}$.* ☕

Lemma 1.2.5. *Let Γ be an ordered abelian group and $\Delta \subseteq \Gamma$ be convex. Then, Γ/Δ can be made an into ordered group by declaring $\gamma + \Delta \leq \gamma' + \Delta$ if and only if $\gamma < \gamma'$ or $\gamma \equiv \gamma' \mod \Delta$.*

Proof. Note that $\Delta \triangleleft \Gamma$ (since Γ is abelian) so Γ/Δ is well-defined as a group. To check the independence of representatives, take $s \equiv \gamma \mod \Delta$ and $\gamma + \Delta < \gamma' + \Delta$. We will show $s + \Delta < s' + \Delta$. Let $s - \gamma \in \Delta$ and $s' - \gamma' \in \Delta$. Now, $\gamma < \gamma'$ implies $-\gamma < -\gamma'$, so $s - \gamma < s' - \gamma' \in \Delta$. Now, $s - \gamma < s' - \gamma'$ implies $-(s - \gamma) < -(s' - \gamma') \in \Delta$, which gives $s' - \gamma' < s - \gamma \in \Delta$. From these two inequalities, we get $(s' - s) + (s' - \gamma') \in \Delta$, implying $s' - s \in \Delta$. Moreover, $s' \equiv \gamma' \mod \Delta$ and $\gamma < \gamma'$, so $s + \Delta < s' + \Delta$. ☕

Given two ordered abelian groups Γ and Δ, we can order the direct product lexicographically as $(r, s) \leq (r', s')$ if and only if $r \leq r'$ or $r = r'$ and $s \leq s'$ for $r \in \Gamma$ and $s \in \Delta$. Clearly, $\{0\} \times \Delta$ is a convex subgroup, which is order isomorphic to Δ.

Definition 1.2.4. Let Γ be an ordered abelian group and ∞ be a symbol satisfying $\infty = \infty + r = r + \infty = \infty + \infty \neq r \in \Gamma$. We define a ***valuation*** v on a field K as a surjective map $v : K \twoheadrightarrow \Gamma \cup \{\infty\}$ such that $\forall x, y \in K$:

i) $v(0) = \infty \iff x = 0$,

ii) $v(xy) = v(x) + v(y)$,

iii) $v(x + y) \geq \min\{v(x), v(y)\}$.

- If $\Gamma = \{0\}$, we call v the *trivial valuation*.
- If Γ has rank 1, we call v a *rank-1 valuation*.
- In general, the rank of v is defined as the rank of the value group $v(K^\times)$.

As earlier, we get $v(1) = 0$, $v(x^{-1}) = -v(x)$, $v(-x) = v(x)$, and $v(x) < v(y) \implies v(x + y) = v(x)$. The set $\mathcal{O}_v := \{x \in K \mid v(x) \geq 0\}$ is a valuation ring of K. The group of units is given by $\mathcal{O}_v^\times = \{x \in K \mid v(x) = 0\}$, and the set of all nonunits $M_v = \{x \in K \mid v(x) > 0\}$ is the unique maximal ideal of $\mathcal{O}_v$. We define the ***residue class field*** of v as $\overline{\mathcal{K}}_v = \mathcal{O}_v/M_v$. If K is a subfield of L and w is a valuation on L, we say w ***extends*** v if $w|_K = v$.

Example 1.5. We define the degree valuation v_∞ on $K[x]$, K a field, as $v_\infty(0) = \infty$ and $v_\infty(f/g) = \deg(g) - \deg(f)$. (Note that we set $v_\infty(K) = 0$.)

Clearly, v_∞ is a valuation. Now, f/g is a unit if and only if $v_\infty(f/g) = 0$, i.e., $\deg(f) = \deg(g)$. Hence, if $f = \sum_{i=0}^n c_i x^i$ with $c_i \in k$ and $c_n \neq 0$, then $f(x)/x^n$ is a unit. Since $K \subseteq \mathcal{O}_{v_\infty}$ and $K \cap \mathcal{M}_{v_\infty} = \{0\}$, we can identify K with its image in the residue class field. Moreover, $\overline{f(x)/x^n} = c_n$ because

$$\frac{f(x)}{x^n} - c_n = \frac{f(x) - c_n x^n}{x^n} = \frac{\sum_{i=0}^{n-1} c_i x^i}{x^n}$$

$$\implies v\left(\frac{f(x)}{x^n} - c_n\right) = n - (n-1) = 1 > 0$$

$$\implies \frac{f(x)}{x^n} - c_n \in \mathcal{M}_v \implies \overline{\frac{f(x)}{x^n}} = \overline{c_n} = c_n.$$

Therefore, $\mathcal{O}_{v_\infty} = \{f/g : \deg(g) \geq \deg(f)\}$ and $\mathcal{M}_{v_\infty} = \{f/g : \deg(g) > \deg(f)\}$. Consider $\overline{0} \neq \overline{f/g} \in \overline{\mathcal{K}_{v_\infty}} = \mathcal{O}_{v_\infty}/\mathcal{M}_{v_\infty}$, i.e., $v_\infty(f/g) = 0$, i.e., $\deg(g) = \deg(f)$. Thus, if $f = \sum_{i=0}^n a_i x^i$ and $g = \sum_{i=0}^n b_i x^i$, then $\overline{f/g} = a_0/b_0$, by the same argument as above, since $f/g = \dfrac{f/x^n}{g/x^n}$. Hence, we have $\overline{\mathcal{K}_{v_\infty}} = \{a/b : a \in K, b \in K^\times\} = K$.

Proposition 1.2.2. *Let $\mathcal{O} \subseteq K$ be a valuation ring of K. There exists a valuation v on K such that $\mathcal{O} = \mathcal{O}_v$.*

Proof. We have $\mathcal{O}^\times \leq K^\times$. Consider $\Gamma = K^\times/\mathcal{O}^\times$ with operation $x\mathcal{O}^\times + y\mathcal{O}^\times := xy\mathcal{O}^\times$. Define a binary relation $\leq$ on Γ by declaring $\overline{x} = x\mathcal{O}^\times \leq y\mathcal{O}^\times = \overline{y}$ if and only if $y/x \in \mathcal{O}$. This makes Γ into an abelian ordered group: for all $\overline{\gamma}, \overline{\delta}, \overline{\lambda} \in \Gamma$, we have:

1. $\overline{\gamma} \leq \overline{\gamma}$ because $\gamma/\gamma = 1 \in \mathcal{O}^\times$.
2. $\overline{\gamma} \leq \overline{\delta}$ and $\overline{\delta} \leq \overline{\gamma}$ implies $\gamma/\delta \in \mathcal{O}$ and $\delta/\gamma \in \mathcal{O} \implies \gamma$ and δ are units, i.e., $\gamma, \delta \in \mathcal{O}^\times \implies \gamma\delta \in \mathcal{O}^\times \implies \overline{\gamma} = \overline{\delta}$.
3. $\overline{\gamma} \leq \overline{\delta}$, $\overline{\delta} \leq \overline{\lambda} \implies \gamma/\delta \in \mathcal{O}$ and $\delta/\lambda \in \mathcal{O} \implies (\gamma/\delta)(\delta/\lambda) = \gamma/\lambda \in \mathcal{O} \implies \overline{\gamma} \leq \overline{\lambda}$.
4. $\overline{\gamma} \leq \overline{\delta}$ or $\overline{\delta} \leq \overline{\gamma}$ because either $\gamma/\delta \in \mathcal{O}$ or $\delta/\gamma \in \mathcal{O}$ (since $\mathcal{O}$ is a valuation ring).
5. $\overline{\gamma} \leq \overline{\delta} \implies \gamma/\delta \in \mathcal{O}$. Now, $\overline{\gamma} + \overline{\lambda} = \overline{\gamma\lambda}$ and $\gamma\lambda/\delta\lambda = \gamma/\delta \in \mathcal{O}$, i.e., $\overline{\gamma\lambda} \leq \overline{\delta\lambda}$, i.e., $\overline{\gamma} + \overline{\lambda} \leq \overline{\delta} + \overline{\lambda}$.

Thus, all axioms of an abelian ordered group hold. We now define a valuation $v(x) := x\mathcal{O}^\times \in \Gamma$, for $x \in K^\times$ and $v(0) := \infty$. Then $v(xy) = v(x) + v(y)$, by definition. If $v(x) \leq v(y)$, then $y/x \in \mathcal{O} \implies (x+y)/x = 1 + y/x \in \mathcal{O}$. Thus, $v(x+y) \geq v(x) = \min\{v(x), v(y)\}$. Hence, v is a well-defined valuation. Furthermore, $\mathcal{O}_v = \{x \in K : v(x) \geq 0\} = \{x \in K : x/1 \in \mathcal{O}\} = \mathcal{O}$.

Now, $\mathcal{M} := \mathcal{O} \setminus \mathcal{O}^\times$ is the unique maximal ideal of $\mathcal{O}$. This is because $\mathcal{O} = \mathcal{O}_v$ and we have already seen in this case that $\mathcal{M}$ (previously called $\mathcal{M}_v$) is the unique maximal ideal of $\mathcal{O} \setminus \mathcal{O}^\times$. We define the ***rank*** of $\mathcal{O}$ as $\operatorname{rank}(\Gamma)$.

Example 1.6. Let $\mathcal{O} = K$. Then, $\mathcal{O}^\times = K^\times$ and $\Gamma = \{0\}$, i.e., $v(x) = 0\ \forall x \neq 0$, and thus v is the trivial valuation. In particular, the only valuation ring of a finite field is the trivial one.

Definition 1.2.5. Two valuations $v_i : K \to \Gamma_i \cup \{\infty\}$ $(i = 1, 2)$ are ***equivalent*** if $\mathcal{O}_{v_1} = \mathcal{O}_{v_2}$.

Proposition 1.2.3. *Two valuations $v_i : K \to \Gamma_i \cup \{\infty\}$ $(i = 1, 2)$ are equivalent if and only if there exists an order-preserving isomorphism $\rho : \Gamma_1 \to \Gamma_2$ such that $\rho \circ v_1 = v_2$.*

$$\begin{tikzcd}
\Gamma_1 \arrow[rr, "\rho"] & & \Gamma_2 \\
& K \arrow[ul, "v_1"] \arrow[ur, "v_2"'] \arrow[u, phantom, "\circ"] &
\end{tikzcd}$$

Proof. $\Longrightarrow$: Note that $v_i : K^\times \to \Gamma_i$ is a surjective group morphism with kernel $\mathcal{O}_{v_i}^\times$; thus it induces an isomorphism $\tau_i : K^\times/\mathcal{O}_{v_i}^\times \xrightarrow{\sim} \Gamma_i$ satisfying $\tau_i(x\mathcal{O}_{v_i}^\times) = v_i(x)$. By hypothesis, $\mathcal{O}_{v_1} = \mathcal{O}_{v_2}$, hence $K^\times/\mathcal{O}_{v_1}^\times \cong K^\times/\mathcal{O}_{v_2}^\times$ by the map $\rho = \tau_2 \circ \tau_1^{-1}$, i.e., $\Gamma_1 \cong \Gamma_2$.

$\Longleftarrow$: If there exists an order-preserving isomorphism $\rho : \Gamma_1 \xrightarrow{\sim} \Gamma_2$, then we have: $\mathcal{O}_{v_1} = \{x \in K \mid v_1(x) \geq 0\} = \{\rho(x) \in K : (\rho \circ v_1)(x) \geq 0\} = \{x \in K : v_2(x) \geq 0\} = \mathcal{O}_{v_2}$, since ρ is an isomorphism.

Hence, valuation rings of K correspond one-to-one to valuations of K up to an order-isomorphism of the value group.

Theorem 1.2.1. *(a) Every nontrivial valuation on $\mathbb{Q}$ is a p-adic valuation for some rational prime p.*

(b) Every nontrivial valuation on $k[x]$, trivial on k, is either the degree valuation v_∞ or a p-adic valuation for some irreducible polynomial $p \in k[x]$.

Proof. Let K be either $\mathbb{Q}$ or $k[x]$ and let v be some nontrivial valuation on K. Then, $\mathcal{O}_v \neq K$. In (b), v is trivial on k, thus $k \subseteq \mathcal{O}_v$. We will write $\mathcal{O}$ instead of $\mathcal{O}_v$ in the sequel.

(a) For any valuation v, $v(1) = v(1)+v(1) \implies v(1) = 0$, i.e., $1 \in \mathcal{O}$, so $\mathbb{Z} \subseteq \mathcal{O}$.

Since $\mathcal{O} \neq \mathbb{Q}$, there exists a prime $p \in \mathcal{M}$. Let $q \neq p$ be another prime, then by Bézout's Lemma, there exist $a, b \in \mathbb{Z}$ such that $ap + bq = 1$. Now, $0 = v(ap+bq) \geq \min\{v(ap), v(bq)\}$. Thus, $v(ap) \geq v(bq)$ since $v(a)+v(b) > 0$ ($\because$ $p \notin \mathcal{M}$ and $a \in \mathbb{Z} \subset \mathcal{O}$). Therefore, $0 \geq v(bq) \implies 0 = v(bq) = v(b) + v(q)$. Since $b \in \mathbb{Z} \subseteq \mathcal{O}$, $v(b) \geq 0$, i.e., $v(q) = -v(b) \leq 0 \implies q \notin \mathcal{M}$. Hence, all primes other than p are units in $\mathcal{O}$. Now, given a/b with $\gcd(a, b) = 1$, we will show $a/b \in \mathcal{O}$ if and only if $p \nmid b$.

Claim: $v(a/b) = v(a) - v(b) \geq 0$ **if and only if** $v(a) \geq v(b)$**.**

Suppose $b = \prod_i q_i^{t_i}$. If $p \nmid b$, then all q_i are units in $\mathcal{O}$. Thus, $v(q_i) = 0$ and so $v(b) = \sum_i t_i v(q_i) = 0$. Thus, $v(a/b) = v(a) - v(b) = v(a) \geq 0$, since $a \in \mathbb{Z}$. Conversely, if $a/b \in \mathcal{O}$, then $v(a) \geq v(b)$. Now, if $p \mid b$, then $v(b) = \sum_{q_j \neq p} t_j v(q_j) + tv(p) = tv(p) > 0$. Thus, $v(a) \geq v(b) \implies v(a) > 0$. Since $\gcd(a, b) = 1$, we have $p \nmid a$, but then, by the same argument, $v(a) = \sum t'_j v(q'_j) = 0$, which is a contradiction. Hence, $p \nmid b$. Therefore, $\mathcal{O} = \mathbb{Z}_{(p)}$ and so v is the p-adic valuation v_p.

(b) If $x \in \mathcal{O}$, then $k[x] \subseteq \mathcal{O}$ and we proceed as in (a), replacing $\mathbb{Z}$ by $k[x]$ and get $v = v_p$ for some irreducible polynomial p. If $x \notin \mathcal{O}$, then $x^{-1} \in \mathcal{O}$

(property of a valuation ring). Consider $v(x^{-1})$. We have $x \notin \mathcal{O} \implies v(x) < 0 \implies -v(x) > 0 \implies v(x^{-1}) > 0$, i.e., $x^{-1} \in \mathcal{M}$. Now, for $0 \leq n < m$, $mv(x) = v(x^m) < v(x^n) = nv(x)$ [since $v(x) < 0$]. Since $v(a) = 0\ \forall a \in k^\times$, we have $v(a_n x^n + \cdots + a_0) = v(a_n x^n)$, because $v\left(\sum_{i=0}^{n-1} a_i x_i\right) \geq \min\{v(a_i x_i)\} = \min\{v(x_i)\}_{i=1}^{n-1}$ and $v(x) < v(y) \implies v(x+y) = v(x)$, (for our case, x corresponds to $a_n x^n$ and y corresponds to $\sum_i^{n-1} a_i x^i$.) Thus, $v(a_n x^n + \cdots + a_0) = v(a_n x^n) = v(a_n) + v(x^n) = v(x^n) = nv(x)$. Hence, for any $a_n x^n + \cdots + a_0 \in k[x]$, we get $v(a_n x^n + \cdots + a_0) = nv(x)$, i.e., $v(k[x]^\times) = \mathbb{Z}v(x)$. Thus, $v(x) \mapsto -1$ gives an isomorphism $v(k[x]^\times) \xrightarrow{\sim} \mathbb{Z}$.

Corollary 1.2.1.1. *Let (K, v) be a complete nonarchimedean real field of characteristic zero with finite residue class field of characteristic q. Then, the restriction of the valuation $v|_{\mathbb{Q}}$ to the rational integers $\mathbb{Q}$ is precisely the q-adic valuation. Moreover, $v(q) = e(K/\mathbb{Q})$, the ramification index (defined more generally in 1.5.2) of this extension.*

Proof. In this case, we provide a different, more algebraic proof of the fact that all rational primes other than q are units in $\mathcal{O}$, as seen in the preceeding theorem.

By the theorem, the restriction $v|_{\mathbb{Q}}$ is an p-adic valuation for some prime p. We will show that $p = q = \mathrm{char}(\mathcal{O}/\mathfrak{p})$. Since the residue class field is finite and of characteristic q, we have a field extension $\mathbb{F}_q = \mathbb{Z}/q\mathbb{Z} \subset \mathcal{O}/\mathfrak{p}$. This is an integral extension and so the maximal ideal $\mathfrak{p}$ contracts to the maximal ideal $q\mathbb{Z}$, i.e., $\mathfrak{p} \cap \mathbb{Z} = q\mathbb{Z}$. Note that since $q \in \mathfrak{p}$, we have $v(q) > 0$. Suppose there exists a rational prime $l \neq q$ which is not a unit, i.e., its extension $l^e \subset \mathfrak{p}$. We contract back to get $l^{ec} \subset \mathfrak{p}^c = q\mathbb{Z}$. We know from commutative algebra that $l\mathbb{Z} \subset l^{ec}$ which yields $l\mathbb{Z} \subset q\mathbb{Z}$, i.e., $q \mid l$, which is a contradiction. Therefore, all rational primes other than q are units in $\mathcal{O}$, and hence $v(l) = 0$ for all primes $l \neq q$ and $v(q) > 0$, which is the characteristic property of the q-adic valuation. Hence, $v|_{\mathbb{Q}} = v_q$.

1.3 Constructing valuations

Theorem 1.3.1. *Suppose K is a field, Γ is an ordered subgroup of an ordered group Γ', and $v : K \to \Gamma \cup \{\infty\}$ is a valuation and $\gamma \in \Gamma'$. For $f = \sum_{i=0}^{\infty} a_i x^i \in K[x]$, define*

$$w(f) := \begin{cases} \infty, & \textit{if } f = 0 \\ \min\limits_{0 \leq i \leq n} \{v(a_i) + i\gamma\}, & \textit{otherwise} \end{cases}$$

For $f, g \in K[x] \setminus \{0\}$, let $w(f/g) = w(f) - w(g)$.

The above equations define a valuation $w : K[x] \to \Gamma' \cup \{\infty\}$ on $K[x]$ that extends v.

Proof. For $f, g \in K[x] \setminus \{0\}$, let $n = \max\{\deg(f), \deg(g)\}$ and $f = \sum_{i=0}^{n} a_i x^i, g = \sum_{j=0}^{n} b_j x^j$. Then, $f + g = \sum_{i=0}^{n} (a_i + b_j) x^i$ and we get

$$\begin{aligned} w(f+g) &= v(a_i + b_i) + i\gamma \geq \min\{v(a_i), v(b_i)\} + i\gamma \\ &= \min\{v(a_i) + i\gamma,\ v(b_i) + i\gamma\} = \min\{w(f), w(g)\}. \qquad (*) \end{aligned}$$

Now,

$$fg = \left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{j=0}^{m} b_j x^j\right) = \sum_{k=0}^{n+m} c_k x^k \text{ where } c_k = \sum_{i+j=k} a_i b_j.$$

For every $i + j = k$, we have $v(a_i b_j) + k\gamma = v(a_i) + v(b_j) + (i+j)\gamma = v(a_i) + i\gamma + v(b_j) + j\gamma \geq \omega(f) + \omega(g)$. Hence, $v(c_k) = v\left(\sum_{i+j=k} a_i b_j\right) \geq \min_{i+j=k}\{v(a_i b_j)\}$. Hence, $v(c_k) + k\gamma \geq \min_{i+j=k}\{v(a_i b_j)\} + k\gamma = \min_{i+j=k}\{v(a_i b_j) + k\gamma\}$.

Therefore, $w(f) + w(g) \leq \min_{i \leq k}\{v(a_i b_i) + k\gamma\} = w(fg)$.

To show the other inequality, let $i_0 = \min\{i : v(a_i) + i\gamma = w(f)\}, j_0 = \min\{v(b_j) + j\gamma = w(g)\}$ and $k_0 = i_0 + j_0$.

Consider

$$c_{k_0} = \sum_{i+j=k_0} a_i b_i = \sum_{i \leq i_0} a_i b_i + a_{i_0} b_{i_0} + \sum_{i \geq i_0} a_i b_i.$$

Note that whenever $i < i_0$, $v(a_i) + i\gamma \geq w(f)$, by definition of i_0.. Hence, in the teal sum, we have

$$\begin{aligned} v(a_i b_j) + k_0\gamma &= v(a_i) + i\gamma + v(b_j) + j\gamma \\ &\geq v(a_i) + i\gamma + w(g) \\ &> w(f) + w(g). \end{aligned}$$

Similarly, in the violet sum,

$$\begin{aligned} v(a_i b_j) + k_0\gamma &= v(a_i) + i\gamma + v(b_j) + j\gamma \\ &\geq w(f) + v(a_j) + j\gamma \\ &> w(f) + w(g) \end{aligned}$$

Hence,

$$v\left(\sum_{i\le i_0} a_ib_i\right) > w(f)+w(g)-k_0 \text{ and } v\left(\sum_{i\ge i_0} a_ib_i\right) > w(f)+w(g)-k_0$$

$$\implies \min\left\{v\left(\sum_{i\le i_0} a_ib_i\right), v\left(\sum_{i\ge i_0} a_ib_i\right)\right\} > w(f)+w(g)-k_0 = v(a_{i_0}b_{i_0}).$$

Recall that $v(x) < v(y) \implies v(x+y) = v(x)$ whence we deduce:

$$v(c_{k_0}) = v\left(\sum_{i\le i_0} a_ib_i + a_{i_0}b_{i_0} + \sum_{i\ge i_0} a_ib_i\right) = v(a_{i_0}b_{i_0}).$$

Therefore, $v(c_{k_0}) + k_0\gamma = v(a_{i_0}b_{i_0}) + k_0\gamma = w(f)+w(g)$ Thus,

$$w(fg) \ge w(f)+w(g) \implies w(fg) = w(f)+w(g) \tag{**}$$

Note that we have proved $(*)$ and $(**)$ for any $f, g \in K[x]\setminus\{0\}$, the polynomial ring, but not for any $f, g \in K(x)\setminus\{0\}$, the rational function field.

The map $w : K[x] \to \Gamma' \cup \{\infty\}$ is well-defined:

If $f_1/g_1 = f_1/g_2$, then $f_1g_2 = f_2g_1$. Thus, $w(f_1g_2) = w(f_2g_1) \implies w(f_1) + w(g_2) = w(f_2) + w(g_1) \implies w(f_1) - w(g_1) = w(f_2) - w(g_2) \implies w(f_1/g_1) = w(f_2/g_2)$. To extend $(*)$ and $(**)$ to $K(x)\setminus\{0\}$, take $h_1, h_2 \in K(x)\setminus\{0\}$. Let g be a common denominator of h_1 and h_2: $h_1 = f_1/g$ and $h_2 = f_2/g$ where $g, f_i \in K[x]\setminus\{0\}$.

Then,

$$\begin{aligned}
w(h_1+h_2) = w\left(\frac{f_1+f_2}{g}\right) &:= w(f_1+f_2) - w(g)\\
&\ge \min\{w(f_1), w(f_2)\} - w(g)\\
&= \min\{w(f_1)-w(g), w(f_2)-w(g)\}\\
&= \min\{w(f_1/g), w(f_2/g)\}\\
&= \min\{w(h_1), w(h_2)\}.
\end{aligned}$$

Similarly,

$$\begin{aligned}
w(h_1h_2) = w\left(\frac{f_1f_2}{g^2}\right) &:= w(f_1)+w(f_2) - 2w(g)\\
&= w(f_1)+w(f_2) - 2w(g)\\
&= w(f_1/g) + w(f_2/g)\\
&= w(h_1) + w(h_2).
\end{aligned}$$

Corollary 1.3.1.1. *Let $v : K \twoheadrightarrow \Gamma \cup \{\infty\}$ be a valuation. There is exactly one extension w of v to $K(x)$ such that $w(x) = 0$ and $\overline{x}$ is transcendental over $\overline{\mathcal{K}}$, the residue class field of v. We have $\overline{K(x)} = \overline{\mathcal{K}}(\overline{x})$ and $w(K(x)^\times) = \Gamma$.*

*This valuation w is called the **Gauss extension** of v.*

Proof. For uniqueness, let $f = \sum_{i=0}^n a_i x^i \in K[x] \setminus \{0\}$. Pick $k \le n$ such that $v(a_k) = \min\limits_{0 \le i \le n} v(a_i)$.

