Course notes for PMATH 945

Christopher Hawthorne

Lectures by Rahim N. Moosa, Winter 2016

Contents

1 p-adic expansions

We'll be following Engler and Prestel's *Valued Fields*. All rings are commutative with identity.

Office hours are Tuesdays 2:00-4:00.

Assignment questions should be done solo.

We begin with an analogy between $\mathbb{Z}$ and $\mathbb{C}[z]$. Note that both are UFDs with respect to the representative primes (primes that represent the class of its multiples by units): in $\mathbb{Z}$ we have the positive prime numbers, and in $\mathbb{C}[z]$ we have the monic irreducible polynomials $z-a$ for $a \in \mathbb{C}$ (since $\mathbb{C}$ is algebraically closed).

In $\mathbb{C}[z]$, elements can be viewed as functions: given $f \in \mathbb{C}[z]$ we get $f\colon \mathbb{C} \to \mathbb{C}$ given by $a \mapsto f(a)$. (Really, this is the projection $\mathbb{C}[z] \to \mathbb{C}[z]/(z-a) \cong \mathbb{C}$.)

In $\mathbb{Z}$, we want to think of elements as functions on the set of positive primes. If $f \in \mathbb{Z}$, we define $f(p) = f + p\mathbb{Z} \in \mathbb{Z}/p\mathbb{Z}$.

In $\mathbb{C}[z]$, given $h = \frac{f}{g} \in \mathbb{C}(z)$ (the fraction field) and given $a \in \mathbb{C}$, as long as $g(a) \neq 0$ (i.e. $z - a \nmid g(z)$), we can declare $h(a) = \frac{f(a)}{g(a)} \in \mathbb{C}$.

In $\mathbb{Z}$, given $h = \frac{f}{g} \in \mathbb{Q}$, if $p \nmid g$ then we can set $h(p) = (f + p\mathbb{Z})(g + p\mathbb{Z})^{-1} \in \mathbb{Z}/p\mathbb{Z}$.

In $\mathbb{C}[z]$, we get Taylor series expansions by differentiating; given $h = \frac{f}{g} \in \mathbb{C}(z)$ and $a \in \mathbb{C}$ with $g(a) \neq 0$, the Taylor series expansion of h at a is the formal power series

$$\sum_{i=0}^{\infty} a_i (z-a)^i$$

where

$$a_i = \frac{h^{(i)}(a)}{i!}$$

Note that for all n we have

$$h \equiv \sum_{i=0}^{n-1} a_i (z-a)^i \pmod{(z-a)^n}$$

(working in $\mathbb{C}[z]/(z-a)^n$, and interpreting h as $(f + ((z-a)^n))(g + ((z-a)^n))^{-1} \in \mathbb{C}[z]/(z-a)^n$).

In $\mathbb{Z}$, given $f \in \mathbb{Z}$, we want $a_0, a_1, a_2, \ldots \in \{0, \ldots, p-1\}$ such that for all n we have

$$f \equiv \sum_{i=0}^{n-1} a_i p^i \pmod{p^n}$$

We do this by writing

$$\begin{aligned} f &= a_0 + f_1 p \\ f_1 &= a_1 + f_2 p \\ &\vdots \end{aligned}$$

where $0 \le a_i < p$. Then, for example

$$f = a_0 + (a_1 + f_2 p)p = a_0 + a_1 + f_2 p^2$$

and $f \equiv a_0 + a_1 p \pmod{p^2}$.

We thus have found $a_0, a_1, \ldots$ such that

$$f \equiv a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1} \pmod{p^n}$$

Definition 1.1. We call the formal sum $\sum_{i=0}^{\infty} a_i p^i$ the *p-adic expansion of f at p*.

Remark 1.2. $a_0 = f(p)$.

Continuing the analogy, we think of $i! a_i$ as the i^{th} *derivative of f at p*.

Definition 1.3. We define the *p-adic integers*, denoted $\mathbb{Z}_p$, to be the set of formal sums $\sum_{i=0}^{\infty} a_i p^i$ where each $a_i \in \{0, \ldots, p-1\}$.

We have thus defined a map $\mathbb{Z} \to \mathbb{Z}_p$.

We can extend this to $h \in \mathbb{Z}_{(p)} = \left\{ \frac{f}{g} : p \nmid g \right\} \subseteq \mathbb{Q}$: for each n there are $a_0, \ldots, a_{n-1} \in \mathbb{Z}/p\mathbb{Z}$ such that $(f + (p^n)) \cdot (g + (p^n))^{-1} = a_0 + a_1 p + \cdots + a_{n-1} p^{n-1} + (p^n)$ in $\mathbb{Z}/p^n\mathbb{Z}$. The a_i do not depend on n; we then declare that $\sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p$ is the *p-adic expansion* of $h = \frac{f}{g} \in \mathbb{Z}_{(p)}$ at p. Hence we have defined a map $\mathbb{Z}_{(p)} \to \mathbb{Z}_p$.

Proposition 1.4. *This map is injective.*

Proof. Suppose $\frac{f_1}{g_1}, \frac{f_2}{g_2} \in \mathbb{Z}_{(p)} \subseteq \mathbb{Q}$ have the same p-adic expansion. (i.e. they have the same coefficients.) Then for all $n > 0$ we have

$$\frac{f_1}{g_1} \equiv \frac{f_2}{g_2} \pmod{p^n}$$

in $\mathbb{Z}/p^n\mathbb{Z}$; so $g_2 f_1 \equiv f_2 g_1 \pmod{p^n}$, and $p^n \mid g_2 f_1 - f_2 g_1$ for all n. So $g_2 f_1 = f_2 g_1$, and $\frac{f_1}{g_1} = \frac{f_2}{g_2}$. □ Proposition 1.4

To summarize the analogy:

$\mathbb{Z}$	$\mathbb{C}[z]$
primes	$\{ z-a : a \in \mathbb{C} \} \cong \mathbb{C}$
$h \in \mathbb{Z}_{(p)}$ yields $h(p) = h \pmod{p}$	$h \in \mathbb{C}(z)$ yields $h \colon \mathbb{C} \to \mathbb{C}$ with $a \mapsto h(a)$ if a is not a pole
$\sum_{i=1}^{\infty} a_i p^i \in \mathbb{Z}_p$	$\sum_{i=0}^{\infty} \frac{h^{(i)}(a)}{i!}(z-a)^i \in \mathbb{C}[[z-a]]$
$\mathbb{Z}_p$	$\mathbb{C}[[z-a]]$

We have previously defined an injection $\mathbb{Z}_{(p)} \to \mathbb{Z}_p$; what of arbitrary $h \in \mathbb{Q}$, perhaps not in $\mathbb{Z}_{(p)}$? In the case of complex functions, we have a Laurent series; we aim for the same thing here. Write $h = \frac{1}{p^m}\frac{f}{g}$ where $\frac{f}{g} \in \mathbb{Z}_{(p)}$ and $m \geq 0$. The "p-adic expansion of h" should then be

$$\frac{1}{p^m} \underbrace{\sum_{i=0} a_i p^i}_{\substack{p\text{-adic} \\ \text{expansion of } f}}$$

Definition 1.5. Thus motivated, we define the *p-adic numbers*, denoted $\mathbb{Q}_p$, to be the set of formal series

$$\sum_{i=-m}^{\infty} a_i p^i$$

where $m \geq 0$ and each $a_i \in \{0, \ldots, p-1\}$.

Remark 1.6. We have a natural embedding $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ given by mapping $h = \frac{1}{p^m}\frac{f}{g}$ (where $p \nmid g$) to

$$\sum_{i=0}^{\infty} a_i p^{i-m}$$

where

$$\sum_{i=0}^{\infty} a_i p^i$$

is the p-adic expansion of $\frac{f}{g}$.

Definition 1.7. We call this the *p-adic expansion of $h \in \mathbb{Q}$*.

2 Ring structure

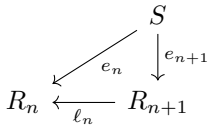
We add a ring structure by projective limits.

For $n \geq 1$ let $R_n = \mathbb{Z}/p^n\mathbb{Z}$. We then have ring homomorphisms $\lambda_n \colon R_{n+1} \to R_n$ given by $a + p^{n+1}\mathbb{Z} \mapsto a + p^n\mathbb{Z}$. (This works since $p^{n+1}\mathbb{Z} \subseteq p^n\mathbb{Z}$.) We let $R = \varprojlim R_n$ be the *projective limit* of the R_i and the λ_i, namely

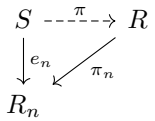
$$R = \{ (r_n : n \geq 1) : r_n \in R_n, \lambda_n(r_{n+1}) = r_n \text{ for all } n \}$$

One can check that this is a subring of $\prod_n R_n$.

This satisfies a universal property: there are surjective ring homomorphisms $\pi_n \colon R \to R_n$ induced by the projection maps on $\prod_n R_n$ such that for any ring S equipped with ring homomorphisms $e_n \colon S \to R_n$ such that the following diagram commutes:



for all n, there is a unique ring homomorphism $\pi \colon S \to R$ such that each e_n factors through π; i.e. the following diagram commutes:



(One should check this universal property.)

Proposition 2.1. *The map $\mathbb{Z}_p \to R$ given by mapping*

$$\sum_{i=0}^{\infty} a_i p^i$$

to $(r_n : n \geq 1)$ where $r_n = a_0 + a_1 p + \cdots + q_{n-1}p^{n-1} + p^n\mathbb{Z} \in \mathbb{Z}/p^n\mathbb{Z} = R_n$ is a bijection.

Proof. It is clear that the codomain is indeed R.

The key fact, which we have previously outlined, is that given $0 \leq f < p^n$ we have that f can be written uniquely in the form

$$f = a_0 + a_1 p + \cdots + a_{n-1}p^{n-1}$$

where $a_0, \ldots, a_{n-1} \in \{0, \ldots, p-1\}$.

For injectivity, suppose

$$\begin{aligned} r &= \sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z} \\ r_n &= \sum_{i=0}^{n-1} a_i p^i \\ s &= \sum_{i=0}^{\infty} b_i p^i \in \mathbb{Z} \\ s_n &= \sum_{i=0}^{n-1} b_i p^i \end{aligned}$$

If $r_n \equiv s_n \pmod{p^n}$ for all n, then since r_n and s_n are $< p^n$, the key fact yields that $a_i = b_i$ for all i.

For surjectivity, suppose $(r_n : n \geq 1) \in R = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$. By the key fact, each r_n can be written

$$r_n = a_{0,n} + a_{1,n}p + \cdots + a_{n-1,n}p^{n-1}$$

where each $a_{i,j} \in \{0, \cdots, p-1\}$. But $\lambda_n(r_{n+1}) = r_n$, so $a_{i,n+1} = a_{i,n}$ for all $n \geq 1$ and all $0 \leq i < n$; i.e. $a_{i,n}$ does not depend on n. We thus get $a_0, a_1, a_2, \ldots \in \{0, \ldots, p-1\}$ such that for all n we have

$$r_n \equiv a_0 + a_1 p + \cdots + a_{n-1}p^{n-1} \pmod{p^n}$$

So

$$\sum_{i=0}^{\infty} a_i \mapsto (r_n : n \geq 1)$$

and our map is indeed surjective. □ Proposition 2.1

We thus get an induced ring structure on $\mathbb{Z}_p$ where

$$\begin{aligned} 0 &= \sum_{i=0}^{\infty} 0 \cdot p^i \\ 1 &= 1 + \sum_{i=1}^{\infty} 0 p^i \end{aligned}$$

Multiplication is given by

$$\left(\sum a_i p^i\right) \cdot \left(\sum b_i p^i\right) = \sum c_i p^i$$

if and only if for all $n \geq 1$ we have

$$\left(\sum_{i=0}^{n-1} a_i p^i\right) \cdot \left(\sum_{i=0}^{n-1} b_i p^i\right) \equiv \sum_{i=0}^{n-1} c_i p^i \pmod{p^n}$$

Addition is given by

$$\sum a_i p^i + \sum b_i p^i = \sum c_i p^i$$

if and only if for all $n \geq 1$

$$\sum_{i=0}^{n-1} a_i p^i + \sum_{i=0}^{n-1} b_i p^i \equiv \sum_{i=0}^{n-1} c_i p^i \pmod{p^n}$$

Note that the mapping $\mathbb{Z} \hookrightarrow \mathbb{Z}_p \to R$ is given by

$$f \mapsto \underbrace{\sum_{i=0}^{\infty} a_i p^i}_{p\text{-adic expansion}} \mapsto \left(\sum_{i=0}^{n-1} a_i p^i + p^n \mathbb{Z} : n \geq 1 \right)$$

so that

$$f \equiv \sum_{i=0}^{n-1} a_i p^i \pmod{p^n}$$

We identify $\mathbb{Z}_{(p)} \subseteq \mathbb{Z}_p = R$.

Proposition 2.2. *$\mathbb{Z}_p$ is an integral domain.*

Proof. Well, $R = \varprojlim R_n$. Suppose we had $r, s \in R$ both non-zero. Say $r = (r_n + p^n\mathbb{Z} : n \geq 1)$, where $r_n \in \{0, \ldots, p^n - 1\}$. Then since $r \neq 0$, we have $r_\ell + p^n\mathbb{Z} \neq 0$ for some $\ell \geq 1$; hence $p^\ell \nmid r_\ell$, and hence $p^\ell \nmid r_n$ for $n \geq \ell$ (since for $n \geq \ell$ we have $r_n \equiv r_\ell \pmod{p^\ell}$). Likewise with s, there is $m \geq 1$ such that for all $n \geq m$ we have $p^m \nmid s_n$. Now, $rs = (r_n s_n + p^n\mathbb{Z} : n \geq 1)$; let $N = \ell + m$. Then if $r_N s_N + p^n\mathbb{Z} = 0$ in $\mathbb{Z}/p^N\mathbb{Z}$ then $p^N \mid r_N s_N$. But $N \geq \ell$, so $p^\ell \nmid r_N$; so $p^m \mid s_N$, a contradiction since $N \geq m$. □ Proposition 2.2

Lemma 2.3. *The units of $\mathbb{Z}_p$ are exactly the sums*

$$\sum_{i=0}^{\infty} a_i p^i$$

where $a_0 \neq 0$.

Proof. Let $R_n = \mathbb{Z}/p^n\mathbb{Z}$ and $\lambda_n \colon R_{n+1} \to R_n$; then $\mathbb{Z}_p = \varprojlim R_n$, as before.