Write $f = a_k \sum_{i=0}^n b_i x^i = a_k g$ where $b_i = a_i/a_k$ and $v(b_i) \ge 0$. Thus, $w(g) = w\left(\sum_{i=0}^n b_i x^i\right) = \min\{w(b_i) + iw(x)\} = \min\{v(b_i)\} \ge 0$. Now, $\overline{g} = \sum \overline{b_i}\overline{x}^i \ne 0$ since $b_k = a_k/a_k = 1$ and $\overline{x}$ is transcendental over $\overline{\mathcal{K}}$. Hence $g \notin \mathcal{M}_w$, i.e., $g \in {\mathcal{O}^\times}_w \implies w(g) = 0 \implies w(f) = w(a_k) + w(g) = v(a_k)$. Thus, $w(f) = \min_{0 \le i \le n} v(a_i)$.

For existence, let $f \in K[x]$ and define $w(f)$ as earlier by taking $\Gamma' = \Gamma$ and $\gamma = 0$. Then, $w(x) = \min\{v(1) + 0\} = 0$.

Claim: $\overline{x}$ is transcendental over $\overline{\mathcal{K}}$.

Suppose, for a contradiction, that $\overline{x}$ is algebraic over $\overline{\mathcal{K}}$. Then, $\exists a_i \in \mathcal{O}_v$ such that $\sum \overline{a_i}\ \overline{x}^i = \sum \overline{a_i x^i} = 0$. Thus, $\sum a_i x^i \in \mathcal{M}_w$, i.e., $w\left(\sum a_i x^i\right) = \min\{v(a_i)\} > 0$, i.e., $v(a_i) > 0\ \forall i \implies \overline{a_i} = 0$, so the only polynomial in $\overline{\mathcal{K}}$ having $\overline{x}$ as a root is the zero polynomial. This proves the claim. Moreover, $w(K(x)^\times) = \Gamma$ because given any $f \in K(x)^\times$, $w(f) = \min\{v(a_i)\} \in \Gamma$, i.e., $w(K(x)^\times) \subseteq \Gamma$. Conversely, for any $t \in \Gamma$, $\exists a \in K^\times$ such that $v(a) = t$, by surjectivity of v. Hence, $\Gamma \subseteq w(K(x)^\times) \implies w(K(x)^\times) = \Gamma$.

Claim: $\overline{K(x)} = \overline{\mathcal{K}}(\overline{x})$.

Let $h \in \mathcal{O}_w^\times$, say $h = f_1/f_2$ with $f_i \in K[x] \setminus \{0\}$. As before, write $f_i = c_i g_i$, $c_i \in K^\times$ and $g_i \in \mathcal{O}_v^\times$. Thus, $h = c_1 g_1 / c_2 g_2 = c \cdot (g_1/g_2)$ where $c = c_1/c_2 \in K^\times$. Moreover, $h, g_1, g_2 \in \mathcal{O}_w^\times \implies c = hg_2/g_1 \in \mathcal{O}_w^\times$, whence we conclude $\overline{h} = \overline{hg_2/g_1} \in \overline{\mathcal{K}}(\overline{x})$. This proves the inclusion $\overline{K(x)} \subset \overline{\mathcal{K}}(\overline{x})$. Conversely, let $\overline{h}(\overline{x}) \in \overline{\mathcal{K}}(\overline{x})$ i.e., $\overline{h} \in \mathcal{O}_w/\mathcal{M}_w \implies h \in \mathcal{O}_w$. Since h is nonzero in $\overline{\mathcal{K}}$, we have $h \notin \mathcal{M}_w \implies h \in \mathcal{O}_w^\times \implies \overline{h} \in \overline{K(x)}$, which yields $\overline{K(x)} \supset \overline{\mathcal{K}}(\overline{x})$.

Corollary 1.3.1.2. *Let $v : K \twoheadrightarrow \Gamma \cup \{\infty\}$, Γ be an ordered subgroup of an ordered group Γ', and $\gamma \in \Gamma'$ has the property that if $n \in \mathbb{Z}$ satisfies $n\gamma \in \Gamma$, then $n = 0$.*

Then, there is exactly one valuation w on $K(x)$ extending v, with $w(x) = \gamma$, and we have $\overline{K(x)} = \overline{\mathcal{K}}$ and $w(K(x)^\times) = \Gamma \oplus \mathbb{Z}\gamma$.

Proof. The existence of w follows from the previous theorem.

For uniqueness, consider an $f \in K[x]$, say $f = \sum_{i=0}^n a_i x^i$, $a_i \in K$. Now, for each $i \le n$, $w(a_i x^i) = v(a_i) + iw(x) = v(a_i) + i\gamma$.

Claim: For $i \ne j$ and $a_i \ne 0 \ne a_j$, $w(a_i x^i) \ne w(a_j x^j)$:

Suppose this is not the case. Then, $w(a_ix^i) = w(a_jx^j) \implies v(a_i) + i\gamma = v(a_j) + j\gamma \implies (i-j)\gamma = v(a_j) - v(a_i)$. Since $i - j \in \mathbb{Z}$ and $(i-j)\gamma \in \Gamma$ we have $i - j = 0 \implies i = j$, a contradiction. Thus, $w(f) = \min_{0\le i\le n}\{w(a_ix^i)\} = \min_{0\le i\le n}\{v(a_i) + i\gamma\}$, which is uniquely determined (by the claim). Hence, w is uniquely determined on $K[x]$ and hence on $K(x)$. Moreover, $w(K(x)^\times) = \Gamma \oplus \mathbb{Z}\gamma$ because given any $f \in K(x)^\times$, $w(f) = \min\{v(a_i)+i\gamma\} \in \Gamma\oplus\mathbb{Z}\gamma$, i.e., $w(K(x)^\times) \subseteq \Gamma \oplus \mathbb{Z}\gamma$. Conversely, for any $t + i\gamma$, there exists $a \in K^\times$ such that $v(a) = t$, and hence $v(ax^i) = t + i\gamma$, so $\Gamma \oplus \mathbb{Z}\gamma \subseteq w(K(x)^\times) \implies w(K(x)^\times) = \Gamma \oplus \mathbb{Z}\gamma$.

Claim: $\overline{K(x)} = \overline{\mathcal{K}}$.

We first show that every $f \in K[x] \setminus \{0\}$ is of the form $f = ax^n(1+u)$ where $a \in K^\times$, $u \in K(x)$, $n \in \mathbb{Z}$, and $w(u) > 0$. For this, write $f = \sum_{i=0}^n a_ix^i$, with $a_i \in K$. Now, $\exists!\ i_0$ such that

$$w(f) = \min_{0\le i\le n}\{w(a_ix^i)\} = w(a_{i_0}x^{i_0}) = v(a_{i_0}) + i_0\gamma.$$

Thus, $f = a_{i_0}x^{i_0}\left(\sum_{i\neq i_0}^n \frac{a_ix^i}{a_{i_0}x^{i_0}} + 1\right) =: a_{i_0}x^{i_0}u$. Now, $w\left(\frac{a_ix^i}{a_{i_0}x^{i_0}}\right) = w(a_ix^i) - w(a_{i_0}x^{i_0}) > 0$ for $i \neq i_0$, hence $w(u) = w\left(\sum_{i\neq i_0}^n \frac{a_ix^i}{a_{i_0}x^{i_0}} + 1\right) = w\left(\sum_{i\neq i_0}^n \frac{a_ix^i}{a_{i_0}x^{i_0}}\right) \geq \min_{i\neq i_0}\left\{w\left(\frac{a_ix^i}{a_{i_0}x^{i_0}}\right)\right\} > 0$, whence, $w(u) > 0$.

Second, we consider any $h \in K(x) \setminus \{0\}$, and write $h = f/g$, with $f, g \in K[x] \setminus \{0\}$.Write $f = ax^m(1+u)$ and $g = bx^n(1+u')$, with $a, b \in K^\times$, $m, n \in \mathbb{N}$, and $w(u), w(u') > 0$. Then $h = \frac{f}{g} = \frac{a}{b}(x^{m-n})\left(\frac{1+u}{1+u'}\right) = cx^r\left(1 + \frac{u-u'}{1+u'}\right)$, where $c = a/b \in K^\times$ and $r = m - n \in \mathbb{Z}$. Since $w(u') > 0$, $w(1+u') = 0$; therefore $w(u - u'/1+u') = w(u-u') - w(1+u') = w(u-u') > 0$. By the same argument as before, there exists $u'' \in K(x)$ with $w(u'') > 0$ such that $h = cx^r(1+u'')$.

We now show that $K(x) = \overline{\mathcal{K}}(\overline{x})$. Let $h \in \mathcal{O}_w^\times$ and write $h = cx^r(1+u'')$ as described above. We then have $0 = w(h) = w(cx^r(1+u'')) = v(c) + r\gamma$, whence $r\gamma = -v(c) \in \Gamma$. By assumption, $r = 0$. Consequently, $v(c) = 0$. Note that $\overline{u''} = 0$ since $w(u'') > 0$, hence it follows $\overline{h} = \overline{c}(1 + \overline{u''}) = \overline{c} \in \overline{\mathcal{K}}$.

1.4 Dependence and Topology of Valuations

Definition 1.4.1. Two valuation rings $\mathcal{O}_1, \mathcal{O}_2 \subseteq K$ are ***dependent*** if $\mathcal{O}_1\mathcal{O}_2 \neq K$, where $\mathcal{O}_1\mathcal{O}_2$ denotes the smallest subring of K containing both $\mathcal{O}_1, \mathcal{O}_2$.

We also define the ***dependence class of*** $\mathcal{O}$ as

$$[\mathcal{O}] := \Big\{\mathcal{O}' \subseteq K : \mathcal{O}' \text{ is a nontrivial valuation ring dependent on } \mathcal{O}\Big\}.$$

Lemma 1.4.1. *Every overring of a valuation ring is also a valuation ring.*

Proof. If $\mathcal{O} \subseteq \mathcal{O}'$ and $\mathcal{O}$ is a valuation ring, then $\forall x \in K$, $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$, i.e., $x \in \mathcal{O}'$ or $x^{-1} \in \mathcal{O}'$. ☕

Such an overring $\mathcal{O}'$ of $\mathcal{O}$ is called a ***coarsening*** of $\mathcal{O}$. Two dependent valuation rings $\mathcal{O}_1, \mathcal{O}_2 \subseteq K$ always have a *lowest common coarsening*, namely $\mathcal{O}_1\mathcal{O}_2$.

Lemma 1.4.2. *The set of overrings $\mathcal{O}'$ of $\mathcal{O}$ in K is linearly ordered by inclusion.*

Proof. Suppose $\mathcal{O}_1$ and $\mathcal{O}_2$ are overrings of $\mathcal{O}$ in K. If $\mathcal{O}_1 \subseteq \mathcal{O}_2$, we are done. Suppose not. Let $a \in \mathcal{O}_1 \setminus \mathcal{O}_2$ and $b \in \mathcal{O}_2$. Now, $a/b \notin \mathcal{O}$, otherwise $a/b \in \mathcal{O} \subseteq \mathcal{O}_2 \implies a = b(a/b) \in \mathcal{O}_2$, but $a \notin \mathcal{O}_2$. Since $\mathcal{O}$ is a valuation ring, $(a/b)^{-1} = b/a \in \mathcal{O} \subseteq \mathcal{O}_1$. Hence, $b = a(b/a) \in \mathcal{O}_1$, i.e., $\mathcal{O}_2 \subseteq \mathcal{O}_1$.

☕

Theorem 1.4.1. *Overrings $\mathcal{O}'$ of $\mathcal{O}$ correspond one-to-one with prime ideals of $\mathcal{O}$.*

Proof. Let $\mathcal{O}$ be a fixed nontrivial valuation ring of K and $\mathcal{O}' \subseteq K$ be an overring. Then, $\mathcal{O} \subseteq \mathcal{O}' \implies \mathcal{M}' \subseteq \mathcal{M}$ because if $x \in \mathcal{M}'$, then $x^{-1} \notin \mathcal{O}'$, hence $x^{-1} \notin \mathcal{O}$, and so $x \in \mathcal{M}$. Note that $\mathcal{M}$ consists exactly of non-units of $\mathcal{O}$. Now, $\mathcal{M}'$ is prime in $\mathcal{O}'$, i.e., $\mathcal{M}'\mathcal{O} \subseteq \mathcal{M}'$. Since $\mathcal{O} \subseteq \mathcal{O}'$, we have $\mathcal{M}'\mathcal{O} \subseteq \mathcal{M}'$, i.e., $\mathcal{M}'$ is also prime in $\mathcal{O}$. Here, given an overring $\mathcal{O}' \supseteq \mathcal{O}$, we have a prime ideal $M' \lhd \mathcal{O}$.

Conversely, if $\mathfrak{p}$ is a prime ideal of $\mathcal{O}$, then $\mathcal{O}_\mathfrak{p} = \{a/b : a \in \mathcal{O}, b \notin \mathfrak{p}\}$ is an overring of $\mathcal{O}$ with maximal ideal $\mathfrak{p}\mathcal{O}_\mathfrak{p}$.

Claim: The correspondence is one-to-one, i.e., $\mathcal{O}_{M'} = \mathcal{O}'$ and $\mathfrak{p}\mathcal{O}_\mathfrak{p} = \mathfrak{p}$.

We need to show that every $x \in \mathcal{O}'$ is of the form a/b, $a \in \mathcal{O}$ and $b \notin \mathcal{M}'$. If $x \in \mathcal{O}$, then $x = x/1$ and we are done. Suppose not. Then, $x^{-1} \in \mathcal{O}$ so $x^{-1} \in \mathcal{M} - \mathcal{M}'$ (since $\mathcal{M}'$ consists of non-units of $\mathcal{O}'$). Thus, $x = 1/x^{-1}$ and we are done. Hence, $\mathcal{O}' \subseteq \mathcal{O}_{\mathcal{M}'}$. Now, let $a/b \in \mathcal{O}_{\mathcal{M}'}$, i.e., $a \in \mathcal{O}$ and $b \notin \mathcal{M}'$, so b is a unit in $\mathcal{O}'$,i.e., $b^{-1} \in \mathcal{O}'$. Hence, $a/b = ab^{-1} \in \mathcal{O}' \implies \mathcal{O}_{\mathcal{M}'} \subseteq \mathcal{O}$. Therefore, $\mathcal{O}_{\mathcal{M}'} = \mathcal{O}'$. Now, given $a/b \in \mathfrak{p}\mathcal{O}_\mathfrak{p}$, we have $a \in \mathfrak{p}$ and $b \notin \mathfrak{p}$. Since $\mathfrak{p} \subseteq \mathcal{M}$, $b \notin \mathcal{M}$, i.e., b is a unit in $\mathcal{O}$. Hence, $b^{-1} \in \mathcal{O}$, so $a/b = ab^{-1} \in \mathfrak{p}$ ($\mathfrak{p}$ is prime and $a \in \mathfrak{p}$). Thus, $\mathfrak{p}\mathcal{O}_\mathfrak{p} \subseteq \mathfrak{p}$. Given $a \in \mathfrak{p}$, $a = a/1 \in \mathfrak{p}\mathcal{O}_\mathfrak{p}$, so $\mathfrak{p} \subseteq \mathfrak{p}\mathcal{O}_\mathfrak{p}$. Hence, $\mathfrak{p}\mathcal{O}_\mathfrak{p} = \mathfrak{p}$. Therefore, the correspondence is one-to-one. ☕

Remark 1.5. If $\mathcal{O}' = K$, then $\mathcal{M}'$ is trivial and we have $K = \mathcal{O}_{(0)} = \{a/b : a \in \mathcal{O}, b \neq 0\}$, which is the quotient field of $\mathcal{O}$. Therefore, K is the quotient field for every valuation ring of K.

Lemma 1.4.3. *Let $\mathcal{O}$ be a nontrivial valuation ring of K corresponding to the valuation $v : K \longrightarrow \Gamma \cup \{\infty\}$. Then, there is a one-to-one correspondence of convex subgroups $\Delta \subseteq \Gamma$ with prime ideals $\mathfrak{p}$ of $\mathcal{O}$, and hence with overrings $\mathcal{O}_{\mathfrak{p}} \supseteq \mathcal{O}$.*

This correspondence is given by

$$\begin{aligned} \Delta &\mapsto \mathfrak{p}_\Delta := \{\, x \in \mathcal{O} : v(x) \notin \Delta \,\}, \\ \mathfrak{p} &\mapsto \Delta_{\mathfrak{p}} := \{\gamma \in \Gamma : \gamma = v(x) \text{ or } v(x^{-1}) \text{ for some } x \in \mathcal{O} \setminus \mathfrak{p}\}. \end{aligned}$$

In particular, if $\mathcal{O}$ has finite rank, then this rank coincides with the Krull dimension of $\mathcal{O}$.

Proof. Consider $\Delta \mapsto \mathfrak{p}_\Delta$. Now, $\mathfrak{p}_\Delta \lhd \mathcal{O}$ since $\forall t \in \mathcal{O}$ and $x \in \mathfrak{p}_\Delta$, we have $v(xt) = v(x) + v(t) \geq v(x) \notin \Delta \implies v(xt) \notin \Delta$ (by convexity ofΔ). To show $\mathfrak{p}_\Delta$ is prime, consider $xy \in \mathfrak{p}_\Delta$, i.e. $v(xy) = v(x) + v(y) \notin \Delta$. If $x \in \mathfrak{p}_\Delta$ or $y \in \mathfrak{p}_\Delta$, we are done. Suppose not. Then $v(x) \in \Delta$ and $v(y) \in \Delta$. Thus, $v(xy) = v(x) + v(y) \in \Delta$(by convexity), a contradiction. Hence, $\mathfrak{p}_\Delta$ is a prime ideal. To show that $\Delta_{\mathfrak{p}}$ is convex, we take $0 \leq \gamma \leq \delta$ with $\delta \in \Delta_{\mathfrak{p}}$. Since v is surjective, we have $\gamma = v(y)$ for some $y \in K$ but since $0 \leq \gamma$, it must be the case that $y \in \mathcal{O}$. This already gives that $\gamma \in \Delta_{\mathfrak{p}}$. Hence, convexity of $\Delta_{\mathfrak{p}}$ follows. Moreover, by definition, we have $\Delta_{\mathfrak{p}} = -\Delta_{\mathfrak{p}}$, hence we need only prove closure under addition to ensure that $\Delta_{\mathfrak{p}}$ is a subgroup. Let $\gamma, \delta \in \Delta_{\mathfrak{p}}$. We may assume without loss of generality that $0 \leq \gamma \leq \delta$, otherwise we work with $-\gamma$ or $-\delta$ as required. Then, we have $\gamma = v(x)$ and $\delta = v(y)$ for some $x, y \in \mathcal{O} \setminus \mathfrak{p}$. Consider now $\gamma + \delta = v(x) + v(y) = v(xy)$. Since $\mathfrak{p}$ is prime in $\mathcal{O}$, we have $x, y \in \mathcal{O} \setminus \mathfrak{p} \implies xy \in \mathcal{O} \setminus \mathfrak{p}$. Hence, $\gamma + \delta = v(xy) \in \Delta_{\mathfrak{p}}$, and thus $\Delta_{\mathfrak{p}}$ is a convex subgroup of Γ. We now show that the two mappings are mutually inverse, i.e., $\Delta_{\mathfrak{p}_\Delta} = \Delta$ and $\mathfrak{p}_{\Delta_{\mathfrak{p}}} = \mathfrak{p}$.

- $\underline{\mathfrak{p}_{\Delta_{\mathfrak{p}}} \subseteq \mathfrak{p}}$: Let $x \in \mathfrak{p}_{\Delta_{\mathfrak{p}}}$ and suppose $x \notin \mathfrak{p}$. Then, $v(x) \in \Delta_{\mathfrak{p}}$, which contradicts $x \in \mathfrak{p}_{\Delta_{\mathfrak{p}}}$.

- $\underline{\mathfrak{p} \subseteq \mathfrak{p}_{\Delta_{\mathfrak{p}}}}$: Let $x \in \mathfrak{p}$ and suppose $x \notin \mathfrak{p}_{\Delta_{\mathfrak{p}}}$. Then, $v(x) \in \Delta_{\mathfrak{p}}$ and so $v(x) = v(y)$ or $v(y^{-1})$ for some $y \in \mathcal{O} \setminus \mathfrak{p}$. Since $x \in \mathfrak{p} \subset \mathcal{O}, v(x) \geq 0 \implies v(x) = v(y)$.

  Then, $v(xy^{-1}) = 0 \implies xy^{-1} \notin \mathcal{M} \implies x^{-1}y \in \mathcal{O}$.

  Since $x \in \mathfrak{p}$ and $x^{-1}y \in \mathcal{O}$, $x(x^{-1}y) = y \in \mathfrak{p}$, a contradiction.

- $\underline{\Delta \subseteq \Delta_{\mathfrak{p}_\Delta}}$: Let $\lambda \in \Delta$. Since v is surjective, we have $\lambda = v(x)$ for some $x \in K$. Now, since Δ is a subgroup, $-\lambda \in \Delta$, thus both $v(x)$ and $v(x^{-1}) \in \Delta$. Moreover, since $\mathcal{O} \subset K$ is a valuation ring, we have x or $x^{-1} \in \mathcal{O}$. Suppose first that $x \in \mathcal{O}$ i.e., $\lambda = v(x) \geq 0$. Further, $\lambda \in \Delta \implies x \notin \mathfrak{p}_\Delta$. Hence, we get $x \in \mathcal{O} \setminus \mathfrak{p}_\Delta \implies \lambda = v(x) \in \Delta_{\mathfrak{p}_\Delta}$. Now, suppose $x^{-1} \in \mathcal{O}$ i.e., $\lambda = v(x) \leq 0$. Since $v(x^{-1}) = -\lambda \in \Delta \implies x^{-1} \notin \mathfrak{p}_\Delta$. Hence, we get $x^{-1} \in \mathcal{O} \setminus \mathfrak{p}_\Delta \implies -\lambda = v(x^{-1}) \in \Delta_{\mathfrak{p}_\Delta} \implies \lambda \in \Delta_{\mathfrak{p}_\Delta}$.

- $\underline{\Delta_{\mathfrak{p}_\Delta} \subseteq \Delta}$: Let $\lambda \in \Delta_{\mathfrak{p}_\Delta}$, i.e., $\lambda = v(t)$ or $v(t^{-1})$, $t \in \mathcal{O} \setminus \mathfrak{p}_\Delta$. Now $t \notin \mathfrak{p}_\Delta$ gives $v(t) \in \Delta$. Since Δ is a subgroup, $-v(t) = v(t^{-1}) \in \Delta$. Thus, $\lambda \in \Delta$.

This concludes the proof.

Corollary 1.4.1.1. *Let $\mathcal{O} \subseteq K$ be a nontrivial valuation ring. Then* $\operatorname{rank}(\mathcal{O}) = 1$ *if and only if $\mathcal{O}$ is a maximal subring of K.*

Proof. $\operatorname{rank}(\mathcal{O}) = 1$ if and only if $\mathcal{O}$ has one convex subgroup; this is equivalent to having one prime ideal, which in turn implies that $\mathcal{O}$ has a single overring. Since K is an overring, it must be the only one; i.e., $\mathcal{O} \subseteq S \subseteq K \implies S = K$ or $S = \mathcal{O}$. Thus, $\mathcal{O}$ is a maximal subring of K.

Now, let $\mathcal{O}$ be a nontrivial valuation ring of K corresponding to the valuation $v : K \twoheadrightarrow \Gamma \cup \{\infty\}$. Assume $\mathfrak{p} \lhd \mathcal{O}$ is prie with corresponding convex subgroup $\Delta \subseteq \Gamma$. The canonical valuation $v_\mathfrak{p}$ corresponding to $\mathcal{O}_\mathfrak{p}$ induces an order-preserving group homomorphism

$$\begin{aligned} \phi : K^\times/\mathcal{O}^\times &\to K^\times/\mathcal{O}_\mathfrak{p}^\times, \\ x\mathcal{O}^\times &\mapsto x\mathcal{O}_\mathfrak{p}^\times. \end{aligned}$$

It is well-defined because $\mathcal{O} \subseteq \mathcal{O}_\mathfrak{p} \implies \mathcal{O}^\times \subseteq \mathcal{O}_\mathfrak{p}^\times$. Now, $\ker \phi = \{x\mathcal{O}^\times : x\mathcal{O}_\mathfrak{p}^\times = \mathcal{O}_\mathfrak{p}^\times\} = \{x\mathcal{O}^\times : x \in \mathcal{O}_\mathfrak{p}^\times\} = \mathcal{O}_\mathfrak{p}^\times/\mathcal{O}^\times$. We want to show that $v_\mathfrak{p}$ is obtained from v by dividing Γ by Δ, i.e.

$$w : K \twoheadrightarrow \Gamma \cup \{\infty\} \twoheadrightarrow \Gamma/\Delta_\mathfrak{p} \cup \{\infty\} : \ x \mapsto v(x) + \Delta_\mathfrak{p}$$

is the same as

$$v_\mathfrak{p} : K \twoheadrightarrow \Gamma_\mathfrak{p} \cup \{\infty\}, \quad \text{where } \Gamma_\mathfrak{p} = K^\times/\mathcal{O}_\mathfrak{p}^\times.$$

We first consider $\mathcal{O}_w$:

$\mathcal{O}_w = \{x \in K : w(x) \geq 0\} = \{x \in K : v(x) + \Delta \geq \Delta\} = \{x \in K : v(x) > 0 \text{ or } v(x) \in \Delta\}$. Let $x \in \mathcal{O}_w$. Then, $v(x) > 0$ or $v(x) \in \Delta$. If $v(x) > 0$, then $x \in \mathcal{M}_v \subseteq \mathcal{O}_v \subseteq \mathcal{O}_{v_\mathfrak{p}}$. Suppose not, i.e., $v(x) \leq 0$. Then since $x \in \mathcal{O}_w$, we must have $v(x) \in \Delta$, i.e., there exists $t \in \mathcal{O} \setminus \mathfrak{p}$ such that $v(x) = v(t^{-1})$ ($\because v(x) \leq 0$). Hence, $v(xt) \geq 0 \implies xt \notin \mathcal{M}_v \implies xt$ and $x^{-1}t^{-1} \in \mathcal{O}_v$. Thus, $x = xt/t \in \mathcal{O}_\mathfrak{p}$, hence $\mathcal{O}_w \subseteq \mathcal{O}_\mathfrak{p}$.

Conversely, given $x = a/b \in \mathcal{O}_\mathfrak{p}$, i.e., $a \in \mathcal{O}$ and $b \in \mathcal{O} \setminus \mathfrak{p}$, we have $v(x) = v(a) - v(b) = v(a) + v(b^{-1}) = v(a) + \delta$ where $\delta \in \Delta$ thus $v(x) + \Delta = v(a) + \Delta \geq \Delta$, since $v(a) \geq 0$ as $a \in \mathcal{O}$. Therefore, $x \in \mathcal{O}_w$, i.e., $\mathcal{O}_\mathfrak{p} \subseteq \mathcal{O}_w$, whence $\mathcal{O}_\mathfrak{p} = \mathcal{O}_w$, i.e., $v_\mathfrak{p} = w$. Therefore, $\Gamma/\Delta_\mathfrak{p} = (K^\times/\mathcal{O}^\times)/\Delta_\mathfrak{p} \cong \Gamma_\mathfrak{p} = K^\times/\mathcal{O}_\mathfrak{p}^\times$

Lemma 1.4.4. *The residue homomorphism $\varphi_\mathfrak{p} : \mathcal{O}_\mathfrak{p} \to \mathcal{O}_\mathfrak{p}/\mathfrak{p} = \overline{\mathcal{K}}_\mathfrak{p}$ maps the valuation ring $\mathcal{O}$ to a valuation ring $\overline{\mathcal{O}} = \mathcal{O}/\mathfrak{p}$ in $\overline{\mathcal{K}}_\mathfrak{p}$.*

Proof. Let $\overline{x} \in \overline{\mathcal{K}}_\mathfrak{p}$, i.e., $\overline{x} = x + \mathfrak{p}$, $x \in \mathcal{O}_\mathfrak{p}$. Now, either $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$. If $x \in \mathcal{O}$, then $\overline{x} \in \overline{\mathcal{O}}$. Otherwise, if $x^{-1} \in \mathcal{O}$, then $\overline{x^{-1}} = \overline{x}^{-1} \in \overline{\mathcal{O}}$ and we are done.

Defining $\overline{v} : \overline{\mathcal{K}}_\mathfrak{p} \twoheadrightarrow \Delta \cup \{\infty\} : \overline{v}(\overline{x}) := v(x)$ yields a valuation on $\overline{\mathcal{K}}_\mathfrak{p}$ corresponding to $\overline{\mathcal{O}}$, with residue class field $\overline{\mathcal{O}}/\overline{\mathcal{M}} = \overline{\mathcal{K}}$ since $\overline{\mathcal{O}}/\overline{\mathcal{M}} = (\mathcal{O}/\mathfrak{p})/(\mathcal{M}/\mathfrak{p}) = \mathcal{O}/\mathcal{M}$.

Hence, passing from $\mathcal{O}$ to a coarsening $\mathcal{O}_\mathfrak{p}$ yields two valuations, namely

$$v_\mathfrak{p} : K \twoheadrightarrow \Gamma/\Delta_\mathfrak{p} \cup \{\infty\} \text{ with valuation ring } \mathcal{O}_\mathfrak{p}, \text{ and}$$

$$\overline{v}_\mathfrak{p} : \overline{\mathcal{K}}_\mathfrak{p} \twoheadrightarrow \Delta_\mathfrak{p} \cup \{\infty\} \text{ on the residue class field of } v_\mathfrak{p}.$$

The last process can be reversed, i.e., given a valuation $v' : K \twoheadrightarrow \Gamma' \cup \{\infty\}$ and another valuation on the residue class field of v', say $\overline{v} : \overline{\mathcal{K}}_{v'} \twoheadrightarrow \Delta' \cup \{\infty\}$, we can define a 'composition' of v' with $\overline{v}$.

Lemma 1.4.5. *Let $\mathcal{O} = \varphi^{-1}(\mathcal{O}_{\overline{v}})$ where $\mathcal{O}_{v'} \xrightarrow{\varphi} \overline{\mathcal{K}}_{v'}$ is the canonical residue homomorphism. Then, $\mathcal{O}$ is a valuation ring of K and $\mathcal{O}_{v'}$ is a coarsening of $\mathcal{O}$.*

Proof. $\mathcal{O} = \varphi^{-1}(\mathcal{O}_{\overline{v}}) = \{x \in \mathcal{O}_{v'} : \varphi(x) = x\mathcal{M}_{v'} \in \mathcal{O}_{\overline{v}}\} = \{x \in \mathcal{O}_{v'} : \overline{v}(x\mathcal{M}_{v'}) \geq 0\}$. Let $x \in K$. If $x \in \mathcal{O}$, then we are done. Otherwise, $x \notin \mathcal{O}$, i.e., $\overline{v}(x\mathcal{M}_{v'}) < 0$ i.e., $x\mathcal{M}_{v'}$ is a unit in $\mathcal{O}_{\overline{v}}$, i.e., $x^{-1}\mathcal{M}_{v'} \in \mathcal{O}_{\overline{v}}$. Hence, $\overline{v}(x^{-1}\mathcal{M}_{v'}) \geq 0 \implies x^{-1} \in \mathcal{O}$. Thus, $\mathcal{O}$ is a valuation ring of K and it follows that $\mathcal{O} \subseteq \mathcal{O}_{v'}$.

Let $v : K \twoheadrightarrow \Gamma \cup \{\infty\}$ be the canonical valuation corresponding to $\mathcal{O}$. Since $\mathcal{O}_{v'}$ is a coarsening, there exists a prime $\mathfrak{p} \triangleleft \mathcal{O}$ such that $\mathcal{O}_{v'} = \mathcal{O}_\mathfrak{p}$. Hence, $v' = v_\mathfrak{p}$, $\mathcal{M}_{v'} = \mathfrak{p}\mathcal{O}_\mathfrak{p}$ and $\overline{\mathcal{K}}_{v'} = \mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p} = \overline{\mathcal{K}}_\mathfrak{p}$. As before, $v_\mathfrak{p} : K \twoheadrightarrow \Gamma/\Delta_\mathfrak{p} \cup \{\infty\}$, and $\Gamma' \cong \Gamma/\Delta_\mathfrak{p}$. Again, as before, we have $\overline{v}_\mathfrak{p} : \overline{K}_\mathfrak{p} \to \Delta_\mathfrak{p} \cup \{\infty\}$ with valuation ring $\mathcal{O}_{\overline{v}_\mathfrak{p}}$. Note that $\overline{v}_\mathfrak{p}(xM_{v'}) := v(x)$, and so $\overline{v}_\mathfrak{p}(xM_{v'}) \geq 0 \implies v(x) \geq 0$, i.e., $\varphi(\mathcal{O}_{\overline{v}_\mathfrak{p}}) \subseteq \mathcal{O}$. If $v(x) \geq 0$, then $\overline{v}_\mathfrak{p}(xM_{v'}) \geq 0$, so $\mathcal{O} \subseteq \varphi^{-1}(\mathcal{O}_{\overline{v}_\mathfrak{p}})$, i.e., $\varphi^{-1}(\mathcal{O}_{\overline{v}_\mathfrak{p}}) = \mathcal{O} = \varphi(\mathcal{O}_{v'})$. Hence, $\mathcal{O}_{\overline{v}_\mathfrak{p}} = \mathcal{O}_{v'}$. Note that we have used the following fact: *If $f : A \to B$ is surjective and $f^{-1}(B_1) = f^{-1}(B_2)$, then $B_1 = B_2$.* Hence, $\overline{v}_\mathfrak{p} = \overline{v}$; so Δ' is isomorphic to a convex subgroup $\Delta_\mathfrak{p} \subset \Gamma$, and $\Gamma' \cong \Gamma/\Delta'$, where $\Gamma = K^\times/\mathcal{O}^\times$. We call this v the ***composition*** of v' with $\overline{v}$.

We now consider the topology induced by a valuation on a field K. We begin by showing that two valuations are dependent if and only if they induce the same topology.

Given a valuation $v : K \twoheadrightarrow \Gamma \cup \{\infty\}$, for any $\gamma \in \Gamma$ and each $a \in K$, we define $\mathcal{U}_\gamma(a) := \{x \in K : v(x-a) > \gamma\} = \{x \in K : |x-a| < e^{-\gamma}\}$.

These sets form a basis of open neighborhoods of a, i.e.,

(i) $a \in \mathcal{U}_\gamma(a)$

(ii) $\forall\, \mathcal{U}_\gamma, \mathcal{U}_\alpha, \exists\, \mathcal{U}_\delta$ such that $\mathcal{U}_\delta \subset \mathcal{U}_\gamma \cap \mathcal{U}_\alpha$

In fact, we have the following properties:

(i) $a \in \mathcal{U}_\gamma(a)$

(ii) $\mathcal{U}_\gamma(a) \cap \mathcal{U}_\alpha(a) = \mathcal{U}_\delta(a)$ where $\delta = \max\{\gamma, \alpha\}$

(iii) For any $b \in \mathcal{U}_\gamma(a)$ with $b \neq a$, $v(b-a) = \gamma' > \gamma$ implies $\mathcal{U}_{\gamma'}(b) \subset \mathcal{U}_\gamma(a)$

The first two follow directly from the definition. The third holds since $v(x-b) > \gamma' = v(b-a)$ implies $v(x-a) = v((x-b)+(b-a)) = \min\{v(x-b), v(b-a)\} = v(b-a) = \gamma' > \gamma$ i.e., $\forall x \in \mathcal{U}_{\gamma'}(b)$, we get $x \in \mathcal{U}_\gamma(a)$. We consider the topology defined by this basis of neighborhoods, i.e., a set $\mathcal{U}$ is open if $\forall x \in \mathcal{U}, \exists\, \mathcal{U}_\gamma(x)$ such that $x \in \mathcal{U}_\gamma(x) \subset \mathcal{U}$.

Lemma 1.4.6. *The topology constructed above is Hausdorff.*

Proof. Let $a \neq b$. Let $v(b-a) = \gamma'$. Consider $\mathcal{U}_{\gamma'}(a) = \{x \in K : v(x-a) > \gamma'\}$. Clearly, $b \notin \mathcal{U}_{\gamma'}(a)$. Pick some $\gamma > \gamma'$ and consider $\mathcal{U}_\gamma(b)$.

Claim: $\mathcal{U}_{\gamma'}(a) \cap \mathcal{U}_\gamma(b) = \emptyset$**.**

Suppose not, i.e., $\exists x \in K$ such that $v(x-a) > \gamma'$ and $v(x-b) > \gamma$.

Then, $\gamma' = v(b-a) = v((x-b)-(x-a)) = \min\{v(x-b), v(x-a)\}$. Since $v(x-a) > \gamma'$, we have $v(x-b) = \gamma'$, but $v(x-b) > \gamma$ and $\gamma' < \gamma$ — a contradiction. ☕

Lemma 1.4.7. $\Gamma = \{0\}$ *if and only if* $\mathcal{U}_\gamma(a) = \{a\}$ *for all* $a \in K$ *and all* $\gamma \in \Gamma$.

Proof. ($\Longrightarrow$): if $\Gamma = \{0\}$, then $v(x) = 0$ for all x, i.e., $x \in \mathcal{O}^\times$ for all x, i.e., $K = \mathcal{O}^\times$. Let $x \in \mathcal{U}_\gamma(a) = \{x \in K : v(x-a) > \gamma\}$ where $x \neq a$. Let $\gamma = t\mathcal{O}^\times$. Since $K = \mathcal{O}^\times, t \in \mathcal{O}^\times$, i.e., $\gamma = 0$, which is a contradiction. Hence, $\mathcal{U}_\gamma(a) = \{a\}$.

($\Longleftarrow$): Let $\mathcal{U}_\gamma(a) = \{a\}$ for all $a \in K$ and all $\gamma \in \Gamma$. Thus, any $x \in K$ satisfying $v(x-a) > \gamma$ must be a itself. Suppose $v(x) \neq 0$ for some x. Let $v(x) = \gamma$. Then, $\mathcal{U}_\gamma(0) = \{y \in K \mid v(y) > 0\} = \{0\}$. Since $v(x) \neq 0$, either $v(x) > 0$ or $v(x) < 0$. If $v(x) > 0$, then $x \in \mathcal{U}_\gamma(0)$, i.e., $x = 0$. Otherwise, $v(x) < 0$, i.e., $0 < -v(x)$, i.e., $0 < v(x^{-1})$, i.e., $x^{-1} \in \mathcal{U}_\gamma(0)$, i.e., $x^{-1} = 0$, i.e., $x = \infty$. Hence, $v(x) \neq 0$ implies $x = 0$ or ∞. Thus, $\Gamma = \{0\}$ ☕

Therefore, v is trivial if and only if the induced topology is discrete.

Remark 1.6. The field operations are continuous with respect to this topology.

Theorem 1.4.2. *Two nontrivial valuation rings $\mathcal{O}_1, \mathcal{O}_2$ of K are dependent if and only if they induce the same topology on K.*

Proof. Since two dependent valuation rings have a common nontrivial coarsening $\mathcal{O}_1\mathcal{O}_2$, to show they induce the same topology, it suffices to consider only the case $\mathcal{O}_1 \subseteq \mathcal{O}_2$. Let $v : K \twoheadrightarrow \Gamma \cup \{\infty\}$ be a valuation on $\mathcal{O}_1$. Then by Lemma 1.2.5, there exists a convex subgroup $\Delta \subseteq \Gamma$ connected with $\mathcal{O}_2$ such that $v_2 : K^\times \twoheadrightarrow \Gamma \twoheadrightarrow \Gamma/\Delta = \Gamma_2$ is a valuation on $\mathcal{O}_2$. Since $\mathcal{O}_1 \neq K$, $\Gamma_2 \neq \{0\}$. Write $\mathcal{U}_\gamma(0) = \{a \in K \mid v(a) > \gamma\}$ and $\mathcal{U}_{\gamma+\Delta}(0) = \{a \in K \mid v_2(a) > \gamma + \Delta\} = \{a \in K \mid v(a) > d \;\forall d \equiv \gamma \bmod \Delta\}$. We have $\mathcal{U}_{\gamma+\Delta}(0) \subseteq \mathcal{U}_\gamma(0)$ since $v(a) > \gamma \implies a \in \mathcal{U}_{\gamma+\Delta}(0)$.

On the other hand, $v(a) > 2\gamma$ implies $v_2(a) \geq 2\gamma + \Delta$. Hence for $\gamma > 0$, if $v_2(a) \leq \gamma + \Delta$, then $\gamma + \Delta \geq 2\gamma + \Delta$, i.e., $\gamma \in \Delta$. Contrapositively, this implies, $0 < \gamma \notin \Delta \implies v(a) \leq 2\gamma$, i.e., $\mathcal{U}_\gamma(0) \subseteq \mathcal{U}_{\gamma+\Delta}(0)$. Therefore, the topologies are equivalent.

Conversely, if $\mathcal{O}_1, \mathcal{O}_2$ induce the same topology on K, then $\mathcal{M}_2$ is an open neighborhood of zero in the topology induced by $\mathcal{O}_1$. Thus, $\mathcal{M}_2$ contains an open set around 0, i.e., $\exists a \in K^\times$ such that $\{x \in K \mid v(x) > \gamma\} = a\mathcal{M}_1 \subseteq \mathcal{M}_2$, where $\gamma = v(a^{-1})$.

Claim: $\mathcal{O}_1 \setminus \mathcal{M}_2$ is multiplicatively closed in $\mathcal{O}_1$:

Suppose $y_1, y_2 \in \mathcal{O}_1 \setminus \mathcal{M}_2$ and $y_1y_2 \notin \mathcal{O}_1 \setminus \mathcal{M}_2 \implies y_1y_2 \in \mathcal{M}_2$. Thus, $v_2(y_1y_2) > 0 \implies v_2(y_1) > v_2(y_2^{-1})$. Since $y_1, y_2 \notin \mathcal{M}_2$, $v_2(y_1) \leq 0$ and $v_2(y_2) \leq 0$. Thus, $v_2(y_1^{-1}) \geq 0$ but $v_2(y_1) > v_2(y_2^{-1}) \geq 0$, i.e., $v_2(y_1) > 0$. This is a contradiction. Hence, $\mathcal{O}_1 \setminus \mathcal{M}_2$ is multiplicatively closed. Thus, we may form the ring $\mathcal{O}_3 := \left\{\frac{x}{y} : x \in \mathcal{O}_1, y \in \mathcal{O}_1 \setminus \mathcal{M}_2\right\}$. Clearly, $\mathcal{O}_1 \subset \mathcal{O}_3$, hence $\mathcal{O}_3$ is a valuation ring. Now, for $x \in \mathcal{O}_2 \setminus \{0\}$, $x^{-1} \notin \mathcal{M}_2$ (since x^{-1} is invertible in $\mathcal{O}_2$). Thus, $x = 1/x^{-1} \in \mathcal{O}_3$, if $x^{-1} \in \mathcal{O}_1$. If $x^{-1} \notin \mathcal{O}_1$, then $x \in \mathcal{O}_1$, and so $x \in \mathcal{O}_3$ ($\because \mathcal{O}_1 \subseteq \mathcal{O}_3$). Hence, in any case, $x \in \mathcal{O}_3$. Thus, $\mathcal{O}_3$ contains $\mathcal{O}_2$ as well. Therefore, $\mathcal{O}_3 \supseteq \mathcal{O}_1\mathcal{O}_2$. We need only show $\mathcal{O}_3 \neq K$ to conclude that $\mathcal{O}_1, \mathcal{O}_2$ are dependent. Take $z \in \mathcal{M}_1 \setminus \{0\}$. Then, $1/az \notin \mathcal{O}_3$ because if $1/az \in \mathcal{O}_3$, then $1/az = x/y$, for some $x \in \mathcal{O}_1$, $y \in \mathcal{O}_1 \setminus \mathcal{M}_1$, implying $y = a(zx) \in a\mathcal{M}_1 \subseteq \mathcal{M}_2$ — contradiction. Thus, $1/ax \in K \setminus \mathcal{O}_3$, and hence $\mathcal{O}_3 \neq K$.

Theorem 1.4.3 (Approximation Theorem)**.** *Suppose $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_n$ are pairwise independent valuation rings of K. For every $1 \leq i \leq n$, let $v_i : K \twoheadrightarrow \Gamma_i \cup \{\infty\}$ be a valuation on $\mathcal{O}_i$.*

Then, for any $a_1, a_2, \ldots, a_n \in K$ and $\gamma_1 \in \Gamma_1, \gamma_2 \in \Gamma_2, \ldots, \gamma_n \in \Gamma_n$, there exists $x \in K$ such that $v_i(x - a_i) > \gamma_i$ for all $i \in \{1, 2, \ldots, n\}$.

Proof. For every i, pick positive $\delta_i \in \Gamma_i$ satisfying $\delta_i \geq \gamma_i$ and $-\delta_i \leq v_i(a_1), v_i(a_2), \ldots, v_i(a_n)$. Some new restrictions will be imposed on each δ_i during the proof.

Consider the open sets

$$M_i = \{x \in K : 2\delta_i < v_i(x)\} \text{ and}$$

$$A_i = \{x \in K : -2\delta_i \leq v_i(x)\}.$$

Note that $\gamma \leq v(x)$ and $\gamma \leq v(y) \implies \gamma \leq \min\{v(x), v(y)\} < v(x \pm y)$, hence M_i and A_i are closed under addition and subtraction.

Claim: We may choose δ_i such that $M_1 \cap \bigcap_{j=2}^{n}(K \setminus A_j) \neq \emptyset$.

We induct on n. For $n = 2$, suppose $M_1 \cap (K \setminus A_2) = \emptyset$, then $M_1 \subseteq A_2$. Now, choosing $c_i \in M_i$ $(i = 1, 2)$, we have $c_i A_i \subseteq \mathcal{M}_i$ and $c_i \mathcal{M}_i \subseteq M_i$. Thus, $M_1 \subseteq A_2 \implies c_2 c_1 \mathcal{M}_1 \subseteq c_2 M_2 \subseteq c_2 A_2 \subseteq \mathcal{M}_2$. Taking $a = c_2 c_1$ gives $a\mathcal{M}_1 \subseteq \mathcal{M}_2$. Proceeding as in Theorem 1.4.2, we get $\mathcal{O}_1$ and $\mathcal{O}_2$ are dependent — contradiction. For $n > 2$, by induction hypothesis, $\exists r \in M_1 \cap (K \setminus A_j)$. We choose $\delta_3, \delta_4, \ldots, \delta_n$ large enough for $r \in A_j$ $\forall j = 3, 4, \ldots, n$, i.e.

$$\delta_i \geq \gamma_i,\ \delta_i \leq v_i(a_1), v_i(a_2), \ldots, v_i(a_n), \text{ and } -2\delta_i \leq v_i(x)\ \forall j = 3, 4, \ldots, n.$$

Thus, r has the following properties:

$$2\delta_i < v_1(r),\ -2\delta_2 \leq v_2(r) \text{ and } -2\delta_i \leq v_i(r)\ \forall j = 3, 4, \ldots, n.$$

By induction hypothesis, $\exists s \in M_1 \cap \bigcap_{3 \leq j \leq n}(K \setminus A_j)$. If $s \notin A_2$, then $s \in M_1 \cap \bigcap_{j=2}^{n}(K \setminus A_j)$ and the claim is proved. Suppose not. Then, $s \in A_2$ and $r \notin A_2 \implies s + r \notin A_2$. Further, $s \notin A_j$ and $r \in A_j$ $\forall j = 3, 4, \ldots, n$ $\implies s + r \notin A_j$ $\forall j = 3, 4, \ldots, n$. Therefore, $s + r \in M_1 \cap \bigcap_{j=2}^{n}(K \setminus A_j)$ and the claim is proved. Analogously, by replacing M_1 with M_i and $\bigcap_{j=2}^{n}(K \setminus A_j)$ with $\bigcap_{j \neq i}(K \setminus A_j)$ and repeating the argument, we get $M_i \cap \bigcap_{j \neq i}(K \setminus A_j) \neq \emptyset$. Now, for any $x \in K \setminus A_j$, we have $v_j(1 + x) = v_j(x)$ since $v_j(1) = 0 > -2\delta_j > v_j(x)$. Thus, $-2\delta_j > v_j(1 + x) \implies 2\delta_j < v_j(1/(1 + x)) \implies 1/(1 + x) \in M_j$ Further, if $x \in M_i$, then $v_i\left(\dfrac{x}{1+x}\right) = v_i(x) - v_i(1 + x) = v_i(x)$, since $v_i(1) = 0 < v_i(x) \implies v_i(1 + x) = v_i(1) = 0$. Thus, $\dfrac{x}{1+x} \in M_i$. Hence, $\dfrac{1}{1+x} = 1 - \dfrac{x}{1+x} \in (1 + M_i)$.

Therefore,

$$\frac{1}{1+x} \in (1+M_i) \cap \bigcap_{j \neq i} M_j \text{ for any } x \in M_i \cap \bigcap_{j \neq i} (K \setminus A_j)$$

Hence, $(1+M_i) \cap \bigcap_{j \neq i} M_j \neq \emptyset$. We now choose $d_i \in (1+M_i) \cap \bigcap_{j \neq i} M_j$ and set $x \coloneqq a_1 d_1 + \cdots + a_n d_n$. Since $d_i - 1 \in M_i$ and $d_j \in M_j \; \forall j \neq i$, $v_i(d_i - 1) > 2\delta_i$ and $v_i(d_j) > 2\delta_i$. Therefore,

$$\begin{aligned} v_i(x - a_i) &= v_i(a_1 d_1 + \cdots + a_i(d_i - 1) + \cdots + a_n d_n) \\ &> \min_{1 \leq j \leq n} \{v_i(a_j) + 2\delta_i\} \geq -\delta_i + 2\delta_i = \delta_i \geq \gamma_i. \end{aligned}$$

☕

We now list and prove some properties of nonarchimedean complete real fields (in the multiplicative notation).

Lemma 1.4.8. *In a nonarchimedean complete real field, all triangles are isoceles, i.e.,* $|x| > |y| \implies |y - x| = |x|$.