Claim 2.4. *An element in $\varprojlim R_n$ is invertible if and only if it is invertible in $\prod_n R_n$.*

Proof.

($\Longrightarrow$) Immediate.

($\Longleftarrow$) Suppose $r \in \varprojlim R_n$ and $s \in \prod_n R_n$ with $rs = 1$ in $\prod_n R_n$; we wish to show that $s \in \varprojlim R_n$. Note that $rs = 1$ if and only if for all n we have $r_n s_n = 1$ (where $r = (r_n : g \geq 1)$ for $r_n \in R_n$, and likewise with s). Fix $n \geq 1$. Then $r_{n+1} s_{n+1} = 1$ in R_{n+1}, so $\lambda_n(r_{n+1})\lambda_n(s_{n+1}) = 1$ in R_n. Since $r \in \varprojlim R_n$, we have that $\lambda_n(r_{n+1}) = r_n$. So $r_n \lambda_n(s_{n+1}) = 1$ in R_n; so $\lambda_n(s_{n+1}) = s_n$ by uniqueness of inverses in R_n. So $s \in \varprojlim R_n$, as desired. □ Claim 2.4

So $\sum a_i p^i \in \mathbb{Z}_p$ is invertible if and only if $a_0 + a_1 p + \cdots + a_{n-1} p^{n-1}$ is invertible in $\mathbb{Z}/p^n\mathbb{Z}$ for all $n \geq 1$, which occurs if and only if $p \nmid a_0 + \cdots + a_{n-1} p^{n-1}$, which occurs if and only if $a_0 \neq 0$. □ Lemma 2.3

Corollary 2.5. *$\mathbb{Z}_p$ is a local ring with maximal ideal $p\mathbb{Z}_p$ and residue field $\mathbb{Z}/p\mathbb{Z}$.*

Proof. Note that

$$p\left(\sum_{i=0}^{\infty} a_i p^i \right) = \sum_{i=0}^{\infty} a_i p^{i+1}$$

since for all $n \geq 1$ we have

$$p(a_0 + \cdots + a_{n-1}p^{n-1}) = a_0 p + \cdots + a_{n-1}p^n \equiv a_0 p + \cdots + a_{n-2}p^{n-1} \pmod{p^n}$$

Hence

$$p\mathbb{Z}_p = \left\{ \sum_{i=0}^{\infty} a_i p^i : a_0 = 0 \right\}$$

which is just the set of non-units. Hence $p\mathbb{Z}_p$ contains every proper ideal and is thus the unique maximal ideal.

For the residue field, note that we have

$$\begin{aligned} \pi_1 \colon \mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z} &\to \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p \\ \sum a_i p^i &\mapsto a_0 + p\mathbb{Z} \end{aligned}$$

Now, π_1 is a surjective ring homomorphism with kernel $p\mathbb{Z}_p$ (since $a_0 < p$); hence $\mathbb{Z}_p/p\mathbb{Z}_p$. □ Corollary 2.5

Notation 2.6. We use $\mathbb{Z}_p$ to denote the p-adics, $\mathbb{Z}_{(p)}$ to denote the localization of $\mathbb{Z}$ at $p\mathbb{Z}$, and $\mathbb{F}_p$ to denote $\mathbb{Z}/p\mathbb{Z}$.

Lemma 2.7. *Every element of* $\operatorname{Frac}(\mathbb{Z}_p)$ *can be represented in the form* $\frac{r}{p^m}$ *for some* $r \in \mathbb{Z}_p$.

Proof. Given

$$\frac{\sum a_i p^i}{\sum b_i p^i} \in \operatorname{Frac}(\mathbb{Z}_p)$$

let $m \geq 0$ be least such that $b_m \neq 0$; i.e. $b_0 = b_1 = \cdots = b_{m-1} = 0$. So

$$\sum b_i p^i = b_m p^m + b_{m+1}p^{+1} + \cdots = p^m \left(\underbrace{b_m + b_{m+1}p + \cdots}_{\text{unit of } \mathbb{Z}_p} \right)$$

We can thus write $\sum b_i p^i = p^m r^{-1}$ for some $r \in \mathbb{Z}_p$; hence

$$\frac{\sum a_i p^i}{\sum b_i p^i} = \frac{r \sum a_i p^i}{p^m}$$

as desired. □ Lemma 2.7

Recall we defined

$$\mathbb{Q}_p = \left\{ \sum_{i=-m}^{\infty} a_i p^i : m \geq 0, 0 \leq a_i < p \right\}$$

We thus get a map $\mathbb{Q}_p \to \operatorname{Frac}(\mathbb{Z}_p)$ given by

$$\sum_{i=-m}^{\infty} a_i p^i \mapsto \frac{\sum_{i=-m}^{\infty} a_i p^{i+m}}{p^m}$$

This is a bijection that is the identity on $\mathbb{Z}_p$; this thus induces a field structure on $\mathbb{Q}_p$.

3 Metric and topological structure

We give a third (and final) characterization of the p-adics that will induce a metric and topology; we now follow chapter 1 of the book.

We use the *p-adic absolute value*: the idea is that we can construct $\mathbb{Q}_p$ from $\mathbb{Q}$ very much as we construct $\mathbb{R}$ from $\mathbb{Q}$ (i.e. as a metric completion), but using a different absolute value on $\mathbb{Q}$.

Fix a prime p.

Definition 3.1 (p-adic absolute value on $\mathbb{Q}$)**.** Suppose $r \in \mathbb{Q}$. If $r = 0$, we set $|r|_p = 0$. If $r \neq 0$, we write $r = p^\eta \frac{a}{b}$ where $a, b \in \mathbb{Z}$, $p \nmid a$, $p \nmid b$, and $\eta \in \mathbb{Z}$; we then set $|r|_p = \exp(-\eta) > 0$.

Remark 3.2. Note that an integer gets smaller in $|\cdot|_p$ the higher the power of p that divides it.

Remark 3.3. Given $r \in \mathbb{Z}_p$ with $r = \sum a_i p^i$, we can consider the sequence of integers $(a_i p^i : i \geq 0)$; this then converges to 0 in $|\cdot|_p$.

Definition 3.4. Suppose K is a field. An *absolute value on* K is a function $|\cdot| \colon K \to \mathbb{R}_{\geq 0}$ satisfying the following:

1. $|x| = 0 \iff x = 0$.
2. $|xy| = |x||y|$.
3. $|x + y| \leq |x| + |y|$.

Proposition 3.5. *$|\cdot|_p$ is an absolute value on $\mathbb{Q}$.*

Proof. (1) and (2) are clear; we check the triangle inequality. Suppose $x, y \in \mathbb{Q}$; say

$$x = p^\theta \frac{a}{b}$$
$$y = p^\gamma \frac{c}{d}$$

where $p \nmid abcd$. So $|x|_p = \exp(-\theta)$ and $|y|_p = \exp(-\gamma)$. Assume without loss of generality that $\theta \leq \gamma$. Then

$$x + y = \frac{p^\theta ad + p^\theta cb}{bd} = p^\theta \left(\frac{ad + p^{\gamma - \theta} cb}{bd} \right)$$

Hence

$$|x + y|_p \leq \exp(-\theta) = \max(\exp(-\theta), \exp(-\gamma)) = \max(|x|_p, |y|_p) \leq |x|_p + |y|_p$$

and $|\cdot|_p$ satisfies the triangle inequality. □ Proposition 3.5

In fact, we showed a stronger property: we showed that

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

Definition 3.6. Such absolute values are called *non-Archimedean.*

So $(\mathbb{Q}, |\cdot|)$ is Archimedean, and $(\mathbb{Q}, |\cdot|_p)$ is non-Archimedean; these turn out to be all the absolute values on $\mathbb{Q}$.

Proposition 3.7 (1.1.1)**.** *Suppose $(K, |\cdot|)$ is an absolute valued field. Then $(K, |\cdot|)$ is Archimedean if and only if $X = \{\, |n| : n \in \mathbb{Z} \,\}$ is unbounded in $\mathbb{R}_{\geq 0}$.*

Proof. We note that

$$|1| = |1 \cdot 1| = |1||1| = |1|^2$$

and hence that $|1| = 1$. We further note that

$$|-1|^2 = |(-1)^2| = |1| = 1$$

and hence in general that $|-x| = |x|$

($\Longleftarrow$) Suppose $(K, |\cdot|)$ is non-Archimedean. Then $|n| = |1 + \cdots + 1| \leq \max\{\, |1|, \ldots, |1| \,\} = 1$; so $|n| \leq 1$. We get a similar result for $n < 0$.

($\implies$) Suppose X is bounded by $C \in \mathbb{R}_{>0}$. Suppose $n \in \mathbb{N}$. Then

$$\begin{aligned} |x+y|^n &= |(x+y)^n| \\ &= \left| \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i} \right| \\ &\leq \sum_{i=0}^{n} \left| \binom{n}{i} \right| |x|^i |y|^{n-i} \\ &\leq \sum_{i=0}^{n} C|x|^i |y|^{n-i} \\ i \leq \sum_{i=0}^{n} C(\max(|x|,|y|)^n) \\ &= (n+1)C(\max(|x|,|y|))^n \end{aligned}$$

So $|x+y| \leq \max(|x|,|y|) \sqrt[n]{(n+1)C}$. But $\sqrt[n]{(n+1)C} \to 1$ as $n \to \infty$; so $|x+y| \leq \max(|x|,|y|)$. □ Proposition 3.7

Now, if $(K, |\cdot|)$ is an absolute valued field, then we have a metric on K defined by $\operatorname{dist}(x,y) = |x-y|$, which in turn induces a topology on K. The basic open sets will be

$$B_\varepsilon(a) = \{\, b \in K : |a-b| < \varepsilon \,\}$$

for $\varepsilon > 0$ real and $a \in K$.

Lemma 3.8. *$|\cdot| : K \to \mathbb{R}_{\geq 0}$ is uniformly continuous. In fact, if $x, y \in K$ then*

$$\Big| |x| - |y| \Big|_{\mathbb{R}} \leq |x-y|$$

Proof. Well,

$$|x| = |x-y+y| \leq |x-y| + |y|$$

so $|x| - |y| \leq |x-y|$. Similarly, we get $|y| - |x| \leq |y-x| = |x-y|$. □ Lemma 3.8

3.1 Completions

Suppose $(K, |\cdot|)$ is an absolute valued field.

Definition 3.9. A sequence $(a_n : n \geq 0)$ in K is *Cauchy* if for every $\varepsilon > 0$ there is an $N \in \mathbb{N}$ such that $|a_n - a_m| < \varepsilon$ for all $n, m > N$. It *converges* to $b \in K$ if and only if for every $\varepsilon > 0$ there is $N \in \mathbb{N}$ such that $|a_n - b| < \varepsilon$ for all $n > N$.

Remark 3.10. By the triangle inequality, convergent sequences are Cauchy.

Definition 3.11. We say $(K, |\cdot|)$ is *complete* if every Cauchy sequence is convergent.

Example 3.12.

- $(\mathbb{Q}, |\cdot|)$ is not complete: take any sequence of rationals converging to an irrational.
- $(\mathbb{Q}, |\cdot|_p)$ (for p prime) is not complete. Let $s = \sum a_i p^i \in \mathbb{Z}_p$; for $n \geq 0$ let $s_n = a_0 + a_1 p + \cdots + a_{n-1} p^{n-1}$. Then $(s_n : n \geq 0)$ is Cauchy in $(\mathbb{Q}, |\cdot|_p)$ since given $m < n$ we have

$$\begin{aligned} |s_n - s_m|_p &= |a_m p^m + \cdots + a_{n-1} p^{n-1}|_p \\ &= |p^m (a_m + a_{m+1} p + \cdots + a_{n-1} p^{n-1-m})|_p \\ &\leq \exp(-m) \\ &\to 0 \end{aligned}$$

  Similarly, if $s \in \mathbb{Q}_p$ and the s_n are the partial sums then $(s_n : n \geq 0)$ is Cauchy.

Exercise 3.13. $(s_n : n \geq 0)$ will converge in $(\mathbb{Q}, |\cdot|_p)$ if and only if $s \in \mathbb{Q}$.

So for $s \in \mathbb{Q}_p \setminus \mathbb{Q}$ we get a non-convergent Cauchy sequence by looking at the partial sums.

Exercise 3.14. $s = \sum a_i p^i \in \mathbb{Q}_p$ is in $\mathbb{Q}$ if and only if $(a_i : i \geq 0)$ is eventually periodic.

Theorem 3.15 (1.1.4)**.** *Given an absolute valued field $(K, |\cdot|)$ there is a complete absolute valued field $(\widehat{K}, \widehat{|\cdot|})$ with a field embedding $\iota \colon K \hookrightarrow \widehat{K}$ satisfying the following:*

1. *$\widehat{|\iota(x)|} = |x|$ for all $x \in K$.*
2. *$\iota(K)$ is dense in $\widehat{K}$.*
3. *The universal property: if $(K_1, |\cdot|_1)$ is another complete absolute valued field with $\iota_1 \colon K \hookrightarrow K_1$ a field embedding satisfying $|\iota_1(x)|_1 = |x|$ then there is a unique continuous field embedding $\varphi \colon \widehat{K} \to K_1$ such that the following diagram commutes:*

$$\begin{array}{ccc} \widehat{K} & \overset{\varphi}{\dashrightarrow} & K_1 \\ {\scriptstyle\iota}\uparrow & \nearrow_{\iota_1} & \\ K & & \end{array}$$

If $\iota_1(K)$ is dense in K, then φ is an isomorphism. We call $(\widehat{K}, \widehat{|\cdot|})$ the completion.

Proof. This imitates the construction of $\mathbb{R}$ from $\mathbb{Q}$. Let $\mathcal{C}$ be the set of all Cauchy sequences in $(K, |\cdot|)$.

Claim 3.16. *$\mathcal{C}$ with coordinate-wise operations is a commutative ring with unity.*

Let

$$\mathcal{N} = \left\{ (a_n : n \geq 0) \in \mathcal{C} : \lim_{n \to \infty} |a_n| = 0 \right\}$$

Note that by uniform continuity if $(a_n : n \geq 0) \in \mathcal{C}$ then $(|a_n| : n \geq 0)$ is Cauchy in $\mathbb{R}$; since $(\mathbb{R}, |\cdot|)$ is complete, we get that $(|a_n| : n \geq 0)$ converges.

Claim 3.17. *$\mathcal{N}$ is an ideal of $\mathcal{C}$.*

Claim 3.18. *If $(a_n : n \geq 0) \in \mathcal{C} \setminus \mathcal{N}$ then $(|a_n| : n \geq 0)$ is bounded away from 0 eventually.*

Claim 3.19. *$\mathcal{N}$ is a maximal ideal.*

Define $\widehat{K} = \mathcal{C}/\mathcal{N}$; then $\widehat{K}$ is a field. Given $\alpha \in \widehat{K}$, say $\alpha = (a_n : n \geq 0) + \mathcal{N}$ for $(a_n : n \geq 0) \in \mathcal{C}$, set

$$\widehat{|\alpha|} = \lim_{n \to \infty} |a_n|$$

One checks that this is a well-defined absolute value on $\widehat{K}$. We now have $\iota \colon K \to \widehat{K}$ given by $x \mapsto (x : n \geq 0) + \mathcal{N}$ represented by the constant sequence. One checks that this is a field embedding preserving absolute value.

Claim 3.20. *$\iota(K)$ is dense in $\widehat{K}$.*

Claim 3.21. *$(\widehat{K}, \widehat{\cdot})$ is complete.*

Claim 3.22. *$(\widehat{K}, \widehat{\cdot})$ satisfies the universal property.*

□ Theorem 3.15

Consider now the completion of $(\mathbb{Q}, |\cdot|_p)$. Let R be the ring of all Cauchy sequences in $(\mathbb{Q}, |\cdot|_p)$; let M be the set of null sequences, and let $\widehat{Q} = R/M$.

Remark 3.23. Given $(a_n : n \geq 0) \in R$, if we let $\alpha = (a_n : n \geq 0) + M \in \widehat{\mathbb{Q}}$, then

$$\widehat{|\alpha|}_p = \lim_{n \to \infty} |a_n|_p \in \mathbb{R}$$

Remark 3.24. Either $\alpha = 0$ or $(|a_n|_p : n \geq 0)$ is eventually constant in $\mathbb{R}$ (since $|a_n|_p$ is an integer power of e).

We now show that $\widehat{\mathbb{Q}} = \mathbb{Q}_p$. Let

$$S = \overline{B}_1(0) = \{\, \alpha \in \widehat{\mathbb{Q}} : \widehat{|\alpha|}_p \leq 1 \,\}$$

Exercise 3.25. S is a subring of $\widehat{\mathbb{Q}}$.

Lemma 3.26. *S is the closure of $\mathbb{Z} \subseteq \widehat{\mathbb{Q}}$.*

Proof. We first note that $\mathbb{Z} \subseteq S$ since if $r \in \mathbb{Z}$ then

$$\widehat{|r|}_p = |r|_p = \exp(-n) \leq 1$$

where $p^n \mid r$ and $p^{n+1} \nmid r$. Suppose now that $(x_n : n \geq 0)$ is a sequence in $\mathbb{Z}$ with

$$\lim_{n\to\infty} x_n = \alpha \in \widehat{\mathbb{Q}}$$

Then

$$1 \geq |x_n|_p \xrightarrow{n\to\infty} \widehat{|\alpha|}_p$$

Hence $\widehat{|\alpha|}_p \leq 1$, and $\alpha \in S$.

Conversely, suppose $\alpha \in S$. If $\alpha = 0$, then $\alpha \in \mathbb{Z}$; assume then that $\alpha \neq 0$. Say $\alpha = (r_n : n \geq 0) + M \in \widehat{\mathbb{Q}}$; then

$$\lim_{n\to\infty} |r_n|_p = \widehat{|\alpha|}_p \leq 1$$

since $\alpha \in S$. Hence there is n_0 such that for all $n \geq n_0$ we have $|r_n|_p \leq 1$, and hence $r_n = \frac{a_n}{b_n}$ with $a_n, b_n \in \mathbb{Z}$ and $p \nmid b_n$. In particular, b_n is invertible in $\mathbb{Z}/p^n\mathbb{Z}$; let $c_n \in \mathbb{Z}$ be such that $b_n c_n \equiv a_n \pmod{p^n}$, so $p^n \mid (a_n - b_n c_n)$. Then

$$|r_n - c_n|_p = \left|\frac{a_n}{b_n} - c_n\right|_p = \left|\frac{a_n - b_n c_n}{b_n}\right|_p \leq \exp(-n) \to 0$$

But $(|r_n - c_n|_p : n \geq 0) \to 0$ as well; so

$$\alpha = (r_n : n \geq 0) + M = (c_n : n \geq 0) + M$$

in $\widehat{\mathbb{Q}}$. So

$$\lim_{n\to\infty} c_n = \alpha$$

in $\widehat{\mathbb{Q}}$. □ Lemma 3.26

It follows that every $\alpha \in S$ is of the form $(a_n : n \geq 0) + M$ where $(a_n : n \geq 0)$ is a Cauchy sequence in $\mathbb{Z}$. We get a projection $\rho_n \colon \mathbb{Z} \to S/p^n S$ (from the inclusion $\mathbb{Z} \to S$); this induces a map $\overline{\rho_n} \colon \mathbb{Z}/p^n\mathbb{Z} \to S/p^n S$.

Lemma 3.27. *$\overline{\rho_n}$ is an isomorphism of rings for all $n \geq 1$.*

Proof. Fix $n \geq 1$.

Surjectivity We first check that ρ_n is surjective. Suppose $\alpha \in S$. If $\alpha \in \mathbb{Z}$, we're done; we may thus assume that $\alpha \notin \mathbb{Z}$. We want $a \in \mathbb{Z}$ such that $\alpha - a \in p^n S$. Pick $a \in \mathbb{Z}$ such that $\widehat{|\alpha - a|}_p \leq \exp(-n)$. Say $\alpha = (b_m : m \geq 0) + M$ for $b_m \in \mathbb{Z}$; then $0 \neq \alpha - a = (b_m - a : m \geq 0) + M$, and

$$\exp(-n) \geq \widehat{|\alpha - a|}_p = \lim_{m\to\infty} |b_m - a|_p$$

with the latter sequence eventually constant; hence there is m_0 such that for all $m \geq m_0$ we have $|b_m - a|_p \leq \exp(-n)$. Hence $p^n \mid (b_m - a)$, and hence $b_m - a = p^n c_m$ for some $c_m \in \mathbb{Z}$. Note that as $(b_m : m \geq 0)$ is Cauchy in $\mathbb{Z}$, so too is $(c_m : m \geq 0)$. But now

$$\alpha - a = (p^n c_m : m \geq 0) + M = p^n((c_m : m \geq 0) + M) \in p^n S$$

so ρ_n is surjective, as desired.

Injectivity We check that $\ker(\rho_n) = p^n\mathbb{Z}$. Suppose $a \in \mathbb{Z}$ has $a \in p^n S$. Then $a = p^n\beta$ with $\beta \in S$, say $\beta = (b_m : m \geq 0) + M$ with $b_m \in \mathbb{Z}$. Then

$$|a|_p = \widehat{|a|}_p = \lim_{m\to\infty} |p^n b_m|_p \leq \exp(-n)$$

so $p^n \mid a$ in $\mathbb{Z}$, as desired. □ Lemma 3.27

Note now that the following diagram commutes:

$$\begin{array}{ccccc} S & \xrightarrow{\theta_{n+1}} & S/p^{n+1}S & \xrightarrow{\cong} & \mathbb{Z}/p^{n+1}\mathbb{Z} \\ & \searrow^{\theta_n} & & & \downarrow{\scriptstyle \lambda_n} \\ & & S/p^n S & \xrightarrow{\cong} & \mathbb{Z}/p^n\mathbb{Z} \end{array}$$

By the universal product of projective limits, we get a map $\theta\colon S \to \varprojlim \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p$ given by $\alpha \mapsto (\theta_n(\alpha) : n \geq 0)$.

Proposition 3.28. *θ is an isomorphism of rings.*

Proof.

Injectivity Suppose $\theta(\alpha) = 0$. Then $\alpha \in p^n S$ for all $n \geq 1$. So

$$\widehat{|\alpha|}_p = \widehat{|p^n \underbrace{\beta_n}_{\in S}|}_p = \widehat{|p^n|}_p \underbrace{\widehat{|\beta_n|}_p}_{\leq 1} \leq \exp(-n)$$

for all $n \geq 1$; so $\widehat{|\alpha|}_p = 0$, and $\alpha = 0$.

Surjectivity Suppose $s \in \mathbb{Z}_p$; let $(s_m : m \geq 0)$ be the sequence of partial sums. We know $(s_m : m \geq 0)$ is Cauchy in $\mathbb{Z}$; let

$$\alpha = (s_m : m \geq 0) + M \in S$$

For each $n \geq 1$, we then have $\alpha - s_n = (s_m - s_n : m \geq 0) + M$. If $m \geq n$, we the have that $p^n \mid s_m - s_n$. Hence $\alpha - s_n \in p^n S$, and hence $\theta(\alpha) = s$. □ Proposition 3.28

TODO 1. *Consistency of indices?*

Note that the above map is given by

$$\sum_{i=0}^{\infty} a_i p^i \mapsto \left(\sum_{i=0}^{n-1} a_i p^i : n \geq 0 \right) + M$$

Lemma 3.29. *$\widehat{\mathbb{Q}} = \mathrm{Frac}(S)$. In fact, if $\alpha \in \widehat{\mathbb{Q}}$ then $\alpha = \frac{\beta}{p^m}$ for some $m \geq 0$ and some $\beta \in S$.*

Proof. Take $\alpha \in \widehat{\mathbb{Q}}$. If $\widehat{|\alpha|}_p \leq 1$ then $\alpha \in S$ and we're done. Suppose then that $\widehat{|\alpha|}_p > 1$; then $\widehat{|\alpha|}_p = \exp(m)$ for some $m > 0$. So $\widehat{|p^m\alpha|}_p = |p^m|_p \widehat{|\alpha|}_p = \exp(-m)\exp(m) = 1$. So $p^m\alpha \in S$, as desired. □ Lemma 3.29

Hence we have commuting isomorphisms

$$\begin{array}{ccc} \widehat{\mathbb{Q}} & \longleftarrow & \mathbb{Q}_p \\ \subseteq\uparrow & & \subseteq\uparrow \\ S & \xleftarrow[f]{\cong} & \mathbb{Z}_p \end{array}$$

Explicitly, $\alpha \in \mathbb{Q}_p$ is $\frac{\beta}{p^m}$ for some $\beta \in \mathbb{Z}_p$. The image is $\frac{f(\beta)}{p^m}$.

We thus obtain an induced absolute value on $\mathbb{Q}_p$ that we denote by $|\cdot|_p$; this extends $|\cdot|_p$ on $\mathbb{Q}$. Note that $\mathbb{Q}_p$ is complete under this absolute value; further note that $\mathbb{Z}_p = \overline{B_1(0)}$.

Given $\alpha \in \mathbb{Q}_p$, if $\alpha = 0$ then $|\alpha|_p = 0$. If $\alpha \neq 0$ then

$$\alpha = \sum_{i=m}^{\infty} a_i p^i$$

for some $m \in \mathbb{Z}$ with $a_m \neq 0$ and $a_i \in \{0, \dots, p-1\}$. Then

$$|\alpha|_p = \left| p^m \sum_{i=m}^{\infty} a_i p^{i-m} \right|_p = |p^m|_p \underbrace{\left| \sum_{i=m}^{\infty} a_i p^{i-m} \right|_p}_{\in \mathbb{Z}_p} = \exp(-m) \lim_{n\to\infty} \Big| \underbrace{a_m}_{\neq 0} + a_{m+1}p + \cdots + a_{m+n-1}p^{n-1} \Big|_p = \exp(-m)$$

Exercise 3.30. In a non-archimedean absolute valued field, every point of an open ball is its center.

Remark 3.31. $p\mathbb{Z}_p = B_1(0)$ since if $\alpha \in \mathbb{Z}_p$ then

$$|p\alpha|_p = |p|_p |\alpha|_p = \exp(-1)|\alpha|_p < 1$$

and if $|\alpha|_p < 1$ and $\alpha \in \mathbb{Z}_p$, the power that appears is negative; so

$$\left| \frac{\alpha}{p} \right|_p \leq 1$$

and $\frac{\alpha}{p} \in \mathbb{Z}_p$, and $\alpha \in p\mathbb{Z}_p$.

Fact 3.32. *The only complete Archimedean absolute valued fields are $\mathbb{R}$ and $\mathbb{C}$, up to inducing the same topology (where $\mathbb{R}$ and $\mathbb{C}$ carry the usual absolute values).*

Fact 3.33 (Ostrowski's theorem)**.** *On $\mathbb{Q}$, up to inducing the same topology, the only Archimedean absolute value is the usual one, and the only non-Archimedean ones are $|\cdot|_p$ for p prime. (Aside from the trivial one.)*

There are many interesting non-Archimedean absolute valued fields besides the family $(\mathbb{Q}, |\cdot|_p)$.

Example 3.34. Let K be any field, and consider the rational functions $K(t)$. We define the *t-adic absolute value* to be

$$\left| \frac{f}{g} \right| = \exp(-\eta)$$

where η is the highest power of t dividing g. The completion is $K((t))$ (Laurent series in t) where

$$\left| \sum_{i=m}^{\infty} a_i t^i \right| = \exp(-m)$$

where $m \in \mathbb{Z}$ and $a_m \neq 0$. (Note that m is the order of vanishing of the Laurent series at 0.)

It is convenient to switch to additive notation at this point: given a non-Archimedean absolute valued field $(K, |\cdot|)$, we define $v \colon K \to \mathbb{R} \cup \{\infty\}$

$$v(x) = \begin{cases} -\log(|x|) & \text{if } x \neq 0 \\ \infty & \text{else} \end{cases}$$

In $(\mathbb{Q}_p, |\cdot|_p)$ we have

$$v\left(\sum_{i=m}^{\infty} a_i p^i \right) = -\log(\exp(-m)) = m$$

In $(K((t)), |\cdot|)$, we have

$$v\left(\sum_{i=m}^{\infty} a_i t^i \right) = m$$

This function v is called a *valuation*. The axioms for $|\cdot|$ become

1. $v(x) = \infty$ if and only if $x = 0$.
2. $v(xy) = v(x) + v(y)$.
3. $v(x + y) \geq \min\{ v(x), v(y) \}$.

By convention we set $\infty = \infty + \infty = r + \infty = \infty + r$ for all $r \in \mathbb{R}$.