Proof. This is simply a restatement of Proposition 1.1.4, but we provide a proof again: if $|x| > |y|$, then $|x - y| = \max\{|x|, |y|\} = |x|$, whence it follows $|x| = |y + (x - y)| \leq \max\{|y|, |x - y|\} \leq \max\{|y|, |x|, |y|\} = |x|$, so the inequalities are equalities, implying $|x - y| = |x|$. Similarly, if $|y| > |x|$ then $|x - y| = |y|$, thus in general two of the numbers $|x|, |y|, |x - y|$ have to be equal. ☕

Lemma 1.4.9. *In a nonarchimedean complete real field, wo balls are either disjoint or concentric, i.e.,* $B(a, r) = B(b, r)$ *for all* $b \in B(x, r)$. *In particular, every point in the open unit ball is a center.*

Proof. Consider an open ball $B(a, r) = \{x \in K : |x - a| < r\}$ and let $b \in B(a, r)$, i.e. $|b - a| < r$. If $c \in K$, then consider the triangle with vertices a, b, c. The above lemma shows that $|c - a| \geq r$ if and only if $|c - b| \geq r$, showing $B(a, r) = B(b, r)$. ☕

Lemma 1.4.10. *The open ball* $B(a, r) = \{x \in K : |x - a| < r\}$, *the closed ball* $\overline{B}(a, r) = \{x \in K : |x - a| \leq r\}$, *and the sphere* $S(a, r) = \{|x - a| = r\}$ *are both open and closed for* $r > 0$. *In particular, the valuation ring* $\mathcal{O} = \{x \in K : |x| \leq 1\} \subseteq K$ *is both closed and open.*

Proof. The open ball $B(a,r)$ is open by definition. We first show that the sphere $S(0,r)$ is open. Let $a \in S(0,r)$ and consider $x \in B(a,r)$. We have $|x| = |a+(x-a)|$ and $|x-a| < r = |a| \implies |x| = |a| = r$, i.e., $|x| = r \implies x \in S(0,r)$. Hence, $B(a,r)$ is an open ball around a contained in $S(0,r)$. Given any sphere $S(a,r)$, we have the translation homeomorphism $S(0,r) \to S(a,r) : x \mapsto a+x$ and so $S(a,r)$ is open as well. Therefore, $\overline{B}(a,r) = B(a,r) \cup S(a,r)$ is also open. Now, consider $X := K \setminus B(0,r)$ and let $x \in X$, i.e., $|x| \geq r$. Let $y \in B(x,r/2)$ then $|x-y| < r/2 \implies |y| = |x-(x-y)| = |x| \geq r$. Hence, $y \in X \implies B(x,r/2) \subset X$, i.e., X is open, whence we get that $B(0,r)$ is closed. Therefore, $B(a,r)$ is closed as well, since it is homeomorphic to $B(0,r)$ via the translation map.

Lemma 1.4.11. *A nonarchimedean complete real field K is totally disconnected, i.e., the only connected components are singletons.*

Proof. Suppose $S \subset K$ is a connected component having at least two distinct points $a, b \in S$ with $|a-b| = r > 0$. We may then write S as

$$\begin{aligned} S &= (S \cap B(a,r/2)) \cup (S \cap K \setminus B(a,r/2)) \\ &= (S \cap \{|x-a| < r/2\}) \cup (S \cap \{|x-a| \geq r/2\}) \end{aligned}$$

Hence, S can be expressed as a union of two disjoint nonempty open sets, which contradicts the fact that S is connected.

1.5 Extensions of Valuations

We now show that for every extension L/K, a valuation on K may be extended to L.

Theorem 1.5.1 (Chevalley)**.** *For a field K, let $R \subseteq K$ be a subring and let $\mathfrak{p} \lhd R$ be prime. Then, there exists a valuation ring $\mathcal{O} \subseteq K$ such that $R \subseteq \mathcal{O}$ and $\mathcal{M} \cap R = \mathfrak{p}$.*

Proof. Consider

$$\Sigma := \{(A, I) : \mathfrak{p}R_{\mathfrak{p}} \subseteq A \subseteq K, \text{ and } \mathfrak{p}R_{\mathfrak{p}} \subseteq I \subset A, \text{ where } A \text{ is a ring and } I \lhd A\}.$$

Since $(R_{\mathfrak{p}}, \mathfrak{p}R_{\mathfrak{p}}) \in \Sigma$, it is nonempty. We partially order Σ as

$$(A_1, I_1) \leq (A_2, I_2) \iff A_1 \subseteq A_2 \text{ and } I_1 \subseteq I_2.$$

Claim: For any chain $\{(A_i, I_i)\}_{i\in J}$ of such pairs, then $\left(\bigcup_i A_i, \bigcup_i I_i\right)$ gives an upper bound. For any $i \neq j$, assume without loss of generality that $A_i \subseteq A_j$ which implies $A_i \cup A_j = A_j$. Hence $\bigcup_i A_i = A_{i'}$ for some $i' \in J$, so $\bigcup_i A_i$ is a ring. To see that $I = \bigcup_j I_j$ is an ideal of A, let $x, y \in I$. Say $x \in I_n$ and $y \in I_m$, and suppose $I_m \subseteq I_n$. Then $x, y \in I_n$ and so $x + y,\ xy \in I_n \subseteq I$. Hence closure under addition and multiplication follows. Clearly, $-x \in I_n \subseteq I$, hence I contains additive inverses. It also contains 0 and 1. Now, to show $IR \subseteq I$, let $r \in R$ and $i \in I$. Then $i \in I_n$ for some n. Thus $ri \in I_n \subseteq I \implies IR \subseteq I$. We have $R \subseteq R_\mathfrak{p} \subseteq \mathcal{O}$ and $\mathfrak{p}R_\mathfrak{p}$ is the unique maximal ideal of $R_\mathfrak{p}$. Hence $\mathcal{M} \cap R_\mathfrak{p} \subseteq \mathfrak{p}R_\mathfrak{p}$.

Conversely, since $\mathfrak{p}R_\mathfrak{p} \subseteq \mathcal{M}$, we get $\mathcal{M} \cap R_\mathfrak{p} \supseteq \mathfrak{p}R_\mathfrak{p}$, thus $\mathfrak{p}R_\mathfrak{p} = \mathcal{M} \cap R_\mathfrak{p}$.

Claim: $\mathfrak{p} = \mathcal{M} \cap R$: Let $x \in \mathfrak{p}$, then $x \in \mathfrak{p}R_\mathfrak{p} \implies x \in \mathcal{M} \cap R_\mathfrak{p} \implies x \in \mathcal{M} \implies x \in \mathcal{M} \cap R$. Hence, $\mathfrak{p} \subseteq \mathcal{M} \cap R$. Let $x \in \mathcal{M} \cap R$, $x \in R \subseteq R_\mathfrak{p}$, and $x \in \mathcal{M} \implies x \in \mathfrak{p}R_\mathfrak{p}$. But $\mathfrak{p}R_\mathfrak{p} \cap R = \mathfrak{p} \implies x \in \mathfrak{p}$. Hence, $\mathcal{M} \cap R \subseteq \mathfrak{p}$. Thus, we need only show that $\mathcal{O}$ is a valuation ring. Now, $(\mathcal{O}, \mathcal{M})$ is a local ring because if there is another maximal ideal $\mathcal{M}'$ of $\mathcal{O}$, then $\mathcal{M}' \subseteq \mathcal{M}$ or $\mathcal{M} \subseteq \mathcal{M}'$. By maximality in Σ, $\mathcal{M}' \subseteq \mathcal{M}$, but since $\mathcal{M}'$ is a maximal ideal, $\mathcal{M}' = \mathcal{M}$. Suppose $\mathcal{O}$ is not a valuation ring, then $\exists\, x \in K^\times$ with $x, x^{-1} \notin \mathcal{O}$. Thus, $\mathcal{O} \subsetneq \mathcal{O}[x]$ and $\mathcal{O} \subsetneq \mathcal{O}[x^{-1}]$. The maximality of $(\mathcal{O}, \mathcal{M})$ implies $\mathcal{M}\mathcal{O}[x] = \mathcal{O}[x]$ (otherwise $(\mathcal{O}, \mathcal{M}) \leq (\mathcal{O}[x], \mathcal{M}\mathcal{O}[x])$). Similarly, $\mathcal{M}\mathcal{O}[x^{-1}] = \mathcal{O}[x^{-1}]$, and hence there exist $a_0, \ldots, a_n, b_0, \ldots, b_m \in \mathcal{M}$ such that

$$1 = \sum_{i=0}^{n} a_i x^i = \sum_{j=0}^{m} b_j x^{-j},$$

with n, m minimal. Without loss of generality, assume $m \leq n$. Now, $b_0 \in \mathcal{M} \implies \sum_{j=1}^{m} b_j x^{-j} = 1 - b_0 \in \mathcal{O}^\times$ (since R is a local ring $\implies$ for all $r \in R$, either r or $1 - r$ is invertible, so $1 - b_0 \in \mathcal{O}^\times$). Put $c_i = b_i(1 - b_0)^{-1}$ to get

$$1 = \Big(\sum_{j=1}^{m} b_j x^{-j}\Big)(1 - b_0)^{-1} = \sum_{j=1}^{m} c_j x^{-j}.$$

Hence, $x^n = \sum_{j=1}^{m} c_j x^{n-j}$. Using $1 = \sum_{i=0}^{n} a_i x^i$, we get

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

But $m \leq n$, so $n - j \geq 0$, for all $j \leq m$. Also $n - j < n$, hence we have an expression for 1 with exponent of x being at most $n - 1$, which contradicts the minimality of n. Therefore, $\mathcal{O}$ is a valuation ring. ☕

Definition 1.5.1. Let K_2/K_1 be a field extension and $\mathcal{O}_i \subseteq K_i$ be valuation rings. We say $\mathcal{O}_2$ is a ***prolongation*** or ***extension*** of $\mathcal{O}_1$ (or $\mathcal{O}_2$ lies over $\mathcal{O}_1$) if $\mathcal{O}_2 \cap K_1 = \mathcal{O}_1,$ denoted as $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2)$.

In this case, we have $\mathcal{M}_2 \cap K_1 = \mathcal{M}_1,\ \mathcal{O}_2 \cap K_1 = \mathcal{O}_1,$ and $\mathcal{O}_2^\times \cap K_1 = \mathcal{O}_1^\times \implies \mathcal{O}_1 = \mathcal{O}_2 \cap K_1$. Given a field extension K_2/K_1 and a valuation ring $\mathcal{O}_1 \subseteq K_1$, we see that $\mathcal{O}_1 := \mathcal{O}_2 \cap K_1$ is a valuation ring of K_1 such that $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2)$.

Theorem 1.5.2. *Let K_2/K_1 be a field extension and $\mathcal{O}_1 \subseteq K_1$ be a valuation ring. Then, there is a prolongation $\mathcal{O}_2 \subseteq K_2$ of $\mathcal{O}_1$.*

Proof. We have $\mathcal{O}_1$ is a subring of K_1 and $\mathcal{M}_1 \lhd \mathcal{O}_1$ is maximal, hence prime. Thus, by Chevalley's Theorem, there exists a valuation ring $\mathcal{O}_2 \subseteq K_2$ with $\mathcal{O}_2 \cap K_1 = \mathcal{O}_1$ and $\mathcal{M}_2 \cap K_1 = \mathcal{M}_1$.

Claim: The maximal ideal of $\mathcal{O}_2 \cap K_1$ is $\mathcal{M}_2 \cap K_1 = \mathcal{M}_1$.

Let $x \in \mathcal{M}_2 \cap K_1$ and $a \in \mathcal{O}_2 \cap K_1$ be arbitrary. We will show that $ax \in \mathcal{M}_2 \cap K_1 = \mathcal{M}_1$. Now, $a \in K_1 \implies a \in \mathcal{O}_1$ or $a^{-1} \in \mathcal{O}_1$. If $a \in \mathcal{O}_1$, then $ax \in \mathcal{M}_1$, and we are done. Otherwise, $a^{-1} \in \mathcal{O}_1$. We already have $ax \in \mathcal{M}_2$, since $a \in \mathcal{O}_2$, $x \in \mathcal{M}_2$, and $\mathcal{M}_2 \subset \mathcal{O}_2$. Thus, we need only show that $ax \in \mathcal{O}_1$. Suppose not, i.e., $ax \notin \mathcal{O}_1$. Then, $(ax)^{-1} = a^{-1}x^{-1} \in \mathcal{O}_1$, since $\mathcal{O}_1 \subseteq K_1$ is a valuation ring. Now, $x \in \mathcal{M}_1 \subset \mathcal{O}_1 \implies (a^{-1}x^{-1})x = a^{-1} \in \mathcal{M}_1 = \mathcal{M}_2 \cap K_1 \implies a^{-1} \in \mathcal{M}_2$. So a^{-1} is not invertible in $\mathcal{O}_2$, i.e., $(a^{-1})^{-1} = a \notin \mathcal{O}_2$ — contradiction.. Hence the claim is true. Since local rings with the same maximal ideal must coincide, we have $\mathcal{O}_2 \cap K_1 = \mathcal{O}_1$, and we are done.

Theorem 1.5.3.

1. *Every valuation ring $\mathcal{O}$ of a field K is integrally closed in K.*
2. *Let $D \subseteq K$ be a subring and $\mathbb{V} = \{\mathcal{O} : D \subseteq \mathcal{O}$ and $\mathcal{M} \cap D$ is a maximal ideal of $D\}$, where $\mathcal{O}$ is a valuation ring. The integral closure R of D in K equals*

$$R_1 := \bigcap_{\mathcal{O} \in \mathbb{V}} \mathcal{O}.$$

Proof.

1. Let $x \in K$ with $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x_n = 0$ for some $a_0, \ldots, a_{n-1} \in \mathcal{O}$. If $x \in \mathcal{O}$, we are done. Suppose not. Then $x \notin \mathcal{O}$, i.e., $x^{-1} \in \mathcal{M}$, so

$$\begin{aligned} &-x^n = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \\ \implies &-1 = a_0 x^{-n} + \cdots + a_{n-1}x^{-1} \in \mathcal{M}, \end{aligned}$$

but $\mathcal{M}$ is a proper ideal — contradiction.

2. Let $x \in K$ be integral over D, i.e., $x^n + \sum_{i=0}^{n-1} a_i x^i = 0$ for some $a_i \in D$. Now, $D \subseteq \mathcal{O} \implies a_i \in \mathcal{O} \implies D \subseteq \mathcal{O}$ for all $\mathcal{O} \in \mathbb{V}$, so $D \subseteq R_1$. Hence, each $a_i \in R_1$, and so x is integral over R_1. By (1), each $\mathcal{O} \in \mathbb{V}$ is integrally closed in K. Thus, $x \in \mathcal{O}$ for all $\mathcal{O} \in \mathbb{V}$, so $x \in R_1$. Thus, $R \subseteq R_1$. Conversely, let $x \notin R$. We will show $x \notin R_1$. First, observe $x \notin R[x^{-1}]$, otherwise $x = \sum_{i=0}^{m} b_i x^{-i}$, $b_i \in R$, then $x^{m+1} = \sum_{i=0}^{m} b_i x^{m-i} = b_0 x^m + b_1 x^{m-1} + \cdots + b_m, \quad b_i \in R$. i.e., x is integral over R, and so integral over D — contradiction. Hence, $x \notin R[x^{-1}]$. Since x^{-1} is not invertible in $R[x^{-1}]$, we have $x^{-1} \in \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$ of $R[x^{-1}]$. By Chevalley's Theorem, there exists a valuation ring $\mathcal{O} \subseteq K$ such that $R[x^{-1}] \subseteq \mathcal{O}$ and $\mathcal{M} \cap R[x^{-1}] = \mathfrak{m}$. Since $x \in \mathfrak{m} = \mathcal{M} \cap R[x^{-1}]$, we get $x \in \mathcal{M} \implies x \notin \mathcal{O}$. Finally, we have $\mathcal{O} \in \mathbb{V}$, i.e., $\mathcal{M} \cap D \lhd D$ is maximal. This follows easily as contraction from an integral extension preserves maximality. Since $x \notin \mathcal{O}$, it follows that $x \notin R_1$, and we are done.

☕

Corollary 1.5.3.1. *Let L/K be any field extension and $\mathcal{O}$ be a valuation ring of K. Let R be the integral closure of $\mathcal{O}$ in L. Then, letting $\mathcal{O}'$ range over the set of prolongations of $\mathcal{O}$ to L, we have*

$$R = \bigcap_{\mathcal{O}' \supseteq \mathcal{O}} \mathcal{O}'.$$

Proof. For each prolongation $\mathcal{O}'$, let $\mathcal{M}'$ be its maximal ideal. Then, by definition, $\mathcal{M} \cap \mathcal{O} = \mathcal{M}$. Conversely, if $\mathcal{O}' \supseteq \mathcal{O}$ has maximal ideal $\mathcal{M}'$ satisfying $\mathcal{M} \cap \mathcal{O} = \mathcal{M}$, then $\mathcal{O}' \cap K = \mathcal{O}$. Hence, the set $\mathbb{V}$ is exactly the set of prolongations of $\mathcal{O}$ to L. The result thus follows from the theorem.

☕

Let $(K_1, \mathcal{O}_1) \subset (K_2, \mathcal{O}_2)$ be an arbitrary extension of valued fields. For each $\mathcal{O}_i$, let $v_i : K \twoheadrightarrow \Gamma_i \cup \{\infty\}$ be a valuation and recall that its restriction $v_i : K_i^\times \twoheadrightarrow \Gamma_i$ is a group homomorphism with kernel $\mathcal{O}_i^\times$ and so $K_i^\times / \mathcal{O}_i^\times \cong \Gamma_i$. Further, the composite map

$$K_1^\times \hookrightarrow K_2^\times \twoheadrightarrow K_2^\times / \mathcal{O}_2^\times \cong \Gamma_2$$

has kernel $K_1^\times \cap \mathcal{O}_2^\times = \mathcal{O}_1^\times$. Thus, $\Gamma_1 \cong K_1^\times / \mathcal{O}_1^\times \hookrightarrow K_2^\times / \mathcal{O}_2^\times \cong \Gamma_2$ is a well-defined group homomorphism. Hence, we may regard Γ_1 as an ordered subgroup of Γ_2.

Definition 1.5.2. Define the ***ramification index*** of this extension as

$$e := e(\mathcal{O}_2/\mathcal{O}_1) := [\Gamma_2 : \Gamma_1].$$

As before, considering $\mathcal{O}_1 \hookrightarrow \mathcal{O}_2 \twoheadrightarrow \mathcal{O}_2/\mathcal{M}_2 = \mathcal{K}_2$ has kernel $\mathcal{O}_1/\mathcal{M}_2 = \mathcal{M}_1$, we get a well-defined map $\mathcal{K}_1 \hookrightarrow \mathcal{K}_2$.

Definition 1.5.3. Define the ***residue degree*** of this extension as

$$f \coloneqq f(\mathcal{O}_2/\mathcal{O}_1) = [\mathcal{K}_2 : \mathcal{K}_1].$$

Now, if $e(\mathcal{O}_2/\mathcal{O}_1) = f(\mathcal{O}_2/\mathcal{O}_1) = 1$, then the extension $\mathcal{O}_2/\mathcal{O}_1$ is called ***immediate***.

Example 1.7. A completion $(\widehat{K}, \widehat{\mathcal{O}})$ of a rank-one valued field $(K, \mathcal{O})$ is an immediate extension, as seen previously.

Remark 1.7. e and f are multiplicative: if $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2) \subseteq (K_3, \mathcal{O}_3)$, then

$$e(\mathcal{O}_3/\mathcal{O}_1) = e(\mathcal{O}_3/\mathcal{O}_2)\, e(\mathcal{O}_2/\mathcal{O}_1)$$

and

$$f(\mathcal{O}_3/\mathcal{O}_1) = f(\mathcal{O}_3/\mathcal{O}_2)\, f(\mathcal{O}_2/\mathcal{O}_1),$$

because degrees of extensions are multiplicative.

Lemma 1.5.1. *Suppose $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2)$, and for $i = 1, 2$, let v_i be the valuation corresponding to $\mathcal{O}_i$. Choose $\omega_1, \ldots, \omega_f \in \mathcal{O}_2$ and $\pi_1, \ldots, \pi_e \in K_2^\times$ so that:*

1. the residues $\overline{\omega}_1, \ldots, \overline{\omega}_f \in \overline{\mathcal{K}}_2$ are linearly independent over $\overline{\mathcal{K}}_1$;

2. the values $v_2(\pi_1), \ldots, v_2(\pi_e)$ are representatives of the distinct cosets of Γ_2/Γ_1.

Then for all $a_{ij} \in K_1$,

$$v_2\left(\sum_{i=1}^{f}\sum_{j=1}^{e} a_{ij}\omega_i\pi_j\right) = \min\{\, v_2(a_{ij}\omega_i\pi_j) \mid 1 \le i \le f,\ 1 \le j \le e\,\}.$$

In particular, the products

$$\{\omega_i\pi_j \mid i = 1, \ldots, f,\ j = 1, \ldots, e\}$$

are linearly independent over K_1.

Proof. Let $a_{ij} \in K_1$ not all zero, and pick $1 \le I \le f$ and $1 \le J \le e$ such that

$$v_2(a_{IJ}\omega_I\pi_J) = \min_{i,j}\{\, v_2(a_{ij}\omega_i\pi_j)\,\}.$$

Claim: $v_2(a_{IJ}\pi_J) < v_2(a_{ij}\pi_j)$ **for all** $j \neq J$**.**

If not, then there exist $j \neq J$ with $v_2(a_{ij}\pi_j) = v_2(a_{IJ}\pi_J)$; i.e. $v_2(a_{IJ}) + v_2(\pi_J) = v_2(a_{IJ}) + v_2(\pi_j)$. Now, $v_2(\pi_j) - v_2(\pi_J) = v_2(a_{IJ}) - v_2(a_{ij}) \in \Gamma_1$ implying $v_2(\pi_j) \equiv v_2(\pi_J) \mod \Gamma_1$, which contradicts the second hypothesis. This proves the claim.

Let $z = \sum_{i=1}^{f} \sum_{j=1}^{e} a_{ij}\omega_i\pi_j$. We know by the strong triangle inequality that $v_2(z) \geq \min_{i,j} v_2(a_{ij}\omega_i\pi_j)$. If equality holds, we are done. Suppose not, i.e. $v_2(z) > \min_{i,j} v_2(a_{ij}\omega_i\pi_j)$. Note that

$$v_2(a_{ij}\omega_i\pi_j) = v_2(a_{ij}\pi_j) + v_2(\omega_i) \geq v_2(a_{ij}\pi_j) \quad (\text{since } \omega_i \in \mathcal{O}_2).$$

Hence $v_2(z) \geq v_2(a_{ij}\pi_j) \geq v_2(a_{IJ}\pi_J)$. Therefore $z(a_{IJ}\pi_J)^{-1} \in \mathcal{M}_2$.

Moreover, by the earlier claim, $a_{ij}\pi_j\omega_i(a_{IJ}\pi_J)^{-1} \in \mathcal{M}_2$ for all $j \neq J$.

Thus

$$z(a_{IJ}\pi_J)^{-1} - \sum_{i=1}^{f} \sum_{j \neq J} a_{ij}\pi_j\omega_i(a_{IJ}\pi_J)^{-1} \in \mathcal{M}_2,$$

and this expression equals $\sum_{i=1}^{f} a_{iJ}(a_{IJ})^{-1}\omega_i$, because

$$z - \sum_{j \neq J} \sum_{i=1}^{f} a_{ij}\pi_j\omega_i = \sum_{i=1}^{f} a_{iJ}\omega_i\pi_J.$$

Hence, $\sum_{i=1}^{f} a_{iJ}(a_{IJ})^{-1}\omega_i \in \mathcal{M}_2$, thus its image in $\mathcal{K}_2$ is zero, i.e., $\sum_{i=1}^{f} \overline{a_{iJ}(a_{IJ})^{-1}}\,\overline{\omega_i} = \overline{0}$, which contradicts hypothesis 1.

☕

Corollary 1.5.3.2. *Suppose $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2)$ and $n = [K_2 : K_1] < \infty$. Then, $e, f < \infty$ and $ef < n$.*

Proof. This follows because $\{\omega_i\pi_j \mid i = 1, \ldots, f,\ j = 1, \ldots, e\}$ is a linearly independent set of cardinality ef. ☕

Theorem 1.5.4. *Let $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2)$ with K_2 algebraic over K_1. Then*

1. *For every $\gamma \in \Gamma_2$, there exists $n \in \mathbb{N}$ such that $n\gamma \in \Gamma_1$, i.e. Γ_2/Γ_1 is a torsion group.*
2. *$\overline{\mathcal{K}_2}$ is an algebraic extension of $\overline{\mathcal{K}_1}$.*

Proof. 1. Let $\gamma \in \Gamma_2$ be arbitrary. Since v_2 is surjective, choose $x \in K_2^\times$ with $v_2(x) = \gamma$. Let $L = K_1(x) \subseteq K_2$. Because x is algebraic over K_1, the extension L/K_1 is finite. Let $\Gamma = v(L^\times) \subseteq \Gamma_2$. Clearly, we have $(L, \mathcal{O}) \subset (K_2, \mathcal{O}_2)$.

Claim: $(K_1, \mathcal{O}_1) \subset (L, \mathcal{O})$**.**

Consider $\mathcal{O} \cap K_1 = \mathcal{O}_2 \cap K_1(x) \cap K_1 = (\mathcal{O}_2 \cap K_1) \cap K_1(x) = \mathcal{O}_1 \cap K_1(x) = \mathcal{O}_1$, because $\mathcal{O}_2 \cap K_1 = \mathcal{O}_1$ and $\mathcal{O}_1 \subseteq K_1 \subseteq K_1(x)$. Therefore, we have $(K_1, \mathcal{O}_1) \subseteq (L, \mathcal{O}) \subseteq (K_1, \mathcal{O}_2)$. Now, $L = K_1(x)$ and x is algebraic over K_1, hence $[L : K_1] < \infty$. Thus, from the previous corollary, we have $[\Gamma_L : \Gamma_1] < \infty$. Clearly, $\Gamma_1 = v(K^\times) \subset v(L^\times) = \Gamma$ and both are abelian groups. Thus $\Gamma_1 \lhd \Gamma$. Therefore Γ/Γ_1 is a group and it is finite. Therefore, $\exists n \in \mathbb{N}$ such that for all $\gamma \in \Gamma$ we have $n\gamma \in \Gamma_1$, showing that Γ_2/Γ_1 is torsion.