Remark 3.35. The triangle inequality for $|\cdot|$ does not have a nice aditive formulation.

Definition 3.36. A *classical valued field* is a field K equipped with a valuation $v\colon K \to \mathbb{R} \cup \{ \infty \}$ satisfying the axioms listed above.

Every classical valued field comees from a non-Archimedean absolute valued field via $|x| = \exp(-v(x))$. We thus identify classical valued fields with non-Archimedean absolute valued fields.

Proposition 3.37. *If (K, v) is a classical valued field and $v(x) \neq v(y)$ then $v(x + y) = \min\{ v(x), v(y) \}$.*

Proof. Assume without loss of generality that $v(x) > v(y)$. If $v(x + y) > v(y)$, then

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

a contradiction. So $v(x + y) = v(y)$. □ Proposition 3.37

Note that $v\colon K^\times \to \mathbb{R}$ is a homomorphism into $\mathbb{R}$ under addition.

Remark 3.38. Given a sequence $(a_n : n \geq 0)$ in K, we have

$$\lim_{n\to\infty} a_n = a$$

if and only if

$$\lim_{n\to\infty} v(a - a_n) = \infty$$

Definition 3.39. Fix a classical valued field (K, v). We define *open balls* $B_\varepsilon(c)$ for $\varepsilon \in \mathbb{R}$ and $c \in K$ to be

$$B_\varepsilon(c) = \{ x \in K : v(x - c) > \varepsilon \}$$

If $x \in K$ then we sometimes use $B_x(c) = \{ x \in K : v(x - c) > v(x) \}$. We define the *valuation ring* to be $\mathcal{O}_v = \overline{B_{v(1)}(0)} = \{ x \in K : v(x) \geq 0 \}$. (As before, this is a subring of K by the valuation axioms.) We set $\mathcal{M}_v = B_{v(1)}(0) = \{ x \in K : v(x) > 0 \}$; this is an ideal of $\mathcal{O}_v$ since for $x \in \mathcal{M}_v$ and $a \in \mathcal{O}_v$ we have $v(ax) = v(a) + v(x) > 0 + 0 = 0$.

Remark 3.40. Given $x \in K^\times$, note that $v\left(\frac{1}{x}\right) = -v(x)$; hence either x or $-x$ lies in $\mathcal{O}_v$. The units of $\mathcal{O}_v$ are the $x \in K^\times$ such that both x and $\frac{1}{x}$ are in $\mathcal{O}_v$; i.e. with $v(x)$ and $v(-x)$ both non-negative, i.e. with $v(x) = 0$. Hence the units of $\mathcal{O}_v$ are precisely the elements not in $\mathcal{M}_v$, so $\mathcal{M}_v$ is the unique maximal ideal of $\mathcal{O}_v$; i.e. $\mathcal{O}_v$ is a local ring.

Definition 3.41. We define the *residue field* of (K, v) to be $\overline{K}_v = \mathcal{O}_v/\mathcal{M}_v$. We use $\mathrm{res}\colon \mathcal{O}_v \to \overline{K}_v$ to denote the quotient map. The image $v(K^\times)$ is a subgrape of $\mathbb{R}$ called the *value grape*.

In all our examples, the value grape has been $\mathbb{Z}$.

	$(\mathbb{Q}, v_p)$	$(\mathbb{Q}_p, v_p)$	$(K(t), v_t)$	$(K((t)), v_t)$	K
$\mathcal{O}_V$	$\mathbb{Z}_{(p)}$	$\mathbb{Z}_p$	$K[t]_{(t)}$	$K[[t]$	$\bigcup_{n\geq 1} K[[t^{\frac{1}{n}}]$
$\mathcal{M}_v$	$p\mathbb{Z}_{(p)}$	$p\mathbb{Z}_p$	$tK[t]_{(t)}$	$tK[[t]$	$\bigcup_{n\geq 1} t^{\frac{1}{n}} k[[t^{\frac{1}{n}}]]$
$\overline{K}_v$	$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$	$\mathbb{F}_p$	K	K	K
$v(K^\times)$	$\mathbb{Z}$	$\mathbb{Z}$	$\mathbb{Z}$	$\mathbb{Z}$	$\mathbb{Q}$

The last column refers to *Puiseux series*, which we now expound on.

Suppose K is a field; fix $n \geq 1$ and consider $K_n = K((t^{\frac{1}{n}}))$. (Note that $K_n \cong K((t))$.) The valuation v_n on K_n is $v_n(\alpha(t^{\frac{1}{n}})) = \frac{v_t(\alpha)}{n}$, for $\alpha \in K((t))$.

If $n \mid \ell$ then there is a natural identification $K_n \subseteq K_\ell$ as a field extension. Indeed, say $\ell = nm$; we then identify $t^{\frac{1}{n}} = \left(t^{\frac{1}{nm}}\right)^m = \left(t^{\frac{1}{\ell}}\right)^m$.

We have $v_\ell \restriction K_n = v_n$; this is easily seen. So we can take the direct limit: we get

$$K = \bigcup_{n \geq 1} K_n$$

and

$$v = \bigcup_{n \geq 1} v_n$$

a classical valuation on K. If $f \in K$ is non-zero, then it takes the form

$$\sum_{i=m}^{\infty} a_i t^{\frac{i}{n}}$$

for $m \in \mathbb{Z}$, $n \geq 1$, $a_m \neq 0$ and $a_m \in K$; then $v(f) = \frac{i}{n}$. Note $f \in \mathcal{O}_v$ if and only if $m \geq 0$ and $f \in \mathcal{M}_v$ if and only if $m > 0$.

Something to try: consider $K((t))^{\mathrm{alg}}$. But K is not complete.

We now return to general classical valued fields. Suppose (K, v) is a classical valued field, with $\mathcal{O}_v = \overline{B_1(0)}$. Let $c \in K$. Then

$$\begin{aligned}
\overline{B_1(c)} &= \{\, x \in K : |x - c| \leq 1 \,\} \\
&= \{\, x \in K : v(x - c) \geq 0 \,\} \\
&= \{\, x \in K : x - c \in \mathcal{O}_v \,\} \\
&= c + \mathcal{O}_v
\end{aligned}$$

Conclusion: the closed unit balls are just the additive translates of $\mathcal{O}_v$ in K.

What of other radii? Consider radii in the value grape; i.e. r is in the image of $|\cdot|$. Suppose $r > 0$ is real and $r = |d|$ for some $d \in K$. Take $c \in K$ and consider $\overline{B_\gamma}(c) = \overline{B_r}(c)$, where $\gamma = v(r) = -\ln(r)$. We consider the case $c = 0$. Then

$$\begin{aligned}
B_r(0) &= \{\, x \in K : |x| \leq |d| \,\} \\
&= \{\, x \in K : v(x) \geq v(d) = \gamma \,\} \\
&= \left\{\, x \in K : v\left(\frac{x}{d}\right) \geq 0 \,\right\} \\
&= \left\{\, x \in K : \frac{x}{d} \in \mathcal{O}_v \,\right\} \\
&= d\mathcal{O}_v
\end{aligned}$$

More generally, $\overline{B_r}(c) = c + d\mathcal{O}_v$. These are all additive translates of $\mathcal{O}_v$-submodules of K, as closed balls whose radius is in the value grape.

Remark 3.42. Suppose (k, v) is a classical valued field; we get an absolute value with $|x| = \exp(-v(x))$. A basis for the topology is sets of the form

$$B_r(c) = \{\, x \in K : |x - c| < r \,\}$$

for $c \in K$ and $r \in \mathbb{R}$ with $r > 0$. In fact one can check that a basis for the topology is the set of open *realized* balls: the $B_r(c)$ where r is in the image of $|\cdot|$. (The point is that every closed realized ball is a union of open realized balls.) In valuation notation, the realized balls take the form

$$B_{v(d)}(c) = \{\, x \in K : v(x - c) > v(d) \,\}$$

for $c \in K$ and $d \in K^\times$.

We saw last time that

$$B_{v(d)}(c) = c + d\mathcal{M}_v$$
$$\overline{B}_{v(d)}(c) = c + d\mathcal{O}_v$$

TODO 2. *I think in the future we will use "balls" to mean realized balls.*

We will visualize the closed balls as trees:

Lemma 3.43. *Let T be the set of closed balls (in valuation notation, i.e. realized) ordered under $\subseteq$. Then T is a (downward) tree; i.e. for $B \in T$ we have $\{ B' \in T : B \subseteq B' \}$ is linearly ordered by $\subseteq$.*

Proof. Suppose $B \subseteq B_1$ and $B \subseteq B_2$. Suppose $c \in B$. Then by the homework we have that c is a center of B_1 and B_2; so

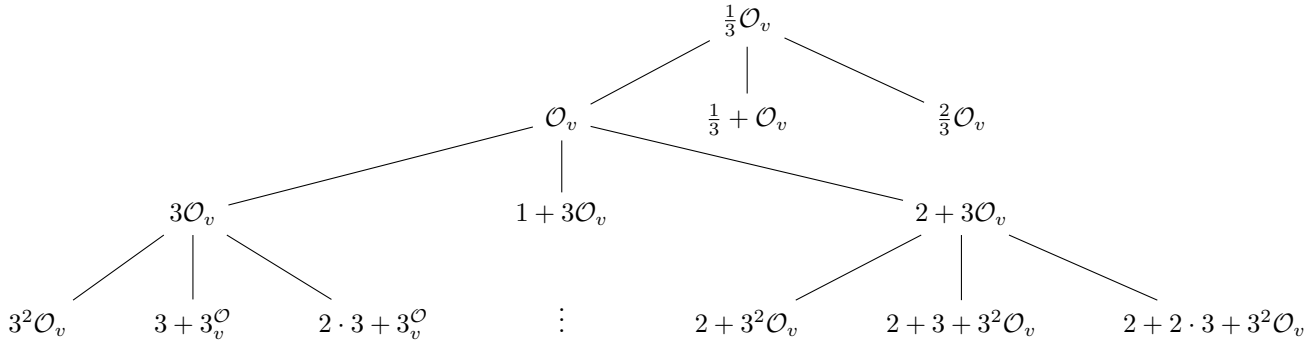
$$B_1 = \overline{B}_{\gamma_1}(c)$$
$$B_2 = \overline{B}_{\gamma_2}(c)$$

for some $\gamma_1, \gamma_2 \in v(K^\times)$. Hence $B_1 \subseteq B_2$ if and only if $\gamma_2 \leq \gamma_1$; since the value grape is totally ordered, we get that $B_1 \subseteq B_2$ or $B_2 \subseteq B_1$. (Recall that

$$\overline{B}_\gamma(c) = \{ x \in K : v(x - c) \geq \gamma \}$$

for $c \in K$ and $\gamma \in v(K^\times)$.) □ Lemma 3.43

Example 3.44. Let $K = \mathbb{Q}$ with $v = v_3$ the 3-adic valuation.



(Note that $3\mathcal{O}_v = \overline{B}_{v=1}(0)$.) In particular for

$$\alpha = \sum_{i=m}^{\infty} a_i 3^i \in \mathbb{Q}_3$$

we have that α is in every closed ball of the form

$$\sum_{i=m}^{m+n-1} a_i 3^i + 3^{m+n}\mathcal{O}_v$$

Furthermore, these balls form a path through the tree; hence we can regard elements of $\mathbb{Q}_3$ as paths through the tree.

3.2 Hensel's lemma

Consider $k[[t]]$ for k a field; suppose

$$f = \sum_{i=0}^{\infty} a_i t^i \in k[[t]]$$

for $a_i \in k$. To find an inverse for f we solve $fX - 1 = 0$; i.e.

$$1 = \left(\sum_{i=0}^{\infty} a_i t^i\right)\left(\sum_{i=0}^{\infty} b_i t^i\right) = a_0 b_0 + (a_0 b_1 + a_1 b_0) + \cdots$$

We need $b_0 \in k$ to be a solution to $a_0 X - 1 = 0$; this is in fact sufficient. Another way to view this is that we simply applied the residue map $k[[t]] \to k$ to the equation $fX - 1 = 0$, and we got a condition for a solution. This is generalized as follows:

Lemma 3.45 (Hensel's lemma)**.** *Suppose (K, v) is a classical complete valued field; suppose $P(x) \in \mathcal{O}_v[x]$. Let $\overline{P}(x) \in \overline{K}_v[x]$ be obtained by applying* res *to each coefficient of P. (Here* res*: $\mathcal{O}_V \to \overline{K}_v = \mathcal{O}_v/\mathcal{M}_v$ is the quotient map $a \mapsto \overline{a}$.) Suppose $\alpha \in \overline{K}_v$ is a solution to $\overline{P}(x) = 0$ such that $\overline{P}'(\alpha) \neq 0$ (where $\overline{P}'$ is the formal derivative of P). Then there is $a \in \mathcal{O}_v$ such that $P(a) = 0$ and $\mathrm{res}(a) = \alpha$.*

Remark 3.46. If we start with any $b \in \mathcal{O}_v$ with $\alpha = \mathrm{res}(b)$ a solution to $\overline{P}(x) = 0$, then since $\mathrm{res}(a) = \mathrm{res}(b)$, we get $a - b \in \mathcal{M}_v = B_{v(1)}(0)$; i.e. a is close to b.

Hensel's lemma is a consequence of:

Lemma 3.47 (Hensel-Rychik (1.3.1))**.** *Suppose (K, v) is a complete classical valued field; suppose $P(x) \in \mathcal{O}_v[x]$ and $a_0 \in \mathcal{O}_v$ satisfy $v(P(u_0)) > 2v(P'(a_0))$. Then there is $a \in \mathcal{O}_v$ such that $P(a) = 0$ and $v(a - a_0) > v(P'(a_0))$.*

Fact 3.48. *Suppose R is a ring, $P \in R[z]$ is a polynomial, and w is another indeterminate. Then $P(z + w)$ can be written in the form $P(z) + P'(z)w + P_2(z)w^2 + \cdots + P_m(z)w^m$ where $P_2, \ldots, P_m \in R[z]$*

Proof of Lemma 3.47. We may assume $P(a_0) \neq 0$. Let $\varepsilon = v(P(a_0)) - 2v(P'(a_0)) > 0$. (So $\varepsilon \in \mathbb{R}$.) Define recursively $(a_n : n < \omega)$ by $a_{n+1} = a_n - \frac{P(a_n)}{P'(a_n)}$; we will show that $(a_n : n \geq 0)$ is Cauchy and converges to a root of P in $\mathcal{O}_v$.

For $n \in \mathbb{N}$ let

$$b_n = P'(a_n)$$
$$c_n = \frac{P(a_n)}{P'(a_n)^2}$$

so $a_{n+1} = a_n - c_n b_n$.

Claim 3.49.

1. *$v(b_n) = v(b_0) = v(P'(a_0))$ for all n.*
2. *$v(c_n) \geq 2^n \varepsilon$.*

Proof. We apply induction on n.

For the case $n = 0$ (1) is immediate; for (2) we simply note that

$$v(c_0) = v\left(\frac{P(a_0}{P'(a_0)^2}\right) = v(P(a_0)) - 2v(P'(a_0)) = \varepsilon$$

Suppose the claim holds for n; we check the case $n + 1$.

1. Using Fact 3.48:

$$\begin{aligned} b_{n+1} &= P'(a_{n+1}) \\ &= P'(a_n - c_n b_n) \\ &= P'(a_n) + (-c_n b_n)d \text{ for some } d \in \mathcal{O}_v \\ &= b_n(1 - c_n d) \end{aligned}$$

Hence

$$v(b_{n+1}) = v(b_n) + \underbrace{v(1 - c_n d)}_{0} = v(b_n) = v(b_0)$$

by the induction hypothesis.

2. Again using Fact 3.48:

$$\begin{aligned} P(a_{n+1}) &= P(a_n - c_n b_n) \\ &= P(a_n) + (-c_n b_n)P'(a_n) + (-c_n b_n)^2 e \text{ for some } e \in \mathcal{O}_v \\ &= P(a_n) + \left(-\frac{P(a_n)}{P'(a_n)^2}P'(a_n)\right)P'(a_n) + c_n^2 b_n^2 e \\ &= c_n^2 b_n^2 e \end{aligned}$$

Hence $v(P(a_{n+1})) = 2v(c_n) + 2v(b_n) + v(e)$. So

$$\begin{aligned} v(c_{n+1}) &= v\left(\frac{P(a_{n+1})}{P'(a_{n+1})^2}\right) \\ &= v(P(a_{n+1})) - 2v(P'(a_{n+1})) \\ &= 2v(c_n) + 2v(b_n) + v(e) - 2v(b_{n+1}) \\ &\geq 2v(c_n) \\ &\geq 2^{n+1}\varepsilon \end{aligned}$$

by the induction hypothesis. □ Claim 3.49

But now

$$v(a_{n+1} - a_n) = v(c_n b_n) = v(c_n) + v(b_n) \geq 2^n \varepsilon + v(b_0) \to \infty$$

as $n \to \infty$; so $(a_n : n \geq 0)$ is Cauchy. Since K is complete, we may thus take

$$a = \lim_{n\to\infty} a_n \in K$$

Then $a \in \mathcal{O}_v$ since $\mathcal{O}_v$ is closed in K.

Exercise 3.50. polynomials are continuous in the topology on K induced by v.

Then

$$\begin{aligned} P(a) &= \lim_{n\to\infty} P(a_n) \\ v(P(a)) &= \lim_{n\to\infty} v(P(a_n)) \end{aligned}$$

But

$$\begin{aligned} v(P(a_n)) &= v(c_n b_n^2) \\ &= v(c_n) + 2v(b_n) \\ &\geq 2^n \varepsilon + 2(b_0) \\ &\to \infty \end{aligned}$$

So $v(P(a)) = \infty$, and $P(a) = 0$.

Finally, note that

$$v(a - a_0) = v((a - a_n) + (a_n - a_0)) \geq \min\{\underbrace{v(a - a_n)}_{\infty}, v(a_n - a_0)\}$$

for any n. But

$$\begin{aligned} v(a_n - a_0) &= v((a_n - a_{n-1}) + (a_{n-1} - a_{n-2}) + \cdots + (a_1 - a_0)) \\ &\geq \min_{0\leq i<n} v(a_{i+1} - a_i) \\ &= \min_{0\leq i<n} v(c_i b_i) \\ &\geq \min_{0\leq i<n} (2^i \varepsilon + v(b_0)) \\ &= v(b_0) + \varepsilon \end{aligned}$$

As $n \to \infty$ we get $v(a - a_0) \geq v(b_0) = v(P'(a_0))$. □ Lemma 3.47

We can now prove Hensel's lemma:

Proof of Lemma 3.45. Pick $a_0 \in \mathcal{O}_v$ with $\overline{a_0} = \alpha$. Then

$$\overline{P(a_0)} = \overline{P}(\overline{a_0}) = \overline{P}(\alpha) = 0$$

Hence $P(a_0) \in \mathcal{M}_v$, and $v(P(a_0)) > 0$. So

$$\overline{P'(a_0)} = \overline{P'}(\overline{a_0}) = \overline{P}'(\overline{a_0}) = \overline{[}'(\alpha) \neq 0$$

Hence $P'(a_0) \notin \mathcal{M}_v$ and $v(P'(a)) = 0$. So $v(P(a_0)) > 2v(P'(a_0))$. By Hensel-Rychik, there is $a \in \mathcal{O}_v$ with $P(a) = 0$ and $v(a - a_0) > v(P'(a_0)) = 0$; so $a - a_0 \in \mathcal{M}_v$, and $\overline{a} = \overline{a_0} = \alpha$. □ Lemma 3.45

4 Krull valuations

Definition 4.1. A *valuation ring* is an integral domain R such that for every $x \in \mathrm{Frac}(R)$ one of x and x^{-1} lies in R.

Given a valuation ring R with $K = \mathrm{Frac}(R)$, we'd like to find a valuation on K of which R is the valuation ring. If (L, v) is a classical, then $v\colon L^\times \to \mathbb{R}$; hence $v(L^\times) \cong L^\times/\mathcal{O}_v^\times$ (where $\mathcal{O}_v^*$ is the units of $\mathcal{O}_v$). Analogously, we may consider $\Gamma = K^\times/R^\times$ as a multiplicative grape. We get a quotient map $v\colon K \to \Gamma \cup \{\infty\}$ given by

$$x \mapsto \begin{cases} \infty & \text{if } x = 0 \\ aR^* & \text{if } a \in K^* \end{cases}$$

Axioms (1) and (2) are satisfied by this construction; to make sense of axiom (3), we need an ordering on Γ.

Definition 4.2. For $a, b \in K^\times$, we set $aR^\times \leq bR^\times$ if and only if $\frac{b}{a} \in R$.

Proposition 4.3. *$\leq$ is well-defined on Γ and makes Γ into an ordered abelian grape; i.e. $\leq$ is a linear order and whenever $\delta, \gamma, \lambda \in \Gamma$ satisfy $\gamma \leq \lambda$ we have $\delta\gamma \leq \delta\lambda$.*

Proof.

(Well-defined) Immediate.

(Reflexive) Suppose $a \in K^\times$. Then $\frac{a}{a} = 1 \in R$, so $aR^\times \leq aR^\times$.

(Tranitive) Suppose $aR^\times \leq bR^\times$ and $bR^\times \leq cR^\times$. So $\frac{b}{a} \in R$ and $\frac{c}{b} \in R$; hence $\frac{b}{a}\frac{c}{b} = \frac{c}{a} \in R$, so $aR^\times \leq cR^\times$.

(Antisymmetry) Suppose $aR^\times \leq bR^\times$ and $bR^\times \leq aR^\times$. Then $\frac{a}{b} \in R$ and $\frac{b}{a} \in R$; so $\frac{a}{b} \in R^\times$, and $aR^\times = bR^\times$.

(Totality) Suppose $a, b \in K^\times$. Since R is a valuation ring, we have either $\frac{a}{b} \in R$ or $\frac{b}{a} \in R$; hence $bR^\times \leq aR^\times$ or $aR^\times \leq bR^\times$.

(Grape ordering) Suppose $aR^\times \leq bR^\times$ and $c \in K^\times$. So $\frac{b}{a} \in R$, and $\frac{cb}{ca} \in R$. So $caR^\times \leq cbR^\times$, and $(cR^\times)(aR^\times) \leq (cR^\times)(bR^\times)$. □ Proposition 4.3

Proposition 4.4. *If $x, y \in K^\times$ then $v(x + y) \geq \min(v(x), v(y))$.*

Proof. Without loss of generality we may assume that $v(y) \leq v(x)$; so $\frac{x}{y} \in R$, and $\min(v(x), v(y)) = v(y)$. But $\frac{x+y}{y} = \frac{x}{y} + 1 \in R$; so $v(y) \leq v(x + y)$, as desired. □ Proposition 4.4

Remark 4.5. $R = \{x \in K : v(x) \geq 0\}$ since $v(x) \geq 0$ if and only if $xR^\times \geq 1R^\times$; i.e. if $\frac{x}{1} \in R$. (Here "0" refers to the identity of $\Gamma = K^\times/R^\times$, which is $1R^\times$.)

Definition 4.6. A *valued field* is a triple (K, v, Γ) where K is a field, $(\Gamma, +, 0)$ is an ordered abelian grape, and $v\colon K \to \Gamma \cup \{\infty\}$ is a surjective map satisfying the following:

1. $v(x) = \infty$ if and only if $x = 0$.
2. $v\colon K^\times \to \Gamma$ is a grape homomorphism.
3. $v(x+y) \geq \min(v(x), v(y))$.

We call Γ the *value grape* of (K, v, Γ). We define the *valuation ring* of (K, v, Γ) to be $\mathcal{O}_v = \{\, x \in K : v(x) \geq 0 \,\}$, and the *maximal ideal* of $\mathcal{O}_v$ to be $\mathcal{M}_v = \{\, x \in K : v(x) > 0 \,\}$. We further define the *residue field* of (K, v, Γ), with res or $\bar{\cdot}$ the quotient map $\mathcal{O}_v \to \overline{K}_v$.

This generalized classical valued fields simply by allowing arbitrary ordered abelian grapes as the value grapes.

Remark 4.7. Just as in the classical case, the axioms imply:

1. $\mathcal{O}_v$ is a valuation ring.
2. $\mathcal{O}_v$ is a local ring with maximal ideal $\mathcal{M}_v$.

We have shown:

Proposition 4.8. *Every valuation ring is the valuation ring of a valued field.*

In fact, we have seen that the valued field structure (K, v, Γ) can be reconstructed from $\mathcal{O}_v$ by ring theory:

$$\begin{aligned} K &= \mathrm{Frac}(\mathcal{O}_v) \\ (\Gamma, +, 0) &\cong (K^\times/\mathcal{O}_v^\times, \cdot, 1) \\ a\mathcal{O}_v^\times \leq b\mathcal{O}_v^\times &\iff \frac{b}{a} \in \mathcal{O}_v \\ v(r) &= r\mathcal{O}_v^\times \end{aligned}$$

For the penultimate, note that

$$\begin{aligned} a\mathcal{O}_v^\times \leq b\mathcal{O}_v^\times &\iff v(a) \leq v(b) \\ &\iff v\Big(\frac{a}{b}\Big) \geq 0 \\ &\iff \frac{b}{a} \in \mathcal{O}_v \end{aligned}$$

Corollary 4.9. *Suppose (K, v, Γ) and (F, w, Δ) are valued fields. Then the following are equivalent:*

1. *$(K, v, \Gamma) \cong (F, w, \Delta)$; i.e. there is a pair (α, ρ) where $\alpha\colon K \to F$ is an isomorphism of fields, $\rho\colon \Gamma \to \Delta$ is an isomorphism of ordered abelian groups, and the following diagram commutes:*

$$\begin{array}{ccc} K & \xrightarrow{\quad\alpha\quad} & F \\ \big\downarrow{\scriptstyle v} & & \big\downarrow{\scriptstyle w} \\ \Gamma \cup \{\infty\} & \xrightarrow{\quad\rho\quad} & \Delta \cup \{\infty\} \end{array}$$

2. *$\mathcal{O}_v \cong \mathcal{O}_w$ as rings.*

The details of the proof are an exercise; it is a manifestation of the previous remark.

Definition 4.10. Suppose v, w are valuations on K. We say v and w are *equivalent* if $\mathcal{O}_v = \mathcal{O}_w$. (True equality, not just isomorphism.)

Exercise 4.11. (K, v, Γ) and (K, w, Δ) are equivalent if and only if there is an isomorphism of ordered abelian grapes $\Gamma \to \Delta$ such that (id_K, ρ) is an isomorphism $(K, v, \Gamma) \to (K, w, \Delta)$.

Fact 4.12 (2.1.1-ish)**.** *Suppose (K, v, Γ) is a valued field. Then the following are equivalent:*

1. *v is equivalent to a classical valuation on K.*
2. *There is an embedding of ordered abelian grapes $(\Gamma, +, 0, \leq) \hookrightarrow (\mathbb{R}, +, 0, \leq)$.*
3. *For any $\beta \in \Gamma$ with $\beta > 0$ and any $\alpha \in \Gamma$ there is $n \in \mathbb{N}$ such that $\alpha \leq n\beta$.*
4. *Γ is a rank 1 ordered abelian grape, where the* rank *of an ordered abelian grape is the number of proper convex subgrapes, where a* convex *subgrape $\Delta \leq \Gamma$ is one where if $\alpha, \beta \in \Delta$ and $\gamma \in \Gamma$ with $\alpha \leq \gamma \leq \beta$ the $\gamma \in \Delta$.*

What about on $\mathbb{Q}$?

Proposition 4.13. *Up to equivalence, the only non-trivial valuations on $\mathbb{Q}$ are the p-adics ones. (We say v on K is* trivial *if $v(K^\times) = 0$; i.e. if $\Gamma = 0$, i.e. if $\mathcal{O}_v = K$.)*

Proof. Since equivalence means having the same valuation ring, it suffices to show that the only proper valuation rings that are subrings of $\mathbb{Q}$ are $\mathbb{Z}_{(p)}$ for p prime.

Suppose $R \subsetneqq \mathbb{Q}$ is a valuation ring. Let M be the maximal ideal of R. Now, $\mathbb{Z} \subseteq R$, so we may consider $M \cap \mathbb{Z}$ an ideal of $\mathbb{Z}$. This is a proper ideal since $1 \notin M$; it is non-trivial since otherwise every element of $\mathbb{Z} \setminus \{0\}$ is a unit of R, contradicting our assumption that $R \neq \mathbb{Q}$. So $M \cap \mathbb{Z}$ is a non-trivial prime ideal of $\mathbb{Z}$ So $M \cap \mathbb{Z} = p\mathbb{Z}$ for some prime p.