2. Take any $x \in \mathcal{O}_2^\times$ and define L as before, then proceeding similarly as before, we obtain $\overline{L}/\overline{\mathcal{K}_1}$ is finite (by the previous corollary) and hence $\overline{x}$ is algebraic over $\overline{\mathcal{K}_1}$.

☕

Lemma 1.5.2. *Suppose $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_n$ are valuation rings of a field K with maximal ideals $\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_n$. Let $R = \bigcap_{i=1}^n \mathcal{O}_i$ and $\mathfrak{p}_i = R \cap \mathcal{M}_i$. Then $\forall\, i,\ R_{\mathfrak{p}_i} = \mathcal{O}_i$.*

Proof. We first show that $R_{\mathfrak{p}_i} \subseteq \mathcal{O}_i$. Let $a/b \in R_{\mathfrak{p}_i}$ with $a, b \in R$ and $b \notin \mathfrak{p}_i$. Then $b \notin \mathcal{M}_i$, so $b^{-1} \in \mathcal{O}_i^\times$. Since $a \in R \subseteq \mathcal{O}_i$, we have $ab^{-1} = a/b \in \mathcal{O}_i$.

Conversely, let $a \in \mathcal{O}_i$ and set $I_a = \{j \mid a \in \mathcal{O}_j\}$. Write $\alpha_j = a + \mathcal{M}_j \in \overline{\mathcal{K}_j}$ for each $j \in I_a$. Choose a prime $p \in \mathbb{N}$ such that for all $j \in I_a$ we have $p > \operatorname{char}(\overline{\mathcal{K}_j})$ and α_j is not a primitive pth root of unity. Set $b = 1 + a + \cdots + a^{p-1}$. Observe that

$$\alpha_j = \overline{a} = 1 \text{ implies } \overline{b} = 1 + 1 + \cdots + 1 = p \neq 0 \text{ in } \overline{\mathcal{K}_j}$$

$$\alpha_j = \overline{a} \neq 1 \text{ implies } \overline{b} = \frac{1 - \alpha_j^p}{1 - \alpha_j} \neq 0 \text{ in } \overline{\mathcal{K}_j}.$$

Thus, $b \notin \mathcal{M}_j$ in both cases, hence $b \in \mathcal{O}_j^\times\ \forall j \in I_a$. For $j \in \{1, 2, \ldots, n\} \backslash I_a,\ a \notin \mathcal{O}_j \implies a^{-1} \in \mathcal{O}_j$ and $a^{-1} \in \mathcal{M}_j$, since a^{-1} is a nonunit of $\mathcal{O}_j$. Thus, $1 + a^{-1} + \cdots + a^{-(p-1)} \in \mathcal{O}_j^\times$, implying $b^{-1} = a^{-(p-1)}\big(1 + a^{-1} + \cdots + a^{-(p-1)}\big)^{-1} \in \mathcal{O}_j$, and so $ab^{-1} = a^{-(p-2)}\big(1 + a^{-1} + \cdots + a^{-(p-1)}\big)^{-1} \in \mathcal{O}_j$.

Thus for all $j = 1, \ldots, n$ we have $b^{-1},\ ab^{-1} \in \mathcal{O}_j$. Therefore $b^{-1},\ ab^{-1} \in R$, and $b^{-1} \notin \mathcal{M}_i \cap R = \mathfrak{p}_i$, since $b \in \mathcal{O}_i^\times$. Hence $a = \dfrac{ab^{-1}}{b^{-1}} \in R_{\mathfrak{p}_i}$. ☕

Theorem 1.5.5. *Suppose $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_n$ are valuation rings of a field K with maximal ideals $\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_n$. Let $R = \bigcap_{i=1}^n \mathcal{O}_i$ and $\mathfrak{p}_i = R \cap \mathcal{M}_i$. Further, suppose that $\mathcal{O}_i \nsubseteq \mathcal{O}_j$ for all $i \neq j$. Then*

1. *for all $i \neq j$, $\mathfrak{p}_i \nsubseteq \mathfrak{p}_j$;*

2. $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ *is the set of all maximal ideals of* R*;*

3. *for each* n*-tuple* $(a_1, \ldots, a_n) \in \mathcal{O}_1 \times \cdots \times \mathcal{O}_n$*, there exists an* $a \in R$ *with* $a - a_i \in \mathcal{M}_i$*.*

Proof. 1. Suppose not, i.e., $\exists i \neq j$ with $\mathfrak{p}_i \subseteq \mathfrak{p}_j$. By the previous lemma, $\mathcal{O}_j = R_{\mathfrak{p}_j} \subseteq R_{\mathfrak{p}_i} = \mathcal{O}_i$, but this contradicts the hypothesis.

2. **Claim: every ideal $\mathfrak{a} \neq R$ is contained in some $\mathfrak{p}_i$, $i = 1, \ldots, n$.**

   Suppose not, i.e., there exists an ideal $\mathfrak{a} \neq R$ such that for each $i = 1, \ldots, n$, there exists $a_i \in \mathfrak{a} \setminus \mathfrak{p}_i$. For each $i \neq j$, use (1) to pick $b_{ij} \in \mathfrak{p}_i \setminus \mathfrak{p}_j$. Then

   $$c_j := \prod_{i \neq j} b_{ij} \in \mathfrak{p}_i \setminus \mathfrak{p}_j, \text{ for every } j = 1, \ldots, n.$$

   Consequently, $a_j c_j \in \mathfrak{p}_i$ for all $i \neq j$ and $a_j c_j \notin \mathfrak{p}_j$. This is because $\mathfrak{p}_j$ is prime, since it is the contraction of the prime ideal $\mathcal{M}_j$ to R.

   Consider $d := \sum_{j=1}^{n} a_j c_j \notin \mathfrak{p}_i$ for all $i = 1, \ldots, n$. Now, $d \in \mathfrak{a} \subset R$ but $d \notin \mathfrak{p}_i = R \cap \mathcal{M}_i \implies d \notin \mathcal{M}_i$, implying $d^{-1} \in \mathcal{O}_i$, for every i such that $1 \leq i \leq n$. Hence $d^{-1} \in R$, yielding $1 = dd^{-1} \in \mathfrak{a}$, a contradiction, since $\mathfrak{a} \neq R$. This proves the claim. Now, note that the above claim holds for any ideal. In particular, it holds for maximal ideals, whence we conclude that every maximal ideal is equal to some $\mathfrak{p}_i$, $i = 1, \ldots, n$. Thus, the set of maximal ideals in a subset of $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. But by (1.), all the $\mathfrak{p}_i$ are distinct, hence the set of maximal ideals must be exactly equal to $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$.

3. For $i \neq j$, $\mathfrak{p}_i + \mathfrak{p}_j = R$, since the only maximal ideals are $\mathfrak{p}_i$ and $\mathfrak{p}_i \nsubseteq \mathfrak{p}_j$. Therefore, by the Chinese Remainder Theorem, the canonical map

   $$R \longrightarrow R/\mathfrak{p}_1 \times \cdots \times R/\mathfrak{p}_n$$

   is surjective. We know, for each i, $R_{\mathfrak{p}_i}/\mathfrak{p}_i R_{\mathfrak{p}_i} \cong R/\mathfrak{p}_i$, and $R_{\mathfrak{p}_i} = \mathcal{O}_i$, it follows that

   $$R \longrightarrow \mathcal{O}_1/\mathcal{M}_1 \times \cdots \times \mathcal{O}_n/\mathcal{M}_n$$

   is surjective. Hence, given any $(\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_n) \in \prod_i \mathcal{O}_i/\mathcal{M}_i$, there exists $a \in R$ such that $a \equiv a_i \mod \mathcal{M}_i$ for all $i \implies a - a_i \in \mathcal{M}_i$.

Lemma 1.5.3. *Suppose* K_2/K_1 *is an algebraic extension of fields and* $\mathcal{O} \subset K_1$ *is a valuation ring. Let* $\mathcal{O}', \mathcal{O}'' \subset K_2$ *be valuation rings lying over* $\mathcal{O}$*.*
If $\mathcal{O}' \subset \mathcal{O}''$*, then* $\mathcal{O}' = \mathcal{O}''$*.*

Proof. We have $\mathcal{O}' \cap K_1 = \mathcal{O}'' \cap K_1 = \mathcal{O}$ and $\mathcal{O}' \subset \mathcal{O}''$, which implies $\mathcal{M}'' \subset \mathcal{M}'$. Hence, we have $\mathcal{O}'/\mathcal{M}'' = \overline{\mathcal{O}'} \subset \mathcal{O}''/\mathcal{M}'' = \overline{\mathcal{K}''}$. Consider the natural order-preserving homomorphism $\mathcal{O}'' \twoheadrightarrow \overline{\mathcal{K}''}$. The image of $\mathcal{O}'$ under this map is $\mathcal{O}'/\mathcal{M}'' = \overline{\mathcal{O}'}$.

Claim: $\overline{\mathcal{O}'}$ is a valuation ring of $\overline{\mathcal{K}''}$: let $\overline{x} \in \overline{\mathcal{K}''}$ be arbitrary; look at its preimage $x \in \mathcal{O}''$. If $x \in \mathcal{O}'$, then $\overline{x} \in \overline{\mathcal{O}'}$ and we are done. If not, then we must have $x^{-1} \in \mathcal{O}'$, as $\mathcal{O}'$ is a valuation ring. Then, $\overline{x^{-1}} = \overline{x}^{-1} \in \overline{\mathcal{O}'}$. Thus, given any $\overline{x} \in \overline{\mathcal{K}''}$, we must have either $\overline{x} \in \overline{\mathcal{O}'}$ or $\overline{x}^{-1} \in \overline{\mathcal{O}'}$ — this proves the claim.

We will now show that $\overline{\mathcal{O}'} = \overline{\mathcal{K}''}$. First, to see that $\overline{\mathcal{O}'}$ is a field, take any nonzero $x \in \overline{\mathcal{O}'}$. We have seen previously that the extension $\overline{\mathcal{K}''}/\overline{\mathcal{K}}$ of residue class fields is algebraic, hence there exist $a_0, a_1, \dots, a_r \in \overline{\mathcal{K}}$ such that $a_0 + a_1 x + \cdots + a_r x^r = 0$ in $\overline{\mathcal{O}'}$. Assume without loss of generality that $a_0 \neq 0$. Note that since $a_0 \in \overline{\mathcal{K}} = \mathcal{O}'/\mathcal{M}'$, which is a field, hence its inverse a_0^{-1} is also in $\mathcal{O}'/\mathcal{M}' \subset \mathcal{O}'/\mathcal{M}'' = \overline{\mathcal{O}}$. Thus, the element $y = -a_0^{-1}(a_1 + \cdots a_r x^{r-1}) \in \overline{\mathcal{O}'}$. It is clear that $xy = 1$, hence $\overline{\mathcal{O}'}$ is a field so it must equal its field of fractions $\overline{\mathcal{K}''}$. We then have $\mathcal{M}''$ is a maximal ideal of $\mathcal{O}'$, but $\mathcal{O}'$ is a local ring so $\mathcal{M}' = \mathcal{M}''$ whence it follows that $\mathcal{O}' = \mathcal{O}''$. ☕

Given an algebraic extension K_2 of K_1 and a valuation ring $\mathcal{O}_1$ of K_1, there may exist infinitely many valuation rings of K_2 lying over $\mathcal{O}_1$. In certain cases, there is a natural bound. Let $K_2 \cap K_1^s = \{x \in K_2 \mid x \text{ is separable over } K_1\}$. The field $K_2 \cap K_1^s$ is a separable extension of K_1.

Definition 1.5.4. $[K_2 \cap K_1^s : K_1]$ is called the ***degree of separability*** of K_2 over K_1. Moreover, $[K_2 : K_2 \cap K_1^s]$ is called the ***degree of inseparability*** of K_2 over K_1.

Every $x \in K_2 \setminus (K_2 \cap K_1^s)$ is purely inseparable over $K_2 \cap K_1^s$.

We use the following notations: $[K_2 : K_1]_s = [K_2 \cap K_1^s : K_1]$, $[K_2 : K_1]_i = [K_2 : K_2 \cap K_1^s]$.

Theorem 1.5.6. *Let K_2 be algebraic over K_1, and $[K_2 : K_1]_s < \infty$. Let $\mathcal{O}$ be a valuation ring of K_1. Then the number n of all prolongations of $\mathcal{O}$ to K_2 is finite, and $n \leq [K_2 : K_1]_s$.*

Proof. Let $\mathcal{O}_1, \dots, \mathcal{O}_m$ be distinct prolongations of $\mathcal{O}$ to K_2, with maximal ideals $\mathcal{M}_1, \dots, \mathcal{M}_m$, respectively. Since they are distinct, they must be pairwise incomparable, by the previous lemma. Consider now the elements $e_j := (0, \dots 1, \dots, 0) \in \prod_{i=1}^m \mathcal{O}_i$. For every j, using Theorem 1.5.5 (3), we conclude the existence of a c_j

such that $c_j - 1 \in \mathcal{M}_j$ and $c_i \in \mathcal{M}_j$ for $i \neq j$. Hence, we obtain $c_1, \ldots, c_m$ such that for all $i, j \in \{1, \ldots, m\}$, $c_j - 1 \in \mathcal{M}_j$ and $c_i \in \mathcal{M}_j$ for $i \neq j$.

We consider two cases:

(i) char $K_1 = p > 0$: we pick $k \in \mathbb{N}$ large enough to ensure the separability of $c_1^{p^k}, \ldots, c_m^{p^k}$ over K_1.

(ii) char $K_1 = 0$: we proceed as above and simply take $k = 0$.

Claim: These m elements are linearly independent over K_1

Suppose not. Then there exist a_i, not all zero, such that $\sum_{i=1}^{m} a_i c_i^{p^k} = 0$. Pick $j \leq n$ such that $v(a_j) = \min_{i \leq m} v(a_i)$. Note that $a_j \neq 0$, otherwise $v(a_j) = \infty \implies v(a_i) = \infty \implies a_i = 0$ for all i. Thus, $c_j^{p^k} = -\sum_{i \neq j} a_i c_i^{p^k} \in \mathcal{M}_j$. Hence, $v_j(c_j^{p^k}) = p^k v_j(c_j) > 0 \implies v_j(c_j) > 0 \implies c_j \in \mathcal{M}_j$. In particular, we have both $c_j - 1 \in \mathcal{M}_j$ and $c_j \in \mathcal{M}_j \implies 1 \in \mathcal{M}_j$, which is a contradiction. This proves the claim and hence $m \leq [K_2 : K_1]_s$.

Note that we may repeat the above argument with $m + 1$ distinct valuations and thus similarly show that $m + 1 \leq [K_2 : K_1]_s$. Proceeding inductively, we can conclude that there can only be finitely many extensions of $\mathcal{O}$ to K_2 since $[K_2 : K_1]_s < \infty$. Moreover, this number must be bounded above by $[K_2 : K_1]_s$ as seen above. This concludes the proof. ☕

Corollary 1.5.6.1. *Suppose K_2 is a purely inseparable algebraic extension of K_1. Then every valuation ring $\mathcal{O}$ of K_1 has exactly one prolongation to K_2.*

Lemma 1.5.4. *Suppose K is a field with a non-trivial valuation v. For every polynomial*

$$g(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n \in K[x]$$

and every γ in the value group Γ of v, there exists a separable polynomial

$$h(x) = b_0 + b_1 x + \cdots + b_{n-1} x^{n-1} + x^n \in K[x]$$

such that $v(a_i - b_i) > \gamma$ for every i with $0 \leq i < n$.

Proof. Let $y_0, y_1, \ldots, y_{n-1}$ be indeterminates over K. Construct

$$f_y(x) = f_{y_0, y_1, \ldots, y_{n-1}}(x) = \sum_{i=0}^{n-1} (a_i + y_i) x^i + x^n \in K(y_0, y_1, \ldots, y_{n-1})[x].$$

Consider the resultant $\mathrm{Res}(f_y, f_y') = \mathrm{disc}(f)$. By the algebraic independence of $y_0, y_1, \ldots, y_{n-1}$ over K, it follows that $\mathrm{Res}(f_y, f_y')$ is a nontrivial polynomial R in

$K[y_0, y_1, \ldots, y_{n-1}]$. Since v is nontrivial, $\exists x \in K$ such that $v(x) = \alpha \neq 0$. Then, $v(x^n) = n\alpha \neq 0\ \forall n \in \mathbb{N}$. Hence, $v(K) = \Gamma$ is infinite. Therefore, K cannot be a finite field. Hence $\forall \delta \in \Gamma, \{x \in K \mid v(x) > \delta\}$ is an infinite set, otherwise it would be a closed set.

Claim: For a nonconstant polynomial $g(x_1, \ldots, x_n)$ **in** $K[x_1, \ldots, x_n]$ **and an infinite subset** $M \subseteq K$, $\exists (m_1, \ldots, m_n) \in M^n$ **such that** $g(m_1, \ldots, m_n) \neq 0$.

We prove this by induction on n. For $n = 1$, we have a polynomial $g(x) \in K[x]$. Suppose $g(x) = 0\ \forall x \in M$, since M is infinite, g has infinite roots, i.e. $g \equiv 0$, a contradiction. Thus, there exists $y \in M$ such that $g(y) \neq 0$.

We now assume the claim for $n = k - 1$ and prove it for $n = k$. We have $g(x_1, \ldots, x_n)$. Fix some $y_n \in M$ and look at $g(x_1, x_2, \ldots, y_n) \in K[x_1, x_2, \ldots, x_{n-1}]$. By induction hypothesis, we have $(y_1, \ldots, y_{n-1}) \in M^{n-1}$ such that $g(y_1, y_2, \ldots, y_n) \neq 0$. Thus, we have a $(y_1, y_2, \ldots, y_n) \in M^n$ such that $g(y_1, \ldots, y_n) \neq 0$.

Applying the claim with $M = \{x \in K \mid v(x) > \delta\}$ and $g = R$, we get $c_0, c_1, \ldots, c_n \in M$ such that $R(c_0, c_1, \ldots, c_n) \neq 0$. Now, $c_i \in M \implies v(c_i) > \delta$.

Set $h(x) := x^n + \sum_{i=0}^{n-1}(a_i + c_i)x^i = (a_0 + c_0) + (a_1 + c_1)x + \ldots + x^n$. It follows that $\mathrm{Res}(h, h') = \mathrm{disc}(h) \neq 0.$, i.e., h and h' have no common roots, i.e., $h(x)$ has no repeated roots, i.e., h is a separable polynomial.

We shall use this lemma to prove the following theorem:

Theorem 1.5.7. *Suppose K is a separably closed field and $\mathcal{O}$ is a proper valuation ring of K. Let $\widetilde{K}$ be an algebraic closure of K and let $\widetilde{\mathcal{O}}$ be the unique extension of $\mathcal{O}$ to $\widetilde{K}$. Then $\widetilde{\mathcal{O}}/\mathcal{O}$ is an immediate extension. In particular, the residue class field $\overline{\mathcal{K}}$ of $\mathcal{O}$ is algebraically closed, and the value group Γ of $\mathcal{O}$ is divisible, i.e., for every $\gamma \in \Gamma$ and any $n \in \mathbb{N} \setminus \{0\}$, there exists $\delta \in \Gamma$ such that $n\delta = \gamma$.*

Proof. Let $\widetilde{\Gamma}$ and $\overline{\widetilde{\mathcal{K}}}$ denote the value group and residue class field of $\widetilde{\mathcal{O}}$.

Note that the multiplicative group $\widetilde{K}^\times$ of $\widetilde{K}$ is divisible. To see this, let $a \in \widetilde{K}^\times$ and $n \in \mathbb{N}$. Consider $g(x) = x^n - a$. Since $\widetilde{K}$ is an algebraic closure of K, $g(x)$ has a root in $\widetilde{K}$, say b. Then, $b^n = a$, whence we conclude that $\widetilde{K}^\times$ is divisible.

Now, $\widetilde{\Gamma} = \widetilde{K}^\times/\widetilde{\mathcal{O}}^\times$ is a quotient of a divisible group, hence it is also divisible. Similarly, for $a_0, a_1, \ldots, a_n \in \widetilde{\mathcal{O}},\ n > 0,\ a_n \in \widetilde{\mathcal{O}}^\times$, the polynomial $\overline{f}(x) = a_0 + a_1x + \ldots + a_nx^n \in \overline{\widetilde{\mathcal{K}}}[x]$ has a root in $\widetilde{K}$ since $f(x) = a_0 + a_1x + \ldots + a_nx^n$ has a root in $\widetilde{\mathcal{O}}$ because $\widetilde{\mathcal{O}}$ is integrally closed in $\widetilde{K}$.

Claim: $\overline{K} = \overline{\widetilde{\mathcal{K}}}$.

Take $x \in \widetilde{\mathcal{O}}^\times$ and let g be the minimal polynomial of $\overline{x}$ over $\overline{\mathcal{K}}$. Consider $g \in \mathcal{O}[x]$, say $g = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + x^n$. By the previous lemma, pick a separable polynomial $h(x) = x^n + \sum_{i=0}^{n-1} b_i x^i$ such that $v(a_i - b_i) > 0\ \forall 1 \le i < n$, then $g(x) - h(x) \in \mathcal{O}[x]$. Hence, $h(x) = g(x) - (g(x) - h(x)) \in \mathcal{O}[x]$. Further, note that $v(a_i - b_i) > 0 \implies g - h \in \mathcal{M}[x]$. Now, h is separable, hence it has a root z in K. We know that $\mathcal{O}$ is integrally closed in K, hence $z \in \mathcal{O}$. Now, $\overline{g}(\overline{z}) = \overline{g(z)} = \overline{g(z) - h(z)} = \overline{\sum_{i=0}^{n-1}(a_i - b_i)z^i} = 0$. As $\overline{g}$ is the minimal polynomial of $\overline{x}$ over $\overline{\mathcal{K}}$, it follows that $\overline{g}$ has degree one and hence $\overline{x} \in \overline{\mathcal{K}}$. This gives $\overline{\widetilde{\mathcal{K}}} \subseteq \overline{\mathcal{K}}$.

Conversely, $\mathcal{O} \subseteq \widetilde{\mathcal{O}}$ and $\mathcal{M} \subseteq \widetilde{\mathcal{M}} \implies \mathcal{O}/\mathcal{M} \subseteq \widetilde{\mathcal{O}}/\widetilde{\mathcal{M}} \implies \overline{\mathcal{K}} \subseteq \overline{\widetilde{\mathcal{K}}}$. Hence, $\overline{\mathcal{K}} = \overline{\widetilde{\mathcal{K}}}$.

Now, we will show $\Gamma = \widetilde{\Gamma}$. Let $\delta \in \widetilde{\Gamma}$, then by Theorem 1.5.4, $\exists n > 1$ and $a \in K$ such that $n\delta = v(a) \in \Gamma$ where v is a valuation corresponding to $\mathcal{O}$. Take $\delta > 0$ without loss of generality and so $v(a) = n\delta > 0 \implies a \in \mathcal{O}$.

Let $g(x) = x^n - a$. By the previous lemma, there exists a separable polynomial $h(x) = x^n + \sum_{i=0}^{n-1} b_i x^i$ with $v(a_i - b_i) > n\delta\ \forall i = 1, 2, \ldots, n$. Note that the a_i here are all zero except $a_0 = -a$. As before, h has a root $z \in \mathcal{O}$ and we have $v(g(z)) = v(g(z) - h(z)) \ge \min_{0 \le i < n}\{v(a_i - b_i) + iv(z)\} > n\delta + \min_{0 \le i < n}\{iv(z)\} = n\delta = v(a)$, because $v(z) \ge 0 \implies z \in \mathcal{O}$. Hence, $v(g(z)) > v(a) \implies v(z^n - a) > v(a) \implies v(z^n) = v(z^n - a + a) = v(a) = n\delta \implies v(z) = \delta \in \Gamma$. Hence, $\widetilde{\Gamma} \subseteq \Gamma$. As before, $\Gamma \subseteq \widetilde{\Gamma}$ follows trivially. Therefore $\widetilde{\mathcal{O}}/\mathcal{O}$ is an immediate extension and we are done.

☕

We now show that the integral closure of a valuation ring in an algebraic extension of its field of fractions has a localisation property in the following sense:

Theorem 1.5.8. *Let L be an algebraic extension of a field K, and let $\mathcal{O}$ be a valuation ring of K. Denote by R the integral closure of $\mathcal{O}$ in L and let $\mathcal{O}'$ be a prolongation of $\mathcal{O}$ to L. If $\mathcal{M}'$ is the maximal ideal of $\mathcal{O}'$ and $\mathfrak{m} = \mathcal{M}' \cap R$, then $R_\mathfrak{m} = \mathcal{O}'$.*

Proof. The containment $R_\mathfrak{m} \subset \mathcal{O}'$ is easy: take any $a/b \in R_\mathfrak{m}$ i.e., $a \in R, b \in R \setminus \mathfrak{m} \subset \mathcal{M}$. Since $b \notin \mathcal{M}$, it follows that $b^{-1} \in \mathcal{O}'$. Now, $a \in R$ and $\mathcal{O}'$ is integrally closed in L, whence we get $a \in \mathcal{O}' \implies ab^{-1} = a/b \in \mathcal{O}'$.

For the converse, let $x \in \mathcal{O}'$. Set $K_2 := K(x)$, $R_2 := R \cap K_2$, $\mathfrak{m}_2 := \mathfrak{m} \cap K_2$, $\mathcal{O}'_2 := \mathcal{O}' \cap K_2$, and $\mathcal{M}_2 := \mathcal{M} \cap K_2$. Since R is the integral closure of $\mathcal{O}$ in L and $K_2 \subset L$, it follows that R_2 is the integral closure of $\mathcal{O}$ in K_2. Hence, via Corollary 1.5.3.1, we obtain $R_2 = \bigcap \mathcal{O}''$ where $\mathcal{O}''$ ranges over all prolongations of $\mathcal{O}$ to K_2. Note that since x is algebraic over K, we have $[K_2 : K] < \infty \implies [K_2 : K]_s < \infty$. We have seen before that in this case $n < [K_2 : K]_s$, i.e., n is finite. Hence, applying Lemma 1.5.2. with $\mathfrak{p}_2 = R_2 \cap \mathcal{M}_2 = (R \cap K_2) \bigcap (\mathcal{M} \cap K_2) = (R \cap \mathcal{M}) \bigcap K_2 = \mathfrak{m} \cap K_2 = \mathfrak{m}_2$, we get $\mathcal{O}_2 = (R_2)_{\mathfrak{m}_2}$. Therefore, there exist $a, b \in R_2$ with $b \notin \mathfrak{m}_2$ such that $x = ab^{-1}$. Clearly, $ab^{-1} \in R_{\mathfrak{m}} \implies x \in R_{\mathfrak{m}}$, yielding $\mathcal{O}' \subset R_{\mathfrak{m}}$.

We now focus on normal extensions and prove some results on prolongations of a fixed valuation ring.

Theorem 1.5.9. *Suppose L/K is a finite normal extension of fields, with $G = Aut(L/K)$. Suppose $\mathcal{O}$ is a valuation ring of K, and $\mathcal{O}'$ and $\mathcal{O}''$ are valuation rings in L extending $\mathcal{O}$. Then $\mathcal{O}'$ and $\mathcal{O}''$ are conjugate over K, i.e., there exists $\sigma \in G$ with $\sigma\mathcal{O}' = \mathcal{O}''$.*

Proof. We have $K \subset L \cap K^s \subset L$. Set $L^s := L \cap K^s$. By Corollary 1.5.6.1., every prolongation of $\mathcal{O}$ to L^s can be uniquely extended to L. We also know from Galois theory that there is a canonical isomorphism $\mathrm{Aut}(L/K) \xrightarrow{\sim} \mathrm{Aut}(L^s/K)$. Hence, it suffices to consider the case where L/K is separable. Let

$$H' = \{\sigma \in G : \sigma\mathcal{O}' = \mathcal{O}'\} \leq G$$

$$H'' = \{\sigma \in G : \sigma\mathcal{O}'' = \mathcal{O}''\} \leq G$$

Claim: For every $\sigma \in H'$, we have $\sigma\mathcal{M}' = \mathcal{M}'$.

This follows because $\sigma\mathcal{O}' = \mathcal{O}'$ and if $\sigma(x) \in \mathcal{O}' \setminus \mathcal{M}'$ for some $x \in \mathcal{M}'$ then $\sigma(x)$ is a unit in $\mathcal{O}'$, i.e., $\sigma(x)^{-1} = \sigma(x^{-1}) \in \mathcal{O}' = \sigma\mathcal{O}' \implies x^{-1} \in \mathcal{O}'$ which contradicts the fact that $x \in \mathcal{M}'$. Now, $\sigma\mathcal{O}'$ is a valuation ring of L since $\sigma\mathcal{O}' = \mathcal{O}'$. By the above argument, it also follows that its maximal ideal is $\sigma\mathcal{M}'$. Similarly, for every $\tau \in H''$, we have $\tau\mathcal{O}''$ is a valuation ring of L with maximal ideal $\tau\mathcal{M}''$. We next write G as the following disjoint unions:

$$G = \coprod_{i=1}^{n} H'\sigma_i^{-1} = \coprod_{j=1}^{m} H''\tau_j^{-1}$$

It then suffices to simply show that there exist i, j such that $\sigma_i\mathcal{O}' \subseteq \tau_j\mathcal{O}''$ or $\sigma_i\mathcal{O}' \supseteq \tau_j\mathcal{O}''$, since this implies $\sigma_i\mathcal{O}' = \tau_j\mathcal{O}''$, by Lemma 1.5.3. We then have $\tau_j^{-1}\sigma_i\mathcal{O}' = \mathcal{O}''$, thus finishing the proof. Thus, we need only show the existence of such i, j. Proceeding by contradiction, we assume no such i, j exist. Since $\{\sigma_i^{-1}\}_{i=1}^n$ is a transversal for G/H', we must have $\sigma_k\mathcal{O}' \nsubseteq \sigma_t\mathcal{O}'$ for all $k \neq t$ otherwise we would obtain $\sigma_k\mathcal{O}' = \sigma_t\mathcal{O}'$ using Lemma 1.5.3. Similarly $\tau_k\mathcal{O}'' \nsubseteq \tau_t\mathcal{O}''$ for all $k \neq t$. Set

$$R = \left(\bigcap_{i=1}^{n} \sigma_i\mathcal{O}'\right) \bigcap \left(\bigcap_{j=1}^{m} \tau_j\mathcal{O}''\right)$$

Using Theorem 1.5.5.(3) with the tuple $(1,\dots,1,0,\dots,0) \in \prod_{i=1}^n \sigma_i\mathcal{O}' \times \prod_{j=1}^m \tau_j\mathcal{O}''$, we obtain $a \in R$ such that

$$a - 1 \in \sigma_i(\mathcal{M}') \text{ for } i = 1,\dots,n \text{ and}$$
$$a \in \tau_j(\mathcal{M}') \text{ for } j = 1,\dots,m.$$

Hence, for $\sigma \in G_1$, write $\sigma = \rho\sigma_i^{-1} \in H'\sigma_i \implies \rho \in H'$. This yields $\sigma(a-1) = \rho\sigma_i^{-1}(a-1) \in \rho\sigma_i^{-1}(\sigma_i(\mathcal{M}')) = \rho(\mathcal{M}') = \mathcal{M}'$. Similarly, $\sigma(a) \in \mathcal{M}''$ for all $\sigma \in G$. Now, $N_{L/K}(a) = \prod_{\sigma\in G_1}\sigma(a) \in (\mathcal{M}''+1) \cap K = \mathcal{M}+1$, where the last equality follows by observing that $1 + m' \in K \implies m' \in K \cap \mathcal{M}' = \mathcal{M}$ for any $m' \in \mathcal{M}'$. Furthermore, we also have $N_{L/K}(a) = \prod_{\sigma\in G_1}\sigma(a) \in \mathcal{M}'' \cap K = \mathcal{M}$. This is a contradiction, and we are done.

Theorem 1.5.10 (Conjugation Theorem)**.** *Suppose L/K is an arbitrary normal extension of fields, $\mathcal{O}$ is a valuation ring of K, and $\mathcal{O}'$ and $\mathcal{O}''$ are valuation rings in L extending $\mathcal{O}$. Then there exists $\sigma \in Aut(L/K)$ with $\sigma(\mathcal{O}') = \mathcal{O}''$.*

Proof. Consider Σ, the set of ordered pairs (K_1,σ_1) where K_1 is a normal extension of L/K, i.e. $L/K_1/K$ with K_1/K normal, $\mathcal{O}_1' := \mathcal{O}' \cap K_1$, $\mathcal{O}_1'' := \mathcal{O}'' \cap K_1$ and $\sigma_i \in \mathrm{Aut}(K_1/K)$ such that $\sigma_1(\mathcal{O}_1') = \mathcal{O}_1''$.

Clearly, $\Sigma \neq \emptyset$ since $(K,\mathrm{id}) \in \Sigma$. We may partially order Σ as

$$(K_1,\sigma_1) \le (K_2,\sigma_2) \iff K_1 \subseteq K_2 \text{ and } \sigma_2|_{K_1} = \sigma_1.$$

Take a chain $(K_i,\sigma_i)_{i\in\mathbb{N}}$ in Σ. Consider (K,σ) where $K := \bigcup K_i$ and $\sigma|_{K_i} := \sigma_i$. Since K_m is a composition of countably many normal extensions contained in L, K_m is also a normal extension of L/K. Thus, $(K,\sigma) \in \Sigma$ and we have an upper bound, whence, by Zorn's Lemma, Σ has a maximal element, say (K_m,σ_m). We have $K \subseteq K_m \subseteq L$ and $\sigma_m(\mathcal{O}_m') = \mathcal{O}_m''$, where $\mathcal{O}_m' = \mathcal{O}' \cap K_m$ and $\mathcal{O}_m'' = \mathcal{O}'' \cap K_m$.

Claim: $K_m = L$**.**

Suppose not. Pick $\alpha \in L \setminus K_m$. Let f be the minimal polynomial of α over K_m and $N = SF_L(f)\cdot K_m = SF_{K_m}(f) \subseteq L$, where $SF_L(f)$ denotes the splitting field of f over L. We extend σ_m to an algebraic closure $\widetilde{K}/K$. Then, since N and L are normal, $\sigma_m(L) = L$ and $\sigma_m(N) = N$. Let $\mathcal{O}^* := \mathcal{O}' \cap N$ and $\mathcal{O}^{**} := \sigma_m^{-1}(\mathcal{O}'' \cap N)$. Consider $\mathcal{O}^* \cap K_m = \mathcal{O}' \cap N \cap K_m = \mathcal{O}' \cap (SF_{K_m}(f) \cap K_m) = \mathcal{O}' \cap K_m = \mathcal{O}_m'$. Similarly,

$$\begin{aligned}\mathcal{O}^{**} \cap K_m &= \sigma_m^{-1}(\mathcal{O}'' \cap N) \cap K_m \\ &= \sigma_m^{-1}(\mathcal{O}'' \cap N) \cap \sigma_m^{-1}(\sigma_m(K_m)) \\ &= \sigma_m^{-1}(\mathcal{O}'' \cap N \cap \sigma_m(K_m)) \\ &= \sigma_m^{-1}(\mathcal{O}'' \cap (SF_{K_m}(f) \cap K_m)) \\ &= \sigma_m^{-1}(\mathcal{O}'' \cap K_m) = \sigma_m^{-1}(\mathcal{O}_m'') = \mathcal{O}_m'\end{aligned}$$

We now apply the previous theorem with $L \mapsto N$, $K \mapsto K_m$, $\mathcal{O}' \mapsto \mathcal{O}^*$ and $\mathcal{O}'' \mapsto \mathcal{O}^{**}$. Note that N is a splitting field, hence normal. We then get an automoprhism $\sigma \in \mathrm{Aut}(N/K_m)$ with $\sigma(\mathcal{O}^*) = \mathcal{O}^{**}$. Then, $(\sigma_m \circ \sigma)(\mathcal{O}' \cap N) = \sigma_m(\sigma(\mathcal{O}^*)) = \sigma_m(\mathcal{O}^{**}) = \mathcal{O}'' \cap N$. Thus, $(N, \sigma_m \circ \sigma) > (K_m, \sigma_m)$ and $(N, \sigma_m \circ \sigma) \in \Sigma$. This contradiction proves the claim.

Finally, we conclude this section by collecting some useful properties of normal extensions:

Proposition 1.5.1. *Let N be a normal extension of a field K, $\mathcal{O}$ a valuation ring of K, and $\mathcal{O}'$ a valuation ring of N lying over $\mathcal{O}$. Let $v : K \twoheadrightarrow \Gamma \cup \{\infty\}$ and $v' : N \twoheadrightarrow \Gamma' \cup \{\infty\}$ be valuations corresponding to $\mathcal{O}$ and $\mathcal{O}'$, respectively, and assume that $v'|_K = v$. Denote the residue class field of $\mathcal{O}'$ by $\overline{N}$.*

1. *For $\sigma \in Aut(N/K)$, the map $v' \circ \sigma$ is the unique valuation of N corresponding to $\sigma^{-1}(\mathcal{O}')$ and Γ'. In particular, if $\sigma(\mathcal{O}') = \mathcal{O}'$, then $v' \circ \sigma = v'$.*
2. *$\overline{N}/\overline{\mathcal{K}}$ is a normal extension.*
3. *The map $\sigma^{-1}(\mathcal{O}') \to \overline{N} : x \mapsto \sigma(x)$ is a ring homomorphism which induces a $\overline{\mathcal{K}}$-isomorphism from $\sigma^{-1}(\mathcal{O}')/\sigma^{-1}(M') \to \overline{N}$ satisfying $\overline{\sigma}(u + \sigma^{-1}(\mathcal{M}')) = \overline{\sigma(u)}$ for every $u \in \sigma^{-1}(\mathcal{O}')$. In particular, if $\sigma(\mathcal{O}') = \mathcal{O}'$, then $\overline{\sigma} \in Aut(\overline{N}/\overline{\mathcal{K}})$.*
4. *$e(\sigma^{-1}(\mathcal{O}')/\mathcal{O}) = e(\mathcal{O}'/\mathcal{O})$ and $f(\sigma^{-1}(\mathcal{O}')/\mathcal{O}) = f(\mathcal{O}'/\mathcal{O})$, for every $\sigma \in Aut(N/K)$.*

Proof. 1. Clearly, $v' \circ \sigma : N \to \Gamma' \cup \{\infty\}$ is a valuation on N such that

$$\sigma^{-1}(\mathcal{O}') = \{x \in N : \sigma(x) \in \mathcal{O}'\} = \{x \in N : (v' \circ \sigma)(x) \geq 0\}.$$

Let w be a valuation with valuation ring $\sigma^{-1}(\mathcal{O}')$, then $v' \circ \sigma$ and w are equivalent. Therefore, there exists an order-preserving isomorphism

$$\rho : \Gamma' \xrightarrow{\sim} \Gamma' \text{ such that } \rho \circ w = v' \circ \sigma.$$

Claim: $\rho(\gamma) = \gamma$ for all $\gamma \in \Gamma = v(K^\times)$.

Let $\gamma \in \Gamma$ be arbitrary, i.e., $\gamma = v(t)$ for some $t \in K^\times$. Then $\rho^{-1}(\gamma) = \rho^{-1}(v(t)) = \rho^{-1}(v'(t)) = \rho^{-1}(v'(\sigma(t))) = \rho^{-1}(\rho(w(t))) = w(t)$. Now we know that $\sigma^{-1}(\mathcal{O}')$ lies over $\mathcal{O}$, hence $w|_K = v$, whence we conclude $w(t) = v(t)$. Therefore, the claim follows. For any $\delta \in \Gamma'$, we apply Theorem 1.5.4. to get an $n > 1$ such that $n\delta \in \Gamma$. Hence, $n\rho(\delta) = \rho(n\delta) = n\delta$ gives $\rho(\delta) = \delta$, since Γ' is torsion-free. Hence, ρ is the identity map on Γ' and so $w = v' \circ \sigma$.

2. Let $\overline{f}$ be an irreducible polynomial over $\overline{K}$ with a root $\alpha \in N$. Let R denote the integral closure of $\mathcal{O}$ in N and $\mathfrak{m} := \mathcal{M}' \cap R$. From Theorem 1.5.8., we have $\mathcal{O}' = R_{\mathfrak{m}}$, hence the residue class field map $\mathcal{O}' \twoheadrightarrow \overline{N}$ induces a map $R \twoheadrightarrow \overline{N}$, since any $\overline{x} \in \overline{N}$ has preimage $x \in \mathcal{O}' = R_{\mathfrak{m}}$, i.e., $x/1 \in R_{\mathfrak{m}} \implies x \in R$.

   Now for any $\sigma \in \operatorname{Aut}(N/K)$, we must have $\sigma(R) = R$, because $\sigma(\mathcal{O}') \subset N$ is a valuation ring lying over $\mathcal{O}$ whenever $\mathcal{O}' \subset N$ is. Further, if $x \in R$, then x is integral over $\mathcal{O}$ if and only if $\sigma(x)$ is also integral over $\mathcal{O}$, i.e., $\sigma(x) \in R \iff x \in R$. Take a preimage $x \in R$ of $\alpha \in \overline{N}$, so $\overline{x} = \alpha$ in $\overline{N}$. Let g be the minimal polynomial of x over K, then $g(x) \in \mathcal{O}[x]$. By the normality of N/K, $g(x) = (x - x_1)(x - x_2) \dots (x - x_n)$ where $x_i \in R$ and $n = \deg(g)$. Consider then its image $\overline{g}$ in $\overline{(}N)$. We have $\overline{g}(\alpha) = 0$, but $\overline{f}$ is the the minimal polynomial of α over $\overline{N}$, whence we conclude $\overline{f} \mid (x - \overline{x_1})(x - \overline{x_2}) \dots (x - \overline{x_n})$. Thus, $\overline{f}$ splits in $\overline{N}$ and we are done.

3. Consider the map $\eta : \sigma^{-1}(\mathcal{O}') \xrightarrow{\sigma} \mathcal{O}' \twoheadrightarrow \overline{N}$. This map is clearly surjective since $\sigma|_{\mathcal{O}'} = \operatorname{id}|_{\mathcal{O}'}$ and the residue class field map $\mathcal{O}' \twoheadrightarrow \overline{N}$ is by definition surjective. Consider its kernel $\ker \eta = \{x \in \sigma^{-1}(\mathcal{O}') : \sigma(x) \in \mathcal{M}'\} = \sigma^{-1}(\mathcal{M}')$. Therefore, η induces an isomorphism $\widetilde{\eta} : \sigma^{-1}(\mathcal{O}')/\sigma^{-1}(\mathcal{M}') \xrightarrow{\sim} \overline{N}$. Let $\overline{x} \in \overline{\mathcal{K}}$, then $x \in \mathcal{O} \subset \sigma^{-1}(\mathcal{O}')$ and $x \notin \mathcal{M}$ whence $\sigma(x) \notin \mathcal{M}$, i.e., $\overline{x} \in \sigma^{-1}(\mathcal{O}')/\sigma^{-1}(\mathcal{M}')$. Therefore, $\overline{\mathcal{K}} \subset \sigma^{-1}(\mathcal{O}')/\sigma^{-1}(\mathcal{M}')$, hence we may consider $\overline{\mathcal{K}}$ as a subfield of $\sigma^{-1}(\mathcal{O}')/\sigma^{-1}(\mathcal{M}')$. Now, by definition, $\widetilde{\eta}(\overline{x}) = \overline{\sigma(x)} = \overline{x}$, since $\sigma|_K = \operatorname{id}|_K$. Therefore, $\widetilde{\eta}|_{\overline{\mathcal{K}}} = \operatorname{id}|_{\overline{\mathcal{K}}}$, hence $\widetilde{\eta}$ is a $\overline{\mathcal{K}}$-isomorphism.

   Claim: $\overline{\sigma}(u + \sigma^{-1}(\mathcal{M}')) = \overline{\sigma(u)}$ **for every** $u \in \sigma^{-1}(\mathcal{O}')$**.**

   Let $u \in \sigma^{-1}(\mathcal{O}')$ and $t \in \sigma^{-1}(\mathcal{M}')$, i.e., $\sigma(u) \in \mathcal{O}'$ and $\sigma(t) \in \mathcal{M}'$. Consider $\overline{\sigma}(u + t) = \overline{\sigma}(u) + \overline{\sigma}(t) = \overline{\sigma(u)} + \overline{\sigma(t)} = \overline{\sigma(u)}$, since $\sigma(t) \in \mathcal{M}'$, which proves the claim.

4. Let Δ denote the value group corresponding to the valuation ring $\sigma^{-1}(\mathcal{O}')$. By part 1, its valuation is given by $v' \circ \sigma$. Therefore, we have $(v' \circ \sigma)(N^\times) = \Delta$. But $\sigma(N^\times) = N^\times$, since $\sigma \in \operatorname{Aut}(N/K)$, hence $(v' \circ \sigma)(N^\times) = v'(N^\times) = \Gamma'$, i.e., $\Delta = \Gamma'$, therefore $e(\sigma^{-1}(\mathcal{O}')/\mathcal{O}) = [\Delta : \Gamma] = e(\mathcal{O}'/\mathcal{O})$. Similarly, the residue class field of $\sigma^{-1}(\mathcal{O}')$ is $\overline{N}$ by part 3, and so $f(\sigma^{-1}(\mathcal{O}')/\mathcal{O}) = [\overline{N} : \overline{\mathcal{K}}] = f(\mathcal{O}'/\mathcal{O})$.

Chapter 2

Class Field Theory

2.1 Local Fields

Definition 2.1.1. All fields which are complete with respect to a discrete valuation and have a finite residue class field are called ***local fields***.

For such a local field, the normalized exponential valuation is denoted by $v_{\mathfrak{p}}$, and $|\cdot|_{\mathfrak{p}}$ denotes the absolute value normalized by $|x|_{\mathfrak{p}} = q^{-v_{\mathfrak{p}}(x)}$, where q is the cardinality of the residue class field.

Definition 2.1.2. A topological space X is said to be ***locally compact*** if for every point $x \in X$, there exists a compact set T and an open set U such that $x \in U \subset T$.

Theorem 2.1.1. *A local field K is locally compact and its valuation ring $\mathcal{O}$ is compact.*

Proof. We have seen before that there is a topological and algebraic isomorphism $\widehat{\mathcal{O}} = \mathcal{O} \xrightarrow{\sim} \varprojlim \mathcal{O}/\mathfrak{p}^n$ and $\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong \mathcal{O}/\mathfrak{p}$. Consider the map $\mathcal{O}/\mathfrak{p}^n \to \mathcal{O}/\mathfrak{p}$ sending $x + \mathfrak{p}^n \mapsto x + \mathfrak{p}$, this is well defined as $\mathfrak{p}^n \subset \mathfrak{p}$ and its kernel is $\mathfrak{p}/\mathfrak{p}^n$, which is finite since $\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong \mathcal{O}/\mathfrak{p}$ is finite. The map is surjective as well since given any $x + \mathfrak{p} \in \mathcal{O}/\mathfrak{p}$, we have a preimage $x + \mathfrak{p}^n \in \mathcal{O}/\mathfrak{p}^n$. Therefore, $\mathcal{O}/\mathfrak{p}^n$ is finite, hence compact. Therefore, the product $\prod_{n=1}^{\infty} \mathcal{O}/\mathfrak{p}^n$ is compact by Tychonoff and hence the closed subset $\varprojlim \mathcal{O}/\mathfrak{p}^n$ is also compact. Therefore, $\widehat{\mathcal{O}} = \mathcal{O}$ is compact. To show that K is locally compact, we consider an arbitrary point $a \in K$. Then, by Lemma 1.4.10, we know $\overline{B}(a, 1)$ is an open set containing a and it is in fact homeomorphic to $\mathcal{O}$ as $\overline{B}(a, 1) = a + \mathcal{O}$, making it compact as well. Therefore, a has a compact neighborhood around it, whence it follows that K is locally compact. ☕

Corollary 2.1.1.1. *The valuation ring of a local field is compact.*

Proof. The valuation ring $\mathcal{O}$ is a closed set of a complete metric space K and hence it is complete as well. ☕

Theorem 2.1.2 (Teichmüller Lift)**.** *Let K be a local field. There is a uniquely determined map $\omega : \mathcal{O}/\mathfrak{p} \to \mathcal{O}$ such that $\omega(a) \equiv a \pmod{\mathfrak{p}}$ and $\omega(ab) = \omega(a)\omega(b)$.*

Proof. **Claim: If $a, b \in \mathcal{O}$ and $a \equiv b \pmod{\mathfrak{p}^m}$, then $a^p \equiv b^p \pmod{\mathfrak{p}^{m+1}}$, where $p = \operatorname{char}(\mathcal{O}/\mathfrak{p})$.**

For $p = 2$, we have $a - b \in \mathfrak{p}^m = \pi^m\mathcal{O}$, i.e., $a = b + x\pi^m, x \in \mathcal{O}$, and $a^2 = b^2 + x^2\pi^{2m} + 2xb\pi^m \equiv b^2 + x^2\pi^{2m} \equiv b^2 \pmod{\pi^{m+1}\mathcal{O}} = \mathfrak{p}^{m+1}$, since $\operatorname{char}(\mathcal{O}/\mathfrak{p}) = 2$.

For odd p, we have $a = b + x\pi^m, x \in \mathcal{O}$, and so $a^p = (b + x\pi^m)^p = b^p + p(\cdots) + x^p\pi^{mp} \equiv b^p + x^p\pi^{mp} \equiv b^p \pmod{\pi^{m+1}\mathcal{O}}$, since $\operatorname{char}(\mathcal{O}/\mathfrak{p}) = p$.

We construct ω as follows: for $a \in \mathcal{O}/\mathfrak{p}$, choose any lift $\widetilde{a} \in \mathcal{O}$. Define the sequence $a_0 = a,\ a_{n+1} = (a_n)^{1/p}$ in $\mathcal{O}/\mathfrak{p}$. This is well-defined because the Frobenius $x \mapsto x^p$ is an automorphism of $\mathcal{O}/\mathfrak{p}$, which is a finite, hence perfect, field.