Hence if $n \in \mathbb{Z}$ is non-zero and $p \nmid n$, then $n \notin M$, so n is a unit of R. So $\frac{1}{n} \in R$; i.e. $\mathbb{Z} \subseteq \mathbb{Z}_{(p)} \subseteq R \subsetneqq \mathbb{Q}$.

Conversely, suppose $\frac{a}{b} \in R$ with $\gcd(a, b) = 1$. If $p \mid b$, then $\nmid a$; so $\frac{1}{a} \in \mathbb{Z}_{(p)} \subseteq R$. Hence $\frac{1}{a}\frac{a}{b} = \frac{1}{b} \in R$. But $p \mid b$, so $b \in p\mathbb{Z} = M \cap \mathbb{Z}$, and $b \in M$, a contradiction. So $p \nmid b$, and $\frac{a}{b} \in \mathbb{Z}_{(p)}$.

Hence $R = \mathbb{Z}_{(p)}$. □ Proposition 4.13

In particular all valuations on $\mathbb{Q}$ are classical.

What of $K(x)$, where K is a field?

Example 4.14. Fix $P \in K[x]$ irreducible. We define the *P-adic valuation* on $K(x)$ as follows: given $f \in K(x)$ write $f = P^n \frac{Q}{R}$ where $Q, R \in K[x]$ and $n \in \mathbb{Z}$ with $P \nmid Q$ and $P \nmid R$; then set $v_P(f) = n$. One checks that v_P is a classical valuation on $K(x)$ with the property that $v_P \restriction K$ is trivial. Note that $\mathcal{O}_{v_P} = K[x]_{(P)}$.

Example 4.15. Define v_∞ on $K(x)$ by $v_\infty\left(\frac{f}{g}\right) = \deg(g) - \deg(f)$ for $f, g \in K[x]$. Then v_∞ is a classical valuation on $K(x)$ with $v_\infty \restriction K$ trivial.

Remark 4.16. If we let $t = \frac{1}{x}$ then v_∞ on $K(x)$ transforms into v_t on $K(t)$. So v_∞ is the "order of vanishing at the point at ∞".

Proposition 4.17. *Suppose K is a field. The only non-trivial valuations on $K(x)$ which are trivial on K are v_P for $P \in K[x]$ irreducible or v_∞.*

In particular, they are all classical.

Proof. Let $R = \mathcal{O}_v \subsetneqq K(x)$. Since $v \restriction K$ is trivial, we get that $K \subseteq R$.

Case 1. Suppose $v(x) \geq 0$ The $K[x] \subseteq R \subsetneqq K(x)$. As before we get that $M \cap K[x] = PK(x)$ for some irreducible $P \in K[x]$. So $K[x]_{(P)} \subseteq R$. Conversely suppose $\frac{f}{g} \in R$ with $\gcd(f, g) \in K$. If $p \mid g$ then $p \nmid f$, so $f \notin M$; hence $\frac{1}{f}\frac{f}{g} = \frac{1}{g} \in R$, a contradiction, since $p \mid g$ implies $g \in M$. So $p \nmid g$. So $\frac{f}{g} \in K[x]_{(P)}$ So $R = K[x]_{(P)}$; so v is equivalent to v_P.

Case 2. Suppose $v(x) < 0$. Suppose $f \in K[x]$ and $f \neq 0$. Write

$$f = a_n x^n + a_{n-1} x n - 1 + \cdots + a_0$$

with $a_n \neq 0$ and $a_0, \ldots, a_n \in K$. Then for $0 \leq i \leq n$ we have

$$v(a_i x^i) = v(a_i) + iv(x) = \begin{cases} \infty & \text{if } a_i = 0 \\ iv(x) & \text{if } a_i \neq 0 \end{cases}$$

We get that

$$v(f) = \min_{\substack{a_i \neq 0 \\ 0 \leq i \leq n}} iv(x) = nv(x) = \deg(f)v(x)$$

So for $\frac{f}{g} \in K(x)$ we have

$$v\left(\frac{f}{g}\right) = v(f) - v(g) = \deg(f)v(x) - \deg(g)v(x) = (\deg(f) - \deg(g))v(x)$$

Hence $\frac{f}{g} \in R$ if and only if $\deg(g) \geq \deg(f)$ (since $v(x) < 0$). Hence v is equivalent to v_∞. □ Proposition 4.17

Aside 4.18. Suppose M is a complex manifold. Suppose $V \subseteq M$ is a $\mathbb{C}$-analytic subset of dimension $n-1$. (i.e. for every $p \in M$ there is a neighborhood $U \ni p$ such that $V \cap U$ is the set of zeroes of some holomorphic $f : U \to \mathbb{C}$.)

Then if g is holomorphic, defined at p, and vanishes on V then $f \mid g$. We may write $g = f^n h$ for some n with $f \nmid h$.

Fact 4.19. *If V is irreducible then n does not depend on p.*

We write $n = \operatorname{ord}_V(g)$.

If $\alpha = \frac{g}{h}$ (locally) is a meromorphic function on M then $\operatorname{ord}_V(\alpha) = \operatorname{ord}_V(g) - \operatorname{ord}_V(h)$. In fact ord_V is a valuation on $\operatorname{Mer}(M)$. (If $M = \mathbb{P}^1(\mathbb{C})$ then $\operatorname{Mer}(M) = \mathbb{C}(x)$.)

Suppose (K, v, Γ) is a valued field and $L \supseteq K$ is a field extension. Can we extend v to L? If so, how many ays? Are there any canonical extensions?

Perhaps (K, v, Γ) is classical, but we should ask about arbitrary (possibly non-classical) extensions to L.

We consider the case $L = K(x)$.

Theorem 4.20 (2.2.1)**.** *Suppose (K, v, Γ) is a valued field. Let $\Gamma' \geq \Gamma$ be an ordered abelian grape extending $(\Gamma, 0, +, \leq)$. Let $\gamma \in \Gamma'$. Then there is an extension of v to $K(x)$ such that $v(x) = \gamma$. The value grape of $(K(x), v)$ is then $\langle \Gamma, \gamma \rangle$, the subgrape of Γ' generated by Γ and γ.*

Proof. First we extend v from K to $K[x]$. Suppose $f \in K[x]$ is non-zero; write $f = a_n x^n + \cdots + a_1 x + a_0$. We then set

$$v(f) = \min_{0 \leq i \leq n} (v(a_i) + i\gamma)$$

Claim 4.21. *Suppose $f, g \in K[x] \setminus \{0\}$. Then $v(f+g) \geq \min(v(f), v(g))$.*

Proof. Write

$$f = \sum_{i=0}^{n} a_i x^i$$
$$g = \sum_{i=0}^{n} b_i x^i$$

Then

$$f + g = \sum_{i=0}^{n} (a_i + b_i) x^i$$

so

$$\begin{aligned} v(f+g) &= \min_{0 \leq i \leq n} (v(a_i + b_i) + i\gamma) \\ &\geq \min_{0 \leq i \leq n} (\min(v(a_i) + i\gamma, v(b_i) + i\gamma)) \\ &\geq \min\left(\min_{0 \leq i \leq n} (v(a_i) + i\gamma), \min_{0 \leq i \leq n} (v(b_i) + i\gamma) \right) \\ &= \min(v(f), v(g)) \end{aligned}$$

as desired. □ Claim 4.21

Claim 4.22. $v(fg) = v(f) + v(g)$.

Proof. As before write

$$f = \sum_{i=0}^{n} a_i x^i$$
$$g = \sum_{i=0}^{n} b_i x^i$$

Then

$$fg = \sum_{k=0}^{2n} \underbrace{\left(\sum_{i+j=k} a_i b_j \right)}_{c_k} x^k$$

Let i_0 be least such that $v(f) = v(a_{i_0}) + i_0\gamma$; let j_0 be least such that $v(g) = v(b_{j_0}) + j_0\gamma$. Let $k = i_0 + j_0$; consider the term of degree k_0 in fg; i.e. $c_{k_0}x^{k_0}$.

Subclaim 4.23. $v(c_{k_0}x^{k_0}) = v(f) + v(g)$.

Proof. Well,

$$\begin{aligned} v(c_{k_0}x^{k_0}) &= v\left(\sum_{i+j=k_0} a_i b_i \right) + k_0\gamma \\ &= v\left(\underbrace{\left(\sum_{\substack{i+j=k_0 \\ i<i_0}} a_i b_i \right)}_{A} + a_{i_0}b_{j_0} + \underbrace{\left(\sum_{\substack{i+j=k_0 \\ i>i_0}} a_i b_j \right)}_{B} \right) + k_0\gamma \end{aligned}$$

For A, we have $v(a_i) + i\gamma > v(f)$ (since $i < i_0$) and $v(b_j) + j\gamma \geq v(g)$. Hence

$$\begin{aligned} v(a_i) + v(b_j) &> v(f) + v(g) - k_0\gamma \\ &= v(a_{i_)}) + i_0\gamma + v(b_{j_0}) + j_0\gamma - k_0\gamma \\ &= v(a_{i_0}) + v(b_{i_0}) \end{aligned}$$

Hence $v(a_ib_j) > v(a_{i_0}b_{j_0})$.

Similarly for B we find $v(a_ib_i) > v(a_{i_0}b_{j_0})$. Hence $v(A) > v(a_{i_0}b_{j_0})$ and $v(B) > v(a_{i_0}b_{j_0})$; so

$$v\left(\sum_{i+j=k_0} a_i b_j \right) = v(a_{i_0}b_{j_0})$$

Hence

$$v(c_{k_0}x^{k_0}) = v(a_{j_0}) + v(b_{j_0}) + i_0\gamma + j_0\gamma = v(f) + v(g)$$

as desired. □ Subclaim 4.23

Hence $v(fg) \leq v(f) + v(g)$. Conversely,

$$\begin{aligned} v(fg) &= \min_{0\leq k\leq 2n} (v(c_k) + k\gamma) \\ &\geq \min_{0\leq k\leq 2n} \left(\left(\min_{i+j=k} (v(a_i) + v(b_j)) \right) + k\gamma \right) \\ &= \min_{0\leq k\leq 2n} \left(\min_{i+j=k} (v(a_i) + i\gamma + v(b_j) + j\gamma) \right) \\ &\geq \min_{0\leq k\leq 2n} \left(\min_{i+j=k} (v(f) + v(g)) \right) \\ &= v(f) + v(g) \end{aligned}$$

as desired. □ Claim 4.22

To be continued.

TODO 3. *From this point on the extension of v will be called w.*

We now define w on all of $K(x)$: given $\frac{f}{g} \in K(x)$ we are forced to define $w\left(\frac{f}{g}\right) = w(f) - w(g)$. One checks that the claims hold for rational functions as well. One further checks that this definition is well-defined.

Hence w is a valuation on $K(x)$ extending v and with $w(x) = \gamma$. Note that $\Gamma \leq w(K(x)^\times)$ as w extends v; note also that $\gamma \leq w(K(x)^\times)$ since $\gamma = w(x)$. Hence $\langle \Gamma, \gamma \rangle \leq w(K(x)^\times)$; that $\langle \Gamma, \gamma \rangle \geq w(K(x)^\times)$ is clear from the construction. □ Theorem 4.20

Remark 4.24. We do not claim that this extension is unique (even when Γ' and γ are fixed). But the proof yields a canonical extension.

This gives us non-classical valuations:

Example 4.25. Consider $(\mathbb{Z} \oplus \mathbb{Z}, 0, +, \leq_{\text{lex}})$. We view $\mathbb{Z} \hookrightarrow \mathbb{Z} \oplus \mathbb{Z}$ via $a \mapsto (0, a)$. Since $\mathbb{Z}$ is a proper convex non-trivial subgrape of $\mathbb{Z} \times \mathbb{Z}$, this ordered abelian grape cannot be embedded in $(\mathbb{R}, 0, +, \leq)$. Extend v_p from $\mathbb{Q}$ to $\mathbb{Q}(x)$ by $w(x) = (1, 0)$, using the above theorem; then $\Gamma_w = \langle \mathbb{Z}, (1, 0) \rangle = \mathbb{Z} \oplus \mathbb{Z}$. Hence $(\mathbb{Q}(x), w, \mathbb{Z} \oplus \mathbb{Z})$ is a non-classical valuation extending v_p.

Definition 4.26. Given (K, v, Γ), the *Gauss extension* of v to $K(x)$ is the valuation w such that

$$w\left(\sum_{i=0}^{n} a_i x^i\right) = \min_{0 \leq i \leq n} v(a_i)$$

This is a special cae of (the proof of) the previous theorem, where $\Gamma' = \Gamma$ and $\gamma = 0$.

Theorem 4.27 (2.2.2)**.** *Let w be the Gauss extension of (K, v, Γ) to $K(x)$. Then*

1. $\Gamma_w = \Gamma_v$.
2. $\overline{K(x)}_w = \overline{K}_v(\overline{x})$ *and* $\overline{x} = \text{res}_w(x)$ *is transcendental over* $\overline{K}_v$.
3. *w is the unique extension of v with $w(x) = 0$ and $\overline{x}$ transcendental over $\overline{K}_v$.*

Proof.

1. Part of 2.2.1.
2. First note that $\mathcal{O}_v \vee \mathcal{O}_w$ and $\mathcal{M}_v = \mathcal{M}_w \cap \mathcal{O}_v$ since $w \restriction K(x) = v$. Hence we get a natural inclusion $\mathcal{O}_v/\mathcal{M}_v \hookrightarrow \mathcal{O}_w/\mathcal{M}_w$; we thus view $\overline{K}_v \subseteq \overline{K(x)}_w$.

   Claim 4.28. *$\overline{x}$ is transcendental over $\overline{K}_v$.*

   Proof. Suppose
   $$\sum_{i=0}^{n} \alpha_i \overline{x}^i$$
   for $\alpha_i \in \overline{K}_v$; say $\alpha_i = \overline{a_i}$ for $a_i \in \mathcal{O}_v$. Then
   $$\overline{\sum_{i=0}^{n} a_i x^i} = \sum_{i=0}^{n} \overline{a_i} \cdot \overline{x}^i = 0$$
   Hence
   $$0 < w\left(\sum_{i=0}^{n} a_i x^i\right) = \min_{0 \leq i \leq n} v(a_i)$$
   Hence $v(a_i) > 0$ for all i, and hence each $a_i \in \mathcal{M}_v$. So $\alpha_i = \overline{a_i} = 0$. □ Claim 4.28

Claim 4.29. $\overline{K(x)}_w = \overline{K}_v(\overline{x})$.

Proof.

($\supseteq$) Clear.

($\subseteq$) A wrong proof:

$$\overline{\left(\frac{\sum a_i x^i}{\sum b_i x^i}\right)} = \frac{\sum \overline{a_i}\overline{x}^i}{\sum \overline{b_i}\overline{x}^i} \in \overline{K}_v(\overline{x})$$

The problem is that $\bar{\cdot} = \mathrm{res}_v \colon \mathcal{O}_v \to \overline{K}_v$, and the a_i and b_i need not be in $\mathcal{O}_v$.
We now begin a proper proof.

Subclaim 4.30. *If $f \in K[x]$ with $f \neq 0$ then we can write $f = cg$ where $c \in K^\times$, $g \in \mathcal{O}_v[x]$, and $w(g) = 0$ (i.e. $g \in \mathcal{O}_w^\times$).*

Proof. Write

$$f = \sum_{i=0}^{n} a_i x^i$$

so

$$w(f) = \min_{0 \le i \le n} v(a_i) = v(a_k)$$

for some $0 \le k \le n$. Let $c = a_k \neq 0$ (since $f \neq 0$); then

$$f = c \underbrace{\sum_{i=0}^{n} \frac{a_i}{a_k} x^i}_{g}$$

Then

$$v\left(\frac{a_i}{a_k}\right) = v(a_i) - v(a_k) \ge 0$$

for all i by choice of a_k. Hence $\frac{a_i}{a_k} \in \mathcal{O}_v$, and $g \in \mathcal{O}_v[x]$. Furthermore, the coefficient of x^k in g is 1, and $v(1) = 0$. So

$$w(g) = \min_{0 \le i \le n} v\left(\frac{a_i}{a_k}\right) = 0$$

as desired. □ Subclaim 4.30

Now, suppose $h \in \mathcal{O}_w$ is non-zero; say $h = \frac{f_1}{f_2}$ for non-zero f and g. By the subclaim we have

$$\underbrace{h}_{\in \mathcal{O}_w} = \underbrace{\frac{c_1}{c_2}}_{\in K} \underbrace{\frac{g_1}{g_2}}_{\in \mathcal{O}_w^\times}$$

(since each $g_i \in \mathcal{O}_w^\times$) where $f_i = c_i g_i$ as in the subclaim. Hence $\frac{c_1}{c_2} = \frac{g_2}{g_1} h \in \mathcal{O}_w \cap K \subseteq \mathcal{O}_v$. Applying residue, we find

$$\mathrm{res}_w(h) = \mathrm{res}_w\left(\frac{c_1}{c_2}\frac{g_1}{g_2}\right) = \underbrace{\mathrm{res}_v\left(\frac{c_1}{c_2}\right)}_{\in \overline{K}_v} \frac{\mathrm{res}_w(g_1)}{\mathrm{res}_w(g_2)}$$

Since $g_i \in \mathcal{O}_v[x]$ we have $\mathrm{res}_w(g_i) \in \overline{K}_v[\overline{x}]$. Hence $\mathrm{res}_w(h) \in \overline{K}_v(\overline{x})$; so $\overline{K(x)}_w \subseteq \overline{K}_v(\overline{x})$, as desired.

□ Claim 4.29

3. Suppose u extends v to $K(x)$ with $v(x) = 0$ and $\mathrm{res}_u(x)$ transcendental over $\overline{K}_v$. Suppose $f \in K[x]$ is non-zero. We will show $u(f) = w(f)$, which will suffice to prove the result.

   By subclaim, we may write $f = cg$ for some $c \in K^\times$ and $g \in \mathcal{O}_v[x]$ with $w(g) = 0$.

   Claim 4.31. $u(g) = 0$.

   Proof. Well,
   $$v(g) \geq \min_i u(b_i x^i) = \min_i (u(b_i) + iu(x)) = \min_i v(b_i) \geq 0$$
   where $g = \sum_i b_i x^i$ for $b_i \in \mathcal{O}_v$. Hence $g \in \mathcal{O}_u$. Applying res_u, we find
   $$\mathrm{res}_u(g) = \sum_i \mathrm{res}_v(b_i)\,\mathrm{res}_u(x)^i \neq 0$$
   Not all $\mathrm{res}_v(b_i) = 0$ since else $\mathrm{res}_w(g) = 0$, a contradiction. Hence $g \in \mathcal{O}_v^\times$; i.e. $u(g) = 0$. □ Claim 4.31

   So $w(g) = v(g) = 0$. So
   $$u(f) = u(cg) = u(c) + u(g) = u(c) = v(c)$$
   But
   $$w(f) = w(cg) = w(c) + w(g) = w(c) = v(c)$$
   as desired. □ Theorem 4.27

We now consider an opposite extreme: where the residue field remains unchanged but the grape grows maximally.

Theorem 4.32 (2.2.3)**.** *Suppose (K, v, Γ) is a valued field; suppose $\Gamma' \geq \Gamma$ is an extension of ordered abelian grapes. Suppose $\gamma \in \Gamma' \setminus \Gamma$ with $\Gamma \cap \langle\gamma\rangle = 0$. Then there is a unique valuation w on $K(x)$ extending v with $w(x) = \gamma$. Moreover,*
$$\overline{K(x)}_w = \overline{K}_v$$
$$\Gamma_w = \Gamma \oplus \langle\gamma\rangle$$

For example, we might consider
$$\Gamma = \mathbb{Z}$$
$$\Gamma' = (\mathbb{Z} \oplus \mathbb{Z}, \leq_{\mathrm{lex}})$$
$$\gamma = (1, 0)$$

Proof. By 2.2.1 there is a valuation w on $K(x)$ with $w(x) = \gamma$; we also get that
$$\Gamma_w = \langle\Gamma, \gamma\rangle = \Gamma + \langle\gamma\rangle = \Gamma \oplus \langle\gamma\rangle$$

For the residue field, we need some claims.

Claim 4.33. *Suppose $f \in K[x] \setminus \{0\}$. Then $f = ax^n(1 + \alpha)$ where $a \in K^\times$, $n \in \mathbb{N}$, and $\alpha \in K(x)$ with $\alpha \in \mathcal{M}_w$.*

Proof. Suppose
$$f = \sum_{i=0}^{m} a_i x^i$$
Let i_0 be such that $w(a_{i_0} x^{i_0}) = v(a_{i_0}) + i_0\gamma$ is minimal among $w(a_i x^i)$ for $i \in \{0, \ldots, m\}$. Note that if $w(a_i x^i) = w(a_{i_0} x^{i_0})$ then $v(a_i) + i\gamma = v(a_{i_0}) + i_0\gamma$; so $(i - i_0)\gamma = v(a_{i_0}) - v(a_i) \in \Gamma$, and $i = i_0$. (Since

ordered abelian grapes are torsion-free.) So all terms in f must have distinct w-values. So $w(f) = w(a_{i_0}x^{i_0}) = v(a_{i_0}) + i_0\gamma$. Now, write

$$f = a_{i_0}x^{i_0}\left(1 + \underbrace{\sum_{i\neq i_0}\frac{a_i x^i}{a_{i_0}x^{i_0}}}_{\alpha}\right)$$

so $\alpha \in K(x)$. Hence

$$w(\alpha) \geq \min_{i\neq i_0}(w(a_i x^i) - w(a_{i_0}x^{i_0})) > 0$$

so $\alpha \in \mathcal{M}_0$. □ Claim 4.33

Claim 4.34. *Suppose $f \in K(x)\setminus\{0\}$. Then $f = ax^n(1+\alpha)$ where $a \in K^\times$, $n \in \mathbb{N}$, and $\alpha \in K(x)$ with $\alpha \in \mathcal{M}_w$.*

Proof. Write $f = \frac{g_1}{g_2}$ with the $g_i \in K[x]\setminus\{0\}$. Applying the previous claim, write $g_i = a_i x^{n_i}(i+\alpha_i)$. So

$$f = \frac{a_1}{a_2}x^{n_1-n_2}\left(\frac{1+\alpha_1}{1+\alpha_2}\right) = \underbrace{\frac{a_1}{a_2}}_{a}\, x^{\overbrace{n_1-n_2}^{n}}\left(1 + \underbrace{\frac{\alpha_1-\alpha_2}{1+\alpha_2}}_{\alpha}\right)$$

and

$$w(\alpha) = \underbrace{w(\alpha_1-\alpha_2)}_{>0} - \underbrace{w(1+\alpha_2)}_{0} > 0$$

so $\alpha \in \mathcal{M}_w$. □ Claim 4.34

Now, if $f \in \mathcal{O}_w\setminus\{0\}$ write $f = ax^n(1+\alpha)$ for some $a \in K^\times$, $n \in \mathbb{Z}$, and $\alpha \in \mathcal{M}_w$. If $w(f) > 0$ then $\overline{f} = 0 \in \overline{K}_v$; assume then that $w(f) = 0$. So

$$0 = w(f) = w(a) + n\gamma + \underbrace{w(1+\alpha)}_{0}$$

So $n\gamma = -v(a) \in \Gamma$; so $n = 0$ since $\Gamma \cap \langle\gamma\rangle = 0$. So$n = 0$ and $v(a) = w(a) = 0$; so $a \in \mathcal{O}_v$. So $f = a(1+\alpha)$, and

$$\overline{f} = \overline{a}(\overline{1}+\overline{\alpha}) = \overline{a} \in \overline{K}_v$$

(since $a, 1, \alpha \in \mathcal{O}_w$). So $\overline{K(x)}_w = \overline{K}_v$.

For uniqueness, suppose w' extends v to $K(x)$ with $w'(x) = \gamma$. Let $f \in K[x]\setminus\{0\}$ be arbitrary; say $f = \sum_i a_i x^i$. On each term we have

$$w'(a_i x^i) = v(a_i) + i\gamma = w(a_i x^i)$$

Since $\Gamma \cap \langle\gamma\rangle = 0$, we know that for $i \neq j$ we have $v(a_i) + i\gamma \neq v(a_j) + j\gamma$. So

$$w'(f) = \min_i(w'(a_i x^i)) = \min_i(v(a_i) + i\gamma) = w(f)$$

and $w' = w$, as desired. □ Theorem 4.32

We now understand extensions of v to $K(x)$. What about arbitrary field extensions of L?

Definition 4.35. Suppose $K \subseteq L$ is a field extension. We say that (L, w, Γ_w) *extends* (K, v, Γ_v) if $w \restriction K$ is a valuation on K that is equivalent to v.

Remark 4.36. The restriction of a valuation is always a valuation (with a restricted value grape); the substance of the above definition lies in the equivalence to the original valuation.

Exercise 4.37. Suppose $K \subseteq L$ is a field extension. Then the following are equivalent:

1. (L, w, Γ_w) extends (K, v, Γ_v).

2. $\mathcal{O}_w \cap K = \mathcal{O}_v$.

3. There is an order-preserving embedding of ordered abelian grapes $\gamma\colon \Gamma_v \to \Gamma_w$ such that the following diagram commutes:

$$\begin{array}{ccc} K^\times & \xrightarrow{\subseteq} & L^\times \\ \downarrow{\scriptstyle v} & & \downarrow{\scriptstyle w} \\ \Gamma_v & \xrightarrow{\varphi} & \Gamma_w \end{array}$$

The point is that "equivalence" means "having the same valuation ring".

Remark 4.38. In studying extensions of v on K to $K(x)$, we used "extend" in a more restrictive way; one can check using the previous exercise that everything we said holds with the new notion of extension (where uniqueness is now only up to equivalence).

A useful lemma:

Theorem 4.39 (Chevalley's theorem)**.** *Suppose K is a field, $R \subseteq K$ is a subring, and $P \subseteq R$ is a prime ideal. Then there is a valuation subring $\mathcal{O} \subseteq K$ with $R \subseteq \mathcal{O}$ and $\mathcal{M} \cap R = P$.*

Proof. Consider the localization $R \subseteq R_P \subseteq K$; by properties of localizations we have $PR_P \cap R = P$. Now, (R_P, PR_P) is local but perhaps not a valuation subring of K: the problem is that R_P may be too small.

Let

$$\Sigma = \{\, (A, I) : R_P \subseteq A \subseteq K \text{ subrings}, I \subseteq A \text{ a proper ideal containing } PR_P \,\}$$

Then $(R_P, PR_P) \in \Sigma$. Order Σ under $\subseteq$ of both the rings and the ideal. Then Σ is closed under unions of chains; so by Zorn's lemma there is a maximal element $(\mathcal{O}, \mathcal{M}) \in \Sigma$.

Claim 4.40. *$\mathcal{O}$ is local with maximal ideal $\mathcal{M}$.*

Proof. By maximality of $(\mathcal{O}, \mathcal{M})$ in Σ, we get that $\mathcal{M}$ is a maximal ideal. Suppose there is $x \in \mathcal{O} \setminus \mathcal{M}$ that is not a unit; so $\frac{1}{x} \notin \mathcal{O}$. Then $\mathcal{O} \subsetneq \mathcal{O}\left[\frac{1}{x}\right] \subseteq K$; so by maximality we have $\left(\mathcal{O}\left[\frac{1}{x}\right], \mathcal{M}\mathcal{O}\left[\frac{1}{x}\right]\right) \notin \Sigma$; so $1 \in \mathcal{M}\mathcal{O}\left[\frac{1}{x}\right]$. So

$$1 = b_0 + b_1 x^{-1} + \cdots + b_m x^{-m}$$

where $b_i \in \mathcal{M}$. So

$$x^m = b_0 x^m + b_1 x^{m-1} + \cdots + b_m \in \mathcal{M}$$

and $x \in \mathcal{M}$, a contradiction. □ Claim 4.40

Claim 4.41. *$\mathcal{O}$ is a valuation ring.*

Proof. If not, there is $x \in K$ such that $x, x^{-1} \notin \mathcal{O}$. So $\mathcal{O} \subsetneq \mathcal{O}[x] \subseteq K$ and $\mathcal{O} \subsetneq \mathcal{O}\left[\frac{1}{x}\right] \subseteq K$; hence $1 \in \mathcal{M}\mathcal{O}[x]$ and $1 \in \mathcal{M}\mathcal{O}\left[\frac{1}{x}\right]$. So

$$1 = \sum_{i=0}^{n} a_i x^i$$
$$1 = \sum_{i=0}^{m} b_i x^{-i}$$

where $a_i, b_i \in \mathcal{M}$ and m, n are minimal. Suppose $m \leq n$. Then

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

So

$$\sum_{i=1}^{m} \underbrace{\frac{b_i}{1 - b_0}}_{c_i \in \mathcal{M}} x^{-i} = 1$$

and

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

But now

$$\begin{aligned} 1 &= \sum_{i=0}^{n} a_i x^i \\ &= \sum_{i=0}^{n-1} a_i x^i + a_n x^n \\ &= \sum_{i=0}^{n-1} a_i x^i + a_n \sum_{i=1}^{m} c_i x^{n-i} \\ &= \sum_{i=0}^{n-i} d_i x^i \end{aligned}$$

with $d_i \in \mathcal{M}$; this contradicts minimality of n. Similarly, if $m \geq n$ we contradict the minimality of m.
So $x \in \mathcal{O}$ or $\frac{1}{x} \in \mathcal{O}$. □ Claim 4.41

Now $R \subseteq R_P \subseteq \mathcal{O} \subseteq K$ with $PR_P \vee \mathcal{M}$ and $PR_P \cap R = P$. Now, $\mathcal{M} \cap R_P \supseteq PR_P$; so, by maximality of PR_P in R_P, we get that $\mathcal{M} \cap R_P = PR_P$. So $\mathcal{M} \cap R = (\mathcal{M} \cap R_P) \cap R = PR_P \cap R = P$. □ Theorem 4.39

Corollary 4.42 (3.1.2)**.** *Suppose (K, v, Γ_v) is a valued field and $K \subseteq L$ is a field extension. Then v extends to a valuation on L.*

Proof. Apply Chevalley's theorem to $R = \mathcal{O}_v \subseteq L$ and $P = \mathcal{M}_v$; we then get a valuation subring $\mathcal{O}_v \subseteq \mathcal{O}_w \subseteq L$ with $\mathcal{M}_w \cap \mathcal{O}_v = \mathcal{M}_v$. To see that w extends v, we need to show that $\mathcal{O}_w \cap K = \mathcal{O}_v$.