Consider the lifted sequence $(b_n)_n = (\widetilde{a}_n^{p^n})_n \subset \mathcal{O}$. We have by construction $\widetilde{a}_{n+1} \equiv \widetilde{a}_n^{1/p} \implies \widetilde{a}_{n+1}^p \equiv \widetilde{a}_n \pmod{\mathfrak{p}}$, i.e., $(\widetilde{a}_{n+1}^p)^p \equiv (\widetilde{a}_n)^p \pmod{\mathfrak{p}^2}$, by applying the claim for $m = 1$. Thus, $\widetilde{a}_{n+1}^{p^2} \equiv \widetilde{a}_n^p \pmod{\mathfrak{p}^2}$. Similarly, applying the claim for $m = 2$, we get $\widetilde{a}_{n+1}^{p^3} \equiv \widetilde{a}_n^{p^2} \pmod{\mathfrak{p}^3}$. Proceeding this way, it follows that $\widetilde{a}_{n+1}^{p^{n+1}} \equiv \widetilde{a}_n^{p^n} \pmod{\mathfrak{p}^{n+1}}$. Thus, $b_{n+1} - b_n = \widetilde{a}_{n+1}^{p^{n+1}} - \widetilde{a}_n^{p^n} \in \mathfrak{p}^{n+1} = \pi^{n+1}\mathcal{O} \implies |b_{n+1} - b_n| < \dfrac{1}{q^n}$, and as $n \to \infty$, $1/q^n \to 0$. Therefore, this sequence is Cauchy and hence it converges in $\mathcal{O}$, because $\mathcal{O}$ is complete. Let its limit be $\omega(a) \in \mathcal{O}$, i.e, $\omega(a) := \lim_{n\to\infty} \widetilde{a}_n^{p^n}$. Then $\omega(a)$ is uniquely determined by uniqueness of limits. Moreover, if $\widetilde{c}_n$ is another lift of a_n, then we have $\widetilde{c}_n \equiv \widetilde{a}_n \pmod{\mathfrak{p}} \implies \widetilde{c}_n^{p^n} \equiv \widetilde{a}_n^{p^n} \pmod{\mathfrak{p}^n}$ by the claim, and so $|\widetilde{c}_n^{p^n} - \widetilde{a}_n^{p^n}| < \frac{1}{p^n} \to 0$ as $n \to \infty$, i.e., $\lim \widetilde{c}_n^{p^n} = \lim \widetilde{a}_n^{p^n}$. Therefore, we have a well-defined map $\omega : \mathcal{O}/\mathfrak{p} \to \mathcal{O}$ as $\omega(a) := \lim_{n\to\infty} \widetilde{a}_n^{p^n}$, where $\widetilde{a}_0 \equiv a$, $\widetilde{a}_{n+1} \equiv (\widetilde{a}_n)^{1/p} \pmod{\mathfrak{p}}$, so $\widetilde{a}_n \equiv (\widetilde{a}_0)^{p^{-n}} \pmod{\mathfrak{p}}$.

It remains to check the two properties of this map. To check reduction modulo $\mathfrak{p}$, we consider again the sequence b_n and reduce it modulo $\mathfrak{p}$. Then, $b_0 \equiv a_0^{p^0} = a \pmod{\mathfrak{p}}$, $b_1 \equiv a_1^{p^1} = (a^{\frac{1}{p}})^p = a \pmod{\mathfrak{p}}, \ldots, b_n \equiv a_n^{p^n} = a \pmod{\mathfrak{p}}$ for all $n \geq 0$. This means that $v(b_n - a) > 0$, and since v is continuous, we may take limit on both sides as $n \to \infty$ to get $\lim v(b_n - a) = v(\omega(a) - a) > 0$, i.e., $\omega(a) - a \in \mathfrak{p}$ and thus $\omega(a) \equiv a \pmod{\mathfrak{p}}$. To show $\omega(ab) = \omega(a)\omega(b)$, we need to show that $\lim \widetilde{x}_n^{p^n} = \lim \widetilde{a}_n^{p^n} \lim \widetilde{b}_n^{p^n} = \lim(\widetilde{a}_n\widetilde{b}_n)^{p^n}$, where $\widetilde{x_n}$ is a lift of the sequence corresponding to $ab \in \mathcal{O}/\mathfrak{p}$, i.e., $x_0 = ab,\ x_{n+1} = (x_n)^{1/p} = (x_0)^{1/p^n} = (ab)^{1/p^n}$. Now, to see that $\widetilde{x}_n \equiv \widetilde{a}_n\widetilde{b}_n \pmod{\mathfrak{p}}$, consider $\widetilde{x}_n + \mathfrak{p} = (ab)^{1/p^n} + \mathfrak{p}$. With all maps below being Frobenius, we have

$$\mathcal{O}/\mathfrak{p} \leftarrow \cdots \leftarrow \mathcal{O}/\mathfrak{p} \leftarrow \mathcal{O}/\mathfrak{p} \leftarrow \mathcal{O}/\mathfrak{p}$$
$$y^{1/p^n} \leftarrow \cdots \leftarrow y^{1/p^2} \leftarrow y^{1/p} \leftarrow y$$

In particular, the map $\mathcal{O}/\mathfrak{p} \to \mathcal{O}/\mathfrak{p}$ sending $y \mapsto y^{1/p^n}$ is a composition of homomorphisms and hence is itself a homomorphism, therefore, $(y^{1/p^n})(z^{1/p^n}) = (yz)^{1/p^n}$. Hence, we have $\widetilde{x}_n + \mathfrak{p} = (ab)^{1/p^n} + \mathfrak{p} = a^{1/p^n} b^{1/p^n} + \mathfrak{p} = (a^{1/p^n} + \mathfrak{p})(b^{1/p^n} + \mathfrak{p}) = (\widetilde{a_n} + \mathfrak{p})(\widetilde{b_n} + \mathfrak{p})$, i.e., $\widetilde{x}_n \equiv \widetilde{a}_n \widetilde{b}_n \pmod{\mathfrak{p}}$. Applying now the claim as before yields $\widetilde{x}_n^{p^n} \equiv (\widetilde{a}_n \widetilde{b}_n)^{p^n} \pmod{\mathfrak{p}^n}$, i.e., $|\widetilde{x}_n^{p^n} - (\widetilde{a}_n \widetilde{b}_n)^{p^n}| < 1/q^{n-1} \to 0$ as $n \to \infty$. Hence, $\lim \widetilde{x}_n^{p^n} = \lim (\widetilde{a}_n \widetilde{b}_n)^{p^n} = \lim \widetilde{a}_n^{p^n} \lim \widetilde{b}_n^{p^n}$ and thus $\omega(ab) = \omega(a)\omega(b)$. From the discussion so far, it also follows that $\omega(1) = 1$, because otherwise any preimage $x \neq 1 \in \mathcal{O}$ of $1 \in \mathcal{O}/\mathfrak{p}$ under the Frobenius must necessarily be a generator of $(\mathcal{O}/\mathfrak{p})^\times$ and therefore must satisfy $x^{q-1} = 1$. But since it is a preimage of 1, it must also satisfy $x^p = 1$, which implies $p \mid q-1$, a contradiction since $q = p^f$. Hence, $x = 1$. Further, note that for any $a \in (\mathcal{O}/\mathfrak{p})^\times$, we have $\omega(a)^{q-1} = \omega(a^{q-1}) = \omega(1) = 1$, i.e., $\omega(a)$ is a $(q-1)$-th root of unity lifting a, which gives us a homomorphism $\omega|_{(\mathcal{O}/\mathfrak{p})^\times} : (\mathcal{O}/\mathfrak{p})^\times \to \mu_{q-1}$, which we call the ***Teichmüller lift***.

☕

Lemma 2.1.1. *The Teichmüller lift* $\omega : (\mathcal{O}/\mathfrak{p})^\times \to \mu_{q-1} \subset \mathcal{O}^\times$ *is an isomorphism.*

Proof. It is easy to see that $\mu_{q-1} \subset \mathcal{O}^\times$ because for any $\zeta \in \mu_{q-1}$, $\zeta^{q-1} = 1 \implies v(\zeta^{q-1}) = (q-1)v(\zeta) = 0 \implies v(\zeta) = 0 \implies \zeta \in \mathcal{O}^\times$. The Teichmüller lift homomorphism is injective because $\omega(a) = \omega(b) \implies a + \mathfrak{p} = b + \mathfrak{p}$, as seen in the last theorem. Moreover, the map is surjective, since given any $\zeta \in \mu_{q-1} \subset \mathcal{O}^\times$, we reduce modulo $\mathfrak{p}$ to get $\zeta + \mathfrak{p}$ whose image is ζ. It only needs to be shown that $\zeta + \mathfrak{p}$ is a unit in $\mathcal{O}/\mathfrak{p}$, but this follows from the fact that reduction modulo $\mathfrak{p}$ maps $\mathcal{O}^\times$ onto $(\mathcal{O}/\mathfrak{p})^\times$, as seen in Proposition 1.1.7. Therefore, $\omega : (\mathcal{O}/\mathfrak{p})^\times \xrightarrow{\sim} \mu_{q-1}$.

☕

Theorem 2.1.3. *The local fields are precisely the finite extensions of the fields* $\mathbb{Q}_p$ *and* $\mathbb{F}_p((t))$.

Proof. It follows by definition that $\mathbb{Q}_p$ and $\mathbb{F}_p((t))$ are local fields: both are complete with respect to their respective discrete valuations and the residue field for both is $\mathbb{F}_p$, as seen earlier. A finite extension of K of F (where $F = \mathbb{Q}_p$) or $F = \mathbb{F}_p((t))$ must be complete: this follows from a result in functional analysis which states that every finite dimensional normed vector space is complete. Moreover, the unique extended valuation given by $|\alpha|_K := (|N_{K/F}(\alpha)|_F)^{1/n}$, which is also discrete since $|\cdot|_F$ is discrete.

Claim: The extension of residue class fields $\overline{\mathcal{K}}/\mathbb{F}_p$ is finite. To see this, it suffices to show that every linearly independent set in $\overline{\mathcal{K}} = \mathcal{O}/\mathfrak{p}$ has finite cardinality. Let $\overline{x_1}, \overline{x_2}, \dots \overline{x_n} \in \mathcal{O}/\mathfrak{p}$ be linearly independent over $\mathbb{F}_p$. Consider their lifts $x_1, x_2, \dots, x_n \in \mathcal{O} \subset K$. We wish to show these are linearly independent over F: suppose not, then there is a nontrivial relation $\sum_{i=1}^n a_i x_i = 0$, not all $a_i = 0$. Take the coefficient a_j such that $v(a_j) = \min_i\{v(a_i)\}$ and divide the equation by a_j to obtain a nontrivial relation $\sum_{i=1}^n (a_i a_j^{-1}) x_i = 0$, i.e., $(a_1 a_j^{-1}) x_1 + \dots 1 x_j + \dots (a_n a_j^{-1}) x_n = 0$. Reducing modulo $\mathfrak{p}$, we get $\sum_{i=1}^n (\overline{a_i a_j}^{-1}) \overline{x_i} = 0$, and note that the j^{th} term in this equation is $\overline{1}\overline{x_j}$, which is nonzero in $\overline{\mathcal{K}} = \mathcal{O}/\mathfrak{p}$, since $1 \notin \mathfrak{p}$, i.e., we have nontrivial linear relation among $\overline{x_1}, \overline{x_2}, \dots \overline{x_n} \in \mathcal{O}/\mathfrak{p}$. This gives the required contradiction, and so $x_1, x_2, \dots, x_n \in \mathcal{O} \subset K$ are linearly independent over F. Since the extension K/F is finite, we have $n \leq [K:F] < \infty$, which proves the claim. Therefore, we have shown that K is a complete discretely valued field with a finite residue class field, i.e., K is a local field.

Conversely, let K be a local field of positive characteristic with valuation v and $p = \mathrm{char}(\mathcal{O}/\mathfrak{p})$. Let π be a uniformizer. Denote the ring of formal power series with coefficients in $\mathcal{O}/\mathfrak{p} = \overline{\mathcal{K}}$ by $\overline{\mathcal{K}}[[t]]$ and consider the map $\phi : \overline{\mathcal{K}}[[t]] \to \mathcal{O}$ sending $\sum_{n\geq 0} a_n T^n \mapsto \sum_{n\geq 0} \omega(a_n)\pi^n$, where ω is the Teichmüller lift. Consider $\phi(\sum_{n\geq 0} a_n T^n + \sum_{n\geq 0} b_n T^n) = \phi(\sum_{n\geq 0}(a_n + b_n)T^n) = \sum_{n\geq 0} \omega(a_n + b_n)\pi^n = \sum_{n\geq 0} \omega(a_n)\pi^n + \sum_{n\geq 0} \omega(b_n)\pi^n = \phi(\sum_{n\geq 0} a_n T^n) + \phi(\sum_{n\geq 0} b_n T^n)$, i.e., ϕ is a homomorphism. To prove surjectivity of ϕ, we recall that every $x \neq 0$ in K admits a unique representation as a convergent series $x = \pi^m(a_0 + a_1\pi + a_2\pi^2 + \cdots)$, where $a_i \in \overline{\mathcal{K}}$, $a_0 \neq 0$, and $m \in \mathbb{Z}$. For injectivity, consider the kernel $\ker\phi = \{\sum_{n\geq 0} a_n T^n \mid \sum_{n\geq 0} \omega(a_n)\pi^n = 0\} = \{\sum_{n\geq 0} a_n T^n \mid \omega(a_n) = 0,\ \forall n \geq 0\} = \{\sum_{n\geq 0} a_n T^n \mid a_n = 0,\ \forall n \geq 0\} = 0$, since $\omega(a_n) = a_n \pmod{\mathfrak{p}}$. Therefore, $\overline{\mathcal{K}}[[t]] \cong \mathcal{O}$, and therefore, their fields of fractions must be isomorphic, yielding $\overline{\mathcal{K}}((t)) \cong K$. Since $p = \mathrm{char}(\overline{\mathcal{K}})$, we get that K is a finite extension of $\mathbb{F}_p((t))$. This also shows that if K has positive characteristic, then $p = \mathrm{char}(\overline{\mathcal{K}}) = \mathrm{char}(K)$. Suppose now that $\mathrm{char}(K) = 0$, then we have $v \mid_{\mathbb{Q}} = v_p$, by 1.2.1.1. Since K has zero characteristic, it contains $\mathbb{Q}$, i.e., $\mathbb{Q} \subset K$. Taking closure on both sides with respect to v, we obtain $\overline{\mathbb{Q}} = \mathbb{Q}_p \subset \overline{K} = K$, since K is complete and $v \mid_{\mathbb{Q}} = v_p$. From the theory of topological vector spaces, we recall that a locally compact topological vector space over a nondiscrete locally compact field has finite dimension, yielding $[K : \mathbb{Q}_p] < \infty$. We will show the finiteness of this extension in another way via the fundamental equality later.

☕

Definition 2.1.3. A local field K is of ***equal characteristic*** if $\mathrm{char}(K) = \mathrm{char}\ (\mathcal{O}/\mathfrak{p})$. Otherwise, it is of ***mixed characteristic***.

Theorem 2.1.4. *The multiplicative group of a local field K admits the decomposition $K^\times = (\pi) \times \mu_{q-1} \times U^{(1)}$, where q is the number of elements in the residue* *field $\mathcal{O}/\mathfrak{p}$, and $U^{(1)} = 1 + \mathfrak{p}$ is the group of principal units.*

Proof. We first show that $K^\times = (\pi) \times \mathcal{O}^\times$. For this, recall that any $x \in K^\times$ can be uniquely written as $\pi^{v(x)}u$ for some unit $u \in \mathcal{O}^\times$, i.e., $K^\times = (\pi)\mathcal{O}^\times$. Further, the intersection $(\pi) \cap \mathcal{O}^\times$ is trivial because elements in (π) have valuation 1 and elements in $\mathcal{O}^\times$ have valuation 0. Moreover, since all the groups are abelian we have $(\pi)\mathcal{O}^\times = \mathcal{O}^\times(\pi)$, and hence $K^\times = (\pi) \times \mathcal{O}^\times$. It remains to show that $\mathcal{O}^\times = \mu_{q-1} \times U^{(1)}$. Consider the sequence $1 \to U^{(1)} \to \mathcal{O}^\times \xrightarrow{\varphi} (\mathcal{O}/\mathfrak{p})^\times \to 1$, which is exact by Proposition 1.1.7. We have $\omega : (\mathcal{O}/\mathfrak{p})^\times \xrightarrow{\sim} \mu_{q-1} \subset \mathcal{O}^\times$, and composing this with the map $\varphi : \mathcal{O}^\times \to (\mathcal{O}/\mathfrak{p})^\times$ given by $\varphi(u) = u + \mathfrak{p}$, we get a map $(\varphi \circ \omega) : (\mathcal{O}/\mathfrak{p})^\times \to (\mathcal{O}/\mathfrak{p})^\times$. Consider $(\varphi \circ \omega)(a + \mathfrak{p}) = \varphi(\omega(a)) = \omega(a) + \mathfrak{p} = a + \mathfrak{p}$, i.e., $\varphi \circ \omega \equiv \mathrm{id}_{(\mathcal{O}/\mathfrak{p})^\times}$. Therefore, the exact sequence splits and hence we obtain $\mathcal{O}^\times \cong U^{(1)} \times (\mathcal{O}/\mathfrak{p})^\times \cong \mu_{q-1} \times U^{(1)}$, where the last isomorphism results from the Teichmüller lift. ☕

Remark 2.1. Alternatively, to see that $1 \to U^{(1)} \to \mathcal{O}^\times \xrightarrow{\varphi} (\mathcal{O}/\mathfrak{p})^\times \to 1$ splits, one may observe that $U^{(1)} = \varprojlim_n U^{(1)}/U^{(n)}$ is a pro-p group, and the order of every $U^{(1)}/U^{(n)}$ is coprime to $|(\mathcal{O}/\mathfrak{p})^\times| = q - 1$, thus by the Schur-Zassenhaus Theorem on finite groups the exact sequence $1 \to \varprojlim_n U^{(1)}/U^{(n)} \to \mathcal{O}^\times \xrightarrow{\varphi} (\mathcal{O}/\mathfrak{p})^\times \to 1$ splits.

Theorem (Schur-Zassenhaus)**.** *If G is a finite group and $N \trianglelefteq G$ is a normal subgroup such that $\gcd\big(|N|, |G/N|\big) = 1$, then G is a semidirect product (i.e., a split extension) of N and G/N. In particular, the exact sequence $1 \to N \to G \to G/N \to 1$ splits.*

We give another proof for the Teichmüller lift, using the basic version of Hensel's lemma, which we state now.

Theorem 2.1.5. *Let $(R, \mathfrak{p})$ be a complete DVR (discrete valuation ring) and $F(x) \in R[x]$ such that there exists $\alpha_1 \in \mathcal{O}$ with $F(\alpha_1) = 0 \pmod{\mathfrak{p}}$ and $F'(\alpha_1) \neq 0 \pmod{\mathfrak{p}}$. Then there exists a unique $\alpha \in R$ such that $\alpha \equiv \alpha_1 \pmod{\mathfrak{p}}$ and $F(\alpha) = 0$.*

Theorem 2.1.6 (Teichmüller lift, second proof)**.** *Let K be a local field. There is a uniquely determined map $\omega : (\mathcal{O}/\mathfrak{p})^\times \to \mu_{q-1}$ such that $\omega(a) \equiv a \pmod{\mathfrak{p}}$ and $\omega(ab) = \omega(a)\omega(b)$.*

Proof. Consider the polynomial $F(x) = x^q - x$, whence $\overline{F}(x) = \overline{x}^q - \overline{x} \in (\mathcal{O}/\mathfrak{p})[x] = \mathbb{F}_q[x]$, where $q = p^f$. Moreover, $\overline{F'}(x) = q\overline{x}^{q-1} - 1$, which is a separable polynomial, i.e., all its roots are simple. Moreover, since $(\mathcal{O}/\mathfrak{p})^\times = \mathbb{F}_q$, every element of $(\mathcal{O}/\mathfrak{p})^\times$

satisfies $\overline{\alpha}^{q-1} = \overline{\alpha}$ and thus is a root of $\overline{F}(x)$. Let $\overline{\alpha_1}$ be any root of $\overline{F}(x)$. Then, by the version of Hensel's Lemma stated above, there is a unique lift $\alpha \in R$ with $F(\alpha) = 0$, i.e., $\alpha \in \mu_{q-1}$. Define $\omega(\alpha_1) := \alpha$, which is unique and reduces to α_1 modulo $\mathfrak{p}$ as seen above. We next show that $\omega(\overline{st}) = \omega(\overline{s})\omega(\overline{t})$, where $\overline{s}, \overline{t}$ are two arbitrary roots of $\overline{F}(x)$. Note that this implies $\overline{st}$ is also a root since we have $\overline{s}^q = \overline{s}$ and $\overline{t}^q = \overline{t}$, which together imply $\overline{st}^q = \overline{st}$, yielding $\overline{st}^q - \overline{st} = 0$. Now, let s, t, r be the unique lifts of $\overline{s}, \overline{t}, \overline{st}$ respectively, i.e., $\omega(\overline{s}) = s$, $\omega(\overline{t}) = t$, $\omega(\overline{st}) = r$. Since reduction modulo $\mathfrak{p}$ is a homomorphism, we also have $\overline{st} = \overline{s} \cdot \overline{t}$, i.e., st is also a lift of $\overline{st}$. Therefore, by uniqueness, we have $r = st$, i.e., $\omega(\overline{st}) = \omega(\overline{s})\omega(\overline{t})$. ☕

Definition 2.1.4. The local fields of mixed characteristic, i.e., the finite extensions $K \supseteq \mathbb{Q}_p$ of the fields of p-adic numbers $\mathbb{Q}_p$, are called ***$\mathfrak{p}$-adic number fields***.

Lemma 2.1.2. *For a $\mathfrak{p}$-adic number field K, the extended p-adic valuation v_p has image $v_p(K^\times) = \frac{1}{e}\mathbb{Z}$, where e is a divisor of $n = [K : \mathbb{Q}_p]$*

Proof. We already know that the image is contained in $\frac{1}{n}\mathbb{Z}$, since $v_p(\alpha) = \frac{1}{n}v_p(N_{L/K}(\alpha))$. Moreover, the image contains all of $\mathbb{Z}$, since $v_p(\mathbb{Q}_p^\times) = \mathbb{Z}$. Now, $v_p(K^\times)$ is a subgroup of $(\mathbb{Q}, +)$ and hence its elements are rational integers. Suppose $\frac{d}{e} \in v_p(K^\times)$ is such that e is the largest denominator possible for a rational integer to be in $v_p(K^\times)$, and without loss of generality, we may assume that $\gcd(d, e) = 1$. By Bézout, there exist integers r, s such that $rd + se = 1$, whence we obtain $r\left(\frac{d}{e}\right) = \frac{1}{e} - s \in v_p(K^\times)$, since $\frac{d}{e} \in v_p(K^\times)$. Note that since the image contains all of $\mathbb{Z}, s \in v_p(K^\times)$, which in turn implies $\frac{1}{e} \in v_p(K^\times)$. By definition, e was the largest denominator possible for a rational integer to be in $v_p(K^\times)$, and so $\frac{1}{e}$ is a minimal value in $v_p(K^\times)$, i.e., $v_p(K^\times) = \frac{1}{e}\mathbb{Z}$. ☕

Remark 2.2. It turns out that the integer e above is the ramification index of this extension $K \supset \mathbb{Q}_p$ (defined in 1.5.2) as we have $v_p(\mathbb{Q}_p^\times) = \mathbb{Z}$ and $v_p(K^\times) = \frac{1}{e}\mathbb{Z}$, giving the ramification index equal to $[v_p(K^\times) : v_p(\mathbb{Q}_p^\times)] = [\frac{1}{e}\mathbb{Z} : \mathbb{Z}] = e$.

Definition 2.1.5. Given a $\mathfrak{p}$-adic number field K, we have $v_p(K^\times) = \frac{1}{e}\mathbb{Z}$. The valuation $v_\mathfrak{p}(\alpha) := ev_p(\alpha)$ is the ***normalized extended valuation*** on K.

Theorem 2.1.7. *For a $\mathfrak{p}$-adic number field K, there is a uniquely determined continuous homomorphism* $\log : K^\times \to K$ *such that* $\log p = 0$*, which on principal* *units* $(1+x)\in U^{(1)}$ *is given by the series*

$$\log(1+x)=\sum_{n=1}^{\infty}\frac{(-1)^{n+1}x^n}{n}=x-\frac{x^2}{2}+\frac{x^3}{3}-\frac{x^4}{4}+\dots$$

Proof. We first define log on $U^{(1)}$ and then extend it to the whole of $K^\times$. Recall that in a nonarchimedean absolute value, convergence of a series $\sum a_n$ is equivalent to $\lim_{n\to\infty}|a_n|=0 \iff \lim_{n\to\infty}v(a_n)=\infty$. Let $1+x\in U^{(1)}$, i.e., $x\in\mathfrak{p}$. Let $n=p^tm$, then $v_p(n)=t\le t+\log_p(m)=\log_p(p^tm)$, i.e., $v_p(n)\le\log_p(p^tm)=\log_p(n)=\ln n/\ln p$. Moreover, since $x\in\mathfrak{p}$, we have $v_p(x)>0 \implies p^{v_p(x)}:=c>1 \implies v_p(x)>\ln c/\ln p$. Consider now $v_p(\frac{x^n}{n})=nv_p(x)-v_p(n)\ge\ln c/\ln p-\ln n/\ln p=\ln(c^nn)/\ln p$. Now, as $n\to\infty$, we get $\ln(c^nn)/\ln p\to\infty$, i.e, $v_p(\frac{x^n}{n})\to\infty$. Therefore, the series $\log(1+x)=\sum_{n=1}^{\infty}\frac{(-1)^{n+1}x^n}{n}$ converges for any $1+x\in U^{(1)}$. To verify the homomorphism property, we define two formal functions $H(x,y):=\log(1+x)+\log(1+y)$ and $G(x,y)=\log((1+x)(1+y))$. It is clear that $\frac{d}{dx}(\log(1+x))=\frac{d}{dx}\left(\sum_{n=1}^{\infty}\frac{(-1)^{n+1}x^n}{n}\right)=\sum_{n=1}^{\infty}(-1)^{n+1}x^{n-1}=\frac{1}{1+x}$. Therefore, we have

$$\frac{\partial G}{\partial x}=\frac{1}{(1+x)(1+y)}\cdot\frac{\partial}{\partial x}(1+x+y+xy)=\frac{1+y}{(1+x)(1+y)}=\frac{1}{1+x}=\frac{\partial H}{\partial x}$$

Therefore, $\frac{\partial}{\partial x}(G-H)=0$. Since G,H are symmetric functions in x,y, it follows mutatis mutandis that $\frac{\partial}{\partial y}(G-H)=0$, which implies that $G\equiv H$, as desired. Hence, we have defined the log homomorphism on $U^{(1)}$; we now extend this to $K^\times$. We have seen earlier that $K^\times$ admits a decomposition as an internal direct product as $K^\times=(\pi)\times\mu_{q-1}\times U^{(1)}$, therefore, any $\alpha\in K^\times$ may be expressed as $\alpha=\pi_{\mathfrak{p}}^{v}(\alpha)\omega(\alpha)\langle\alpha\rangle$, where $v_{\mathfrak{p}}=ev_p$ is the normalized valuation on K, $\langle\alpha\rangle\in U^{(1)}$ and ω is the Teichmüller lift. In particular, $p=\pi^e\omega(p)\langle p\rangle$. We define $\log\pi:=(-1/e)\log\langle p\rangle$ to obtain the homomorphism $\log:K^\times\to K$ mapping $\alpha\mapsto v_{\mathfrak{p}}(\alpha)\log\pi+\log\langle\alpha\rangle$. This map is continuous as $v_{\mathfrak{p}}$ and $\log|_{U^{(1)}}$ are both continuous. It also follows that $\log p=v_{\mathfrak{p}}(p)\log\pi+\log\langle p\rangle=e(-1/e)\log\langle p\rangle+\log\langle p\rangle=0$. It remains to show uniqueness; suppose $\lambda:K^\times\to K$ is another continuation of $\log:U^{(1)}\to K$ with $\lambda(p)=0$. Then, for any $\zeta\in\mu_{q-1}$, one has $\lambda(\zeta)=\frac{1}{q-1}\lambda(\zeta^{q-1})=\frac{1}{q-1}\lambda(1)=0$. Now, $0=\lambda(p)=\lambda(\pi^e\omega(p)\langle p\rangle)=l\lambda(\pi)+\lambda(\omega(p))+\lambda(\langle p\rangle)=l\lambda(\pi)+\lambda(\langle p\rangle)=l\lambda(\pi)+\log(\langle p\rangle)$, since λ is a continuation of $\log:U^{(1)}\to K$. Therefore, it follows that $\lambda(\pi)=(-1/l)\log(\langle p\rangle)=\log\pi$. Therefore, $\lambda(\alpha)=\lambda(\pi_{\mathfrak{p}}^{v}(\alpha)\omega(\alpha)\langle\alpha\rangle)=v_{\mathfrak{p}}(\alpha)\lambda(\pi)+\lambda(\omega(\alpha))+\lambda(\langle\alpha\rangle)=v_{\mathfrak{p}}(\alpha)\log\pi+\log(\langle\alpha\rangle)=\log(\alpha)$, whence we obtain $\lambda\equiv\log$. Hence, log is a uniquely determined continuous homomorphism independent of the choice of π. ☕

Lemma 2.1.3. *Let $n = \sum_{i=0}^{r} a_i p^i$ be the p-adic expansion of $n \in \mathbb{N}$, i.e., $0 \le a_i < p$. Then, $v_p(n!) = \frac{1}{p-1} \sum_{i=0}^{r} a_i(p^i - 1)$.*

Proof. Consider the floor function $[\cdot]$. We have $[n/p] = \sum_{i=0}^{r} a_i p^{i-1} = [a_0/p + a_1 + \cdots + a_r p^{r-1}] = a_1 + \cdots + a_r p^{r-1}$. Similarly, we have $[n/p^2] = a_2 + \cdots + a_r p^{r-2}$ and so on until $[n/p^r] = a_r$. Observe that $[n/p]$ counts the number of positive integers from 1 to n which are divisble by p. Similarly, $[n/p^i]$ counts the number of positive integers from 1 to n which are divisble by p^i, for any $1 \le i \le r$. Hence, the sum $[n/p] + [n/p^2] + [n/p^3] + \cdots + [n/p^r]$ counts the the number of positive integers from 1 to n which are divisble by p, with multiplicity. On the other hand, $v_p(n!) = v_p(n) + v_p(n-1) + \cdots + v_p(2) + v_p(1)$ and $v_p(t)$ counts the highest power of p dividing t and any positive integer coprime to p contributes zero to the above sum. Therefore, $v_p(n!)$ also counts the the number of positive integers from 1 to n which are divisble by p, with multiplicity. Hence, we have $v_p(n!) = [n/p] + [n/p^2] + [n/p^3] + \cdots + [n/p^r] = a_1 + \cdots + a_r p^{r-1} + a_2 + \cdots + a_r p^{r-2} + \cdots + a_r = \sum_{i=1}^{r} a_i(p^i + p^{i-1} + \cdots + p + 1)$. Multiplying both sides by $p-1$, we obtain $(p-1)v_p(n!) = \sum_{i=1}^{r} a_i(p^{i-1} + p^{i-2} + \cdots + p + 1)(p-1) = \sum_{i=0}^{r} a_i(p^i - 1)$, as desired.

We now define the p-adic exponential function and use the lemma above to show its convergence in an appropriate domain. In the succeeding theorem, we show it is the inverse to the the p-adic logarithm, yielding isomorphisms $\mathfrak{p}^n \cong U^{(n)}$ for all large enough n.

Lemma 2.1.4. *For a $\mathfrak{p}$-adic number field K, there is a continuous homomorphism $\exp : \mathfrak{p}^n \to U^{(n)}$, given by $\exp(x) = \sum_{n=0}^{\infty} \dfrac{x^n}{n!} = 1 + x + \dfrac{x^2}{2!} + \dfrac{x^3}{3!} + \ldots$ for all $n > \frac{e}{p-1}$.*

Proof. Let $x \in \mathfrak{p}^n$ i.e., $v_{\mathfrak{p}}(x) \ge n > \frac{e}{p-1}$. For any $n > 0$, we write the base-p expansion of $n = a_0 + a_1 p + \cdots + a_r p^r$. From the previous lemma, we have $v_p(n!) = \frac{1}{p-1} \sum_{i=0}^{r} a_i(p^i - 1) = \frac{1}{p-1} \left(\sum_{i=0}^{r} a_i p^i - \sum_{i=0}^{r} a_i\right) = \frac{1}{p-1} \left(n - \sum_{i=0}^{r} a_i\right)$. Let $s_n = \sum_{i=0}^{r} a_i$, then $v_p(n!) = \dfrac{n - s_n}{p-1}$, whence we get $v_p\left(\dfrac{x^n}{n!}\right) = n v_p(x) - \left(\dfrac{n - s_n}{p-1}\right) = n\left(v_p(x) - \dfrac{1}{p-1}\right) + \dfrac{s_n}{p-1} > \dfrac{s_n}{p-1}$, i.e., $v_p\left(\dfrac{x^n}{n!}\right) \to \infty$ as $n \to \infty$, implying the convergence of $\exp(x) = \sum_{n=0}^{\infty} \dfrac{x^n}{n!}$. Note that exp satisfies the property that $\dfrac{d}{dx}\exp(x) = \exp(x)$ since $\dfrac{d}{dx} \sum_{n=0}^{\infty} \dfrac{x^n}{n!} = \sum_{n=1}^{\infty} \dfrac{x^{n-1}}{(n-1)!} = \exp(x)$. Further, since exp is a power series, it is also a continuous map.

Theorem 2.1.8. *Let $K/\mathbb{Q}_p$ be a $\mathfrak{p}$-adic number field with valuation ring $\mathcal{O}$ and maximal ideal $\mathfrak{p}$. Let $p\mathcal{O} = \mathfrak{p}^e$ where $p = \mathrm{char}(\mathcal{O}/\mathfrak{p})$ and e is the ramification index. For $n > \dfrac{e}{p-1}$, the power series $\exp : \mathfrak{p}^n \to U^{(n)}$ and $\log : U^{(n)} \to \mathfrak{p}^n$, given by*

$$\exp(x) = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots \text{ and } \log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \dots$$

yield two mutually inverse isomorphisms (and homeomorphisms).

Proof. As before, $v_{\mathfrak{p}}(\alpha) := ev_p(\alpha)$ denotes the normalized extended valuation on K, and we assume $n > \frac{e}{p-1}$ throughout the proof. We first show that for every natural $s > 1$, $\dfrac{v_p(s)}{s-1} \leq \dfrac{1}{p-1}$. For this, write $s = p^a s_0$ where $\gcd(s_0, p) = 1$. Note that if $a = 0$, then $v_p(s) = v_p(s_0) = 0$ and the inequality follows trivially, hence we may assume $a > 0$. Further, we have $p^a + \dots + p + 1 \geq 1 + 1 + \dots + 1 = a$. It then follows that

$$\frac{v_p(s)}{s-1} = \frac{a}{p^a s_0 - 1} \leq \frac{a}{p^a - 1} = \frac{1}{p-1}\left(\frac{a}{p^a + \dots + p + 1} \leq \frac{1}{p-1}.\right)$$

We now prove that log, as defined above, maps $U^{(n)} \to \mathfrak{p}^n$ for $n > \frac{e}{p-1}$. Let $1+z \in U^{(n)}$, i.e., $z \in \mathfrak{p}^n \implies v_{\mathfrak{p}}(z) \geq n$. Consider $v_p(z^s/s) - v_p(z) = (s-1)v_p(z) + v_p(s) > (s-1)\dfrac{1}{p-1} - \left(\dfrac{s-1}{p-1} = 0\right)$, i.e., $v_p(z^s/s) > v_p(z) \implies v_{\mathfrak{p}}(z^s/s) > v_{\mathfrak{p}}(z)$, whence it follows that $v_{\mathfrak{p}}(\log(1+z)) = v_{\mathfrak{p}}(z - \frac{z^2}{2} + \frac{z^3}{3} - \frac{z^4}{4} + \dots) = v_{\mathfrak{p}}(z) \geq n$. Hence, $\log(1+z) \in \mathfrak{p}^n$, as desired.

To see that exp maps $\mathfrak{p}^n \to U^{(n)}$, we take some $0 \neq x \in \mathfrak{p}^n$ i.e., $v_{\mathfrak{p}}(x) \geq n > \dfrac{e}{p-1}$. Now, for $i > 1$, we have

$$\begin{aligned}
v_p\left(\frac{x^i}{i!}\right) - v_p(x) &= (i-1)v_p(x) - v_p(i!) \\
&= (i-1)v_p(x) - \left(\frac{i-s_i}{p-1}\right) \\
&= \left((i-1)v_p(x) - \frac{i-1}{p-1}\right) + \left(\frac{s_i - 1}{p-1}\right) \\
&= (i-1)\left(v_p(x) - \frac{1}{p-1}\right) + \frac{s_i-1}{p-1} > \frac{s_i-1}{p-1} \geq 0
\end{aligned}$$

Therefore, $v_p\left(\sum_{i=1}^{\infty} \dfrac{x^i}{i!}\right) > v_p(x) = v_p(\exp(x) - 1) = v_p(x) \geq n$, i.e., $\exp(x) - 1 \in \mathfrak{p}^n \implies \exp(x) \in U^{(n)}$. Therefore, exp maps $\mathfrak{p}^n \to U^{(n)}$, as required.

Now, let $F := (\exp \circ \log) : U^{(n)} \to U^{(n)}$ and $G := (\log \circ \exp) : \mathfrak{p}^n \to \mathfrak{p}^n$. Consider $G'(x) = \dfrac{1}{\exp(x)} \exp(x) = 1$, implying $G(x) = a_0 + x$. Putting $x = 0$ gives $a_0 = G(0) = \log(\exp(0)) = \log(1+0) = 0$, therefore, $G(x) = x$. In particular, $G \equiv \mathrm{id}_{\mathfrak{p}^n}$ and similarly, $F \equiv \mathrm{id}_{U^{(n)}}$. Hence, $\exp : \mathfrak{p}^n \to U^{(n)}$ and $\log : U^{(n)}$ are mutually inverse isomorphisms. They are homeomorphisms as well since both functions are continuous.

☕

We next describe the $\mathbb{Z}_p$-module structure on $U^{(1)}$, for which we require the three facts stated below:

Lemma 2.1.5. *For an arbitrary local field K, with $q = p^f = |\mathcal{O}/\mathfrak{p}|$, we have*

1. *The order of $U^{(1)}/U^{(n+1)}$ is q^n, i.e., $U^{(1)}/U^{(n+1)}$ is a $\mathbb{Z}/q^n\mathbb{Z}$-module*
2. *$U^{(1)} = \varprojlim_n U^{(1)}/U^{(n+1)}$*
3. *$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/q^n\mathbb{Z}$*

Proof.
1. We have seen earlier that $U^{(i)}/U^{(i+1)} \cong \mathcal{O}/\mathfrak{p}$, which has order q. Hence, $|U^{(1)}/U^{(n+1)}| = \prod_{i=1}^n |U^{(i)}/U^{(i+1)}| = q^n$.
2. To see this, we restrict the canonical isomorphism (cf. Prop 1.1.8) $\varphi^\times : \mathcal{O}^\times \xrightarrow{\sim} \varprojlim_n \mathcal{O}^\times/U^{(n)}$ to $U^{(1)}$. Then, $\varphi^\times(U^{(1)}) = \{(yU^{(n)})_n : y \in U^{(1)}\} = \varprojlim_n U^{(1)}/U^{(n+1)}$.
3. We have seen this earlier but it also follows from Prop 1.1.8 in the special case where $K = \mathbb{Q}_p$, $\mathcal{O} = \mathbb{Z}_p$, $\mathfrak{p} = p\mathbb{Z}_p$ an‘d $\mathcal{O}/\mathfrak{p} = \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$.

☕

We now define the $\mathbb{Z}_p$-module structure on $U^{(1)}$ as $z \cdot y = y^z \in U^{(1)}$ in the following way. Let $y = (y_n)_n \in U^{(1)}$ and $z = (z_n)_n \in \mathbb{Z}_p$. Then, since $U^{(1)}/U^{(n+1)}$ is a $\mathbb{Z}/q^n\mathbb{Z}$-module, each $y_n \cdot y_n \cdots y_n = y_n^{z_n} \in U^{(1)}/U^{(n+1)}$. It remains to show that the infinite tuple $(y_n^{z_n})_n$ is an element in $\varprojlim_n U^{(1)}/U^{(n+1)}$. Let $y_n^{z_n} = t_n^{z_n} U^{(n+1)}$, where $t_n \in U^{(1)}$. We need to show that $y_n^{z_n}\left(y_{n-1}^{z_{n-1}}\right)^{-1} = \left(t_n^{z_n}U^{(n+1)}\right)\left(t_{n-1}^{z_{n-1}}U^{(n)}\right)^{-1} = t_n^{z_n}(t_{n-1}^{z_{n-1}})^{-1}U^{(n)} = U^{(n)}$, i.e., $t_n^{z_n}(t_{n-1}^{z_{n-1}})^{-1} \in U^{(n)}$. Now, since $(z_n)_n \in \mathbb{Z}_p$, we have $z_n = z_{n-1} + \alpha$, where $\alpha \in q^{n+1}\mathbb{Z}$. Hence, $t_n^{z_n}(t_{n-1}^{z_{n-1}})^{-1} = t_n^{z_{n-1}} t_n^{\alpha}(t_{n-1}^{z_{n-1}})^{-1} = t_n^{\alpha}(t_n t_{n-1}^{-1})^{z_{n-1}}$. Now, since $\alpha \in q^{n+1}\mathbb{Z}$, $t_n^\alpha \in U^{(n)}$ and since $(y_n^{z_n})_n = (t_n^{z_n} U^{(n+1)})_n \in \varprojlim_n U^{(1)}/U^{(n+1)}$, we have $t_n t_{n-1}^{-1} \in U^{(n)} \implies (t_n t_{n-1}^{-1})^{z_{n-1}} \in U^{(n)}$. Hence, the product $t_n^{z_n}(t_{n-1}^{z_{n-1}})^{-1} = t_n^{\alpha}(t_n t_{n-1}^{-1})^{z_{n-1}} \in U^{(n)}$, as desired. Therefore, we have a well defined map $\mathbb{Z}_p \times U^{(1)} \to U^{(1)}$ where $z \cdot y = y^z := (y_n^{z_n})_n \in \varprojlim_n U^{(1)}/U^{(n+1)} = U^{(1)}$.

To prove it is an action, we must further check that $1\cdot y = y$ and $z'\cdot(z\cdot y) = (z'z)\cdot y$ for all $y \in U^{(1)}$ and $z, z' \in \mathbb{Z}_p$. We have $1 \cdot y = y^1 = (y_n^1)_n = (y_n)_n = y$. Now, $z'\cdot(z\cdot y) = z'\cdot(y^z) = z'\cdot(y_n^{z_n})_n = ((y_n^{z_n})^{z'_n})_n = (y_n^{z_n z'_n})_n = y^{zz'} = y^{z'z} = (z'z)\cdot y$, as desired. Finally, we check that $(z+z')\cdot y = (z\cdot y)(z'\cdot y)$ and $z\cdot(yy') = (z\cdot y)(z\cdot y')$. For the former, we have $(z+z')\cdot y = y^{z+z'} = (y_n^{z_n+z'n})_n = (y_n^{z_n}y_n^{z'_n})_n = (y_n^{z_n})_n(y_n^{z'_n})_n = (z\cdot y)(z'\cdot y)$. The latter follows in a similar fashion by observing $(yy')^z = y^z y'^z$.

Lemma 2.1.6. *Let M be a module over the integral domain R such that M contains a submodule N that is free of rank d and M/N is a torsion R-module. Then M has rank n.*

Proof. Let $y_1, y_2, \ldots, y_{d+1}$ be elements of M and let $\overline{y_i}$ denote the coset $y_i + N \in M/N$. Since M/N is torsion, for each i there exists a nonzero $a_i \in R$ such that $a_i\overline{y_i} = 0 \in N$, i.e., $a_iy_i \in N$. Now, since N is free of rank n, there exists a nontrivial R-linear dependence relation $a_1y_1e_1 + \ldots, a_{n+1}y_{n+1}e_{n+1}$, where $\{e_i\}_{i=1}^n$ is an R-basis of N. This gives a nontrivial R-linear dependence relation among the y_i as the a_i are nonzero and hence not zero divisors, because R is an integral domain. Hence the rank of M is atmost d. However, the rank of M is at least d since $\{e_i\}_{i=1}^n$ is an R-linearly independent set in M. Therefore, the rank of M is precisely d.

☕

Lemma 2.1.7. *Let K/F be a finite separable extension of local fields. The ring $\mathcal{O}_K$ is a free $\mathcal{O}_F$-module of rank $d = [K : F]$.*

Proof. Let v be the normalized valuation of F with uniformizer π and $a_1, a_2, \ldots, a_d$ be an F-basis of K. If $v(a_i) = d_i \geq 0$, we keep it as it is, otherwise if $d_i < 0$, we replace a_i by $a'_i = \pi^{d_i}a_i$ to ensure $v(a'_i) \geq 0$. In this way, we may assume without loss of generality that each $a_i \in \mathcal{O}_K$. Let M be the $\mathcal{O}_F$-module spanned by $a_1, a_2, \ldots, a_n$, so that $M \subset \mathcal{O}_K$. By construction, M is a free $\mathcal{O}_F$-module of rank n. For each $x \in \mathcal{O}_K$, we can find an integer k such that $\pi^k x \in M$, by clearing denominators of the coefficients of x written in the basis.

Claim: There exists $d \in \mathcal{O}_F$ such that $d\mathcal{O}_K \subset M$.

Pick $x \in \mathcal{O}_K$ and write $x = \sum_{j=1}^n f_ja_j$, with $f_j \in F$. For any fixed a_i, we then have $a_ix = \sum_j a_ia_jf_j$, whence $\mathrm{Tr}_{K/F}(a_ix) = \sum_j \mathrm{Tr}_{K/F}(a_ia_j)f_j$, where Tr denotes the trace map. We write all these equalities (when i varies) as $AC_1 = C_2$, where A is the $n\times n$ matrix given by $(\mathrm{Tr}_{K/F}(a_ia_j))_{i,j}$, C_1 is the column containing $f_1, \ldots, f_n$, and C_2 is another column containing $\mathrm{Tr}_{K/F}(a_1x), \ldots, \mathrm{Tr}_{K/F}(a_nx)$. We know that $\mathrm{Tr}_{K/F}(a_ix) \in \mathcal{O}_F$. Let $d = \det(A)$, which is the discriminant $d(a_1, a_2, \ldots, a_d)$. To see that $d \neq 0$, observe that A is the matrix associated with the trace bilinear form $K \times K \to F$ given by $(x, y) \mapsto \mathrm{Tr}_{K/F}(xy)$. If $\det(A) = 0$, then there exists $y \neq 0$ such that $\mathrm{Tr}_{K/F}(xy) \equiv 0$, since a bilinear form is degenerate if and only if the determinant of the associated matrix is zero. But for $x = 1/y$, we have $\mathrm{Tr}_{K/F}(xy) = \mathrm{Tr}_{K/F}(1) = n \neq 0$, a contradiction. Hence, $d \neq 0$ and we may write $C_1 = A^{-1}C_2$, implying $df_i \in \mathcal{O}_F$ for each i, so that $dx \in \mathcal{O}_F$, as desired. Now, since $d\mathcal{O}_K$ is a submodule of a free-module over a PID (which, in our case, is $\mathcal{O}_F$), $d\mathcal{O}_K$ must also be free of rank $m \leq d$, as an $\mathcal{O}_F$-module. But as modules over $\mathcal{O}_F$, we have $\mathcal{O}_K \cong d\mathcal{O}_K$. The inclusion $M \subset \mathcal{O}_K$ similarly gives $d \leq m$. Therefore, $\mathcal{O}_K$ is a free $\mathcal{O}_F$-module of rank $d = [K : F]$.

Corollary 2.1.8.1. *Let $K/\mathbb{Q}_p$ be a $\mathfrak{p}$-adic number field, then $\mathcal{O}_K \cong \mathbb{Z}_p^d$, as $\mathbb{Z}_p$-modules, where $d := [K : \mathbb{Q}_p]$.*

We now describe the structure of the multiplicative group of a local field in full generality. For this, let us recall that we started initially with the decomposition $K^\times = (\pi) \times \mathcal{O}^\times$, using which we showed $K^\times = (\pi) \times \mu_{q-1} \times U^{(1)}$ in 2.1.4. Hence, we have $K^\times \cong \mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus U^{(1)}$. It now remains to compute the the $\mathbb{Z}_p$-module $U^{(1)}$; this is the content of the next theorem.

Theorem 2.1.9. *Let K be a local field and $q = p^f = |\mathcal{O}/\mathfrak{p}|$.*

1. *if char(K) $= 0$, then $K^\times \cong \mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}_p^d$, where $a \geq 0$ and $d = [K : \mathbb{Q}_p]$.*

Proof. 1. If $\mathrm{char}(K) = 0$, then we have the (algebraic and topological) isomorphism $\log : U^{(n)} \to \mathfrak{p}^n$ for $n > \frac{e}{p-1}$. Now, $\mathfrak{p}^n \cong \pi^n\mathcal{O} \cong \mathcal{O} \cong \mathbb{Z}_p^d$, as $\mathbb{Z}_p$-modules. Composing these, we get a $\mathbb{Z}_p$-module isomorphism $U^{(n)} \xrightarrow{\sim} \mathbb{Z}_p^d$. Note that $[U^{(1)} : U^{(n)}] = q^n$ is finite (hence torsion) and $U^{(n)}$ is a free $\mathbb{Z}_p$-module of rank d. Therefore, by Lemma 2.1, $U^{(1)}$ is also has rank d. From the structure theorem for finitely generated modules over PIDs, we obtain $U^{(1)} \cong \mathbb{Z}_p^d \oplus T$, where T denotes the torsion subgroup of $U^{(1)}$.

Claim: $T = \mu_{p^a}(K)$, the group of p-power roots of unity in K: Let $y \in T$, then there exists $z \in \mathbb{Z}_p$ such that $y^z = 1$. We write $z = p^a u$ where $u \in \mathbb{Z}_p^\times$ and pick $v \in \mathbb{Z}_p$ such that $uv = 1$ in $\mathbb{Z}_p$. Then, $y^z = y^{p^a u} = 1 \implies y^{p^a uv} = 1 \implies y^{p^a} = 1 \implies y \in \mu_{p^a}(K)$. Conversely, if $y \in \mu_{p^a}(K)$, then we already have $y^{p^a} = 1$, i.e., y is a torsion element, i.e., $y \in T$. This proves the claim. Hence, we finally obtain $U^{(1)} \cong \mathbb{Z}_p^d \oplus T = \mathbb{Z}_p^d \oplus \mu_{p^a}(K) \cong \mathbb{Z}_p^d \oplus \mathbb{Z}/p^a\mathbb{Z}$, as desired.