Claim 4.43. *$S = \mathcal{O}_w \cap K$ is a valuation subring of K.*

Proof. Suppose $x \in K^\times$. Then $x \in L^\times$, so $x \in \mathcal{O}_w$ or $x^{-1} \in \mathcal{O}_w$; hence either $x \in \mathcal{O}_w \cap K = S$ or $x^{-1} \in \mathcal{O}_w \cap K = S$. □ Claim 4.43

Claim 4.44. *$\mathcal{N} = \mathcal{M}_w \cap K$ is the maximal ideal of S.*

Proof. Suppose $x \in S$. Then x is a unit of S if and only if x is a unit of $\mathcal{O}_w$; this is equivalent to requiring that $x \notin \mathcal{M}_w$, which is in turn equivalent to requiring that $x \notin \mathcal{M}_w \cap K$. □ Claim 4.44

Claim 4.45. *$\mathcal{M}_w \cap K = \mathcal{M}_w \cap \mathcal{O}_v$.*

Proof.

($\supseteq$) Clear.

($\subseteq$) Suppose $x \in \mathcal{M}_w \cap K$. If $x \notin \mathcal{O}_v$ then $x^{-1} \in \mathcal{O}_v \subseteq \mathcal{O}_w$, contradicting our assumption that $x \in \mathcal{M}_w$. So $x \in \mathcal{O}_v$. □ Claim 4.45

Hence $S = \mathcal{O}_w \cap K$ and $\mathcal{M}_w \cap K = \mathcal{M}_w \cap \mathcal{O}_v = \mathcal{M}_v$.
But for $x \in K$ we have

$$\begin{aligned} x \notin S &\iff x^{-1} \in \mathcal{N} \\ &\iff x^{-1} \in \mathcal{M}_v \\ &\iff x \notin \mathcal{O}_v \end{aligned}$$

So $S = \mathcal{O}_v$. □ Corollary 4.42

Note that the above proof in fact shows:

Proposition 4.46. *Suppose (K, v, Γ_v) is a valued field and $K \subseteq L$. Then a valuation w on L extends v if and only if $\mathcal{M}_w \cap \mathcal{O}_v = \mathcal{M}_v$.*

Proof.

($\Longrightarrow$) Suppose w extends v to L; so $\mathcal{O}_w \cap K = \mathcal{O}_v$. We saw in Claim 4.44 and Claim 4.45 that $\mathcal{M}_v = \mathcal{M}_w \cap K = \mathcal{M}_w \cap \mathcal{O}_v$.

($\Longleftarrow$) By Claim 4.43, Claim 4.44, and Claim 4.45, we have that $\mathcal{O}_w \cap K$ is a valuation ring on K and $\mathcal{M}_w \cap K$ is its maximal ideal; furthermore we have $\mathcal{M}_w \cap K = \mathcal{M}_w \cap \mathcal{O}_v = \mathcal{M}_v$ by assumption. We also proved that two valuation subrings of a field with the same maximal ideal are the same; so $\mathcal{O}_w \cap K = \mathcal{O}_v$, and w extends v. □ Proposition 4.46

Definition 4.47. Suppose $R \subseteq S$ are domains; suppose $a \in S$. We say a is *integral* over R if there is a monic $f(x) \in R[x]$ such that $f(a) = 0$. We say R is *integrally closed in* S if whenever $a \in S$ is integral over R, we must have $a \in R$.

Lemma 4.48. *Valuation subrings are integrally closed.*

Proof. Suppose $\mathcal{O}$ is a valuation subring of the field K; suppose $x \in K \setminus \mathcal{O}$. Suppose for contradiction that x is integral over $\mathcal{O}$; so

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

for some $n \geq 1$ and $a_i \in \mathcal{O}$. Then

$$1 + a_1 x^{-1} + a_2 x^{-2} + \cdots + a_n x^{-n} = 0$$

Since $x \notin \mathcal{O}$ we must then have that $x^{-1} \in \mathcal{O}$, and in fact that $x^{-1} \in \mathcal{M}$. So $1 \in \mathcal{M}$, a contradiction. □ Lemma 4.48

Theorem 4.49 (3.1.3)**.** *Suppose (K, v, Γ_v) is a valued field; suppose $L \supseteq K$ is a field extension. Let*

$$\mathbb{V} = \{\, \mathcal{O}_w : w \text{ a valuation on } L \text{ extending } V \,\}$$

Then

$$\bigcap \mathbb{V} = \{\, a \in L : a \text{ is integral over } \mathcal{O}_v \,\} = \mathcal{O}_v^{\text{int}}$$

is the integral closure of $\mathcal{O}_v$ in L.

Some facts about integral closures:

Fact 4.50.

1. *If $R \subseteq L$ then R^{int} is a subring of L.*
2. *$(R^{\text{int}})^{\text{int}} = R^{\text{int}}$.*

Note that by Proposition 4.46 we get that

$$\mathbb{V} = \{\, \mathcal{O} \subseteq L : \mathcal{O} \text{ a valuation subring}, \mathcal{O}_v \subseteq \mathcal{O}, \mathcal{M} \cap \mathcal{O}_v = \mathcal{M}_v \,\}$$

More generally, given any subring $R \subseteq L$, consider

$$\mathcal{S}_R = \{\, \mathcal{O} \subseteq L : \mathcal{O} \text{ a valuation subring}, R \subseteq \mathcal{O}, \mathcal{M} \cap R \text{ maximal in } R \,\}$$

So $\mathbb{B} = \mathcal{S}_{\mathcal{O}_v}$.

So Theorem 4.49 follows from the following more general claim:

Proposition 4.51. *For any subring $R \subseteq L$ we have*

$$\bigcap \mathcal{S}_R = R^{\text{int}}$$

Proof.

($\supseteq$) If $a \in L$ is integral over R then for any $\mathcal{O} \in \mathcal{S}_R$ we have that a is integral over $\mathcal{O}$. By Lemma 4.48 we get that $\mathcal{O}$ is integrally closed; so $a \in \mathcal{O}$.

($\subseteq$) Suppose $x \in L \setminus R^{\text{int}}$. We seek $\mathcal{O} \in \mathcal{S}_R$ with $x \notin \mathcal{O}$. We achieve this by finding $\mathcal{O} \in \mathcal{S}_r$ such that $x^{-1} \in \mathcal{M}$ (and hence $x \notin \mathcal{O}$).

Consider $R^{\text{int}}[x^{-1}] \subseteq L$.

Claim 4.52. $x \notin R^{\text{int}}[x^{-1}]$.

Proof. If

$$x = a_n x^{-n} + a_{n-1} x^{-n+1} + \cdots + a_0$$

with $a_i \in R^{\text{int}}$, then

$$x^{n+1} = a_n + a_{n-1} x + \cdots + a_0 x^n$$

and $x \in (R^{\text{int}})^{\text{int}}$, a contradiction. □ Claim 4.52

So x^{-1} is not a unit in $R^{\text{int}}[x^{-1}]$; so there is a maximal ideal M of $R^{\text{int}}[x^{-1}]$ with $x^{-1} \in M$.

Claim 4.53. *$M \cap R$ is maximal.*

Proof. We first show that $M \cap R^{\text{int}}$ is maximal. We have $\pi \colon R^{\text{int}}[x^{-1}] \to R^{\text{int}}[x^{-1}]/M$, where the codomain is a field; so $\pi \restriction R^{\text{int}} \colon R^{\text{int}} \to R^{\text{int}}[x^{-1}]/M$. This last is surjective since

$$\underbrace{a_n x^{-n} + \cdots + a_1 x^{-1}}_{\in M} + a_0 \in R^{\text{int}}[x^{-1}]$$

since $x^{-1} \in M$; so modulo M we have that every element of $R^{\text{int}}[x^{-1}]$ is in R^{int}. So $\pi \restriction R^{\text{int}}$ is surjective; hence the kernel $M \cap R^{\text{int}}$ is maximal.

We now have the following diagram

$$\begin{array}{ccc} R^{\text{int}} & \longrightarrow & R^{\text{int}}/M \cap R^{\text{int}} \\ \uparrow & & \uparrow \\ R & \longrightarrow & R/M \cap R \end{array}$$

Exercise 4.54. If $A \subseteq B$ is an integral extension and B is a field, then A is a field.

Hence $R/M \cap R$ is a field, and $M \cap R$ is maximal in R. □ Claim 4.53

We now apply Chevalley's theorem to $R^{\text{int}}[x^{-1}]$ and M; we get a valuation subring $\mathcal{O} \subseteq L$ such that $R^{\text{int}}[x^{-1}] \subseteq \mathcal{O}$ and $\mathcal{M} \cap R^{\text{int}}[x^1] = M$. Then $\mathcal{M} \cap R = (\mathcal{M} \cap R^{\text{int}}[x^{-1}]) \cap R = M \cap R$ is maximal by the claim. So $\mathcal{O} \in \mathcal{S}_R$. But $x^{-1} \in M \subseteq \mathcal{M}$; so $x \notin \mathcal{O}$, and

$$x \notin \bigcap \mathcal{S}_R$$

as desired. □ Proposition 4.51

The above proof probably works without passing to the integral closure.
Assignment 2 question 6: assume $c \in K$.

Notation 4.55. We will often write $(K, \mathcal{O}_v)$ for a valued field, rather than (K, v, Γ_v). We will also write $(K, \mathcal{O}_v) \subseteq (L, \mathcal{O}_w)$ to mean that $K \subseteq L$ is a subfield and $\mathcal{O}_w \cap K = \mathcal{O}_v$; i.e. that w is an extension of v.

Definition 4.56. Suppose $(K, \mathcal{O}_v) \subseteq (L, \mathcal{O}_w)$. The *ramification index* of this extension is

$$e(\mathcal{O}_w/\mathcal{O}_v) = [\Gamma_w : \Gamma_v] \in \mathbb{N} \cup \{\infty\}$$

The *residue degree* of the extension is

$$f(\mathcal{O}_w/\mathcal{O}_v) = [\overline{L}_w : \overline{K}_v] \in \mathbb{N} \cup \{\infty\}$$

We say $(L, \mathcal{O}_w)$ is an *immediate* extension of $(K, \mathcal{O}_v)$ if $e(\mathcal{O}_w/\mathcal{O}_v) = f(\mathcal{O}_w/\mathcal{O}_v) = 1$; i.e. $\Gamma_w = \Gamma_v$ and $\overline{L}_w = \overline{K}_v$.

Example 4.57. $(\mathbb{Q}, \mathbb{Z}_{(p)}) \subseteq (\mathbb{Q}_p, \mathbb{Z}_p)$ is an immediate extension. (This in fact generalizes to all completions of classical valuations.)

Remark 4.58. If $(K_1, \mathcal{O}_{v_1}) \subseteq (K_2, \mathcal{O}_{v_2}) \subseteq (K_3, \mathcal{O}_{v_3})$ then

$$e(\mathcal{O}_{v_3}/\mathcal{O}_{v_2})e(\mathcal{O}_{v_2}/\mathcal{O}_{v_1}) = e(\mathcal{O}_{v_3}/\mathcal{O}_{v_1})$$
$$f(\mathcal{O}_{v_3}/\mathcal{O}_{v_2})f(\mathcal{O}_{v_2}/\mathcal{O}_{v_1)}) = f(\mathcal{O}_{v_3}/\mathcal{O}_{v_1})$$

Theorem 4.59 (3.2.3)**.** *Suppose $(K, \mathcal{O}_v) \subseteq (L, \mathcal{O}_w)$ is an extension of valued fields where L/K is finite. Then e and f are finite and $ef \leq [L : K]$.*

This is a corollary of the following:

Proposition 4.60. *Suppose $(K, \mathcal{O}_v) \subseteq (L, \mathcal{O}_w)$; let E be a $\overline{K}_v$-basis for $\overline{L}_w$, and let G be a set of representatives for the cosets of Γ_v in Γ_w. For each $e \in E$ let $a_e \in \mathcal{O}_w$ be such that $\overline{a_e} = e$; for each $\gamma \in G$, let $b_\gamma \in L$ satisfy $w(b_\gamma) = \gamma$. Then $X = \{ a_e b_\gamma : e \in E, \gamma \in G \}$ is a K-linearly independent subset of L.*

Proof. We prove a stronger statement: if

$$c_1 a_{e_1} b_{\gamma_1} + \cdots + c_\ell a_{e_\ell} b_{\gamma_\ell}$$

is a K-linear combination of elements of X, then

$$w(d) = \min_{1 \leq i \leq \ell} w(c_i a_{e_i} b_{\gamma_i})$$

This would prove the proposition by taking $d = 0$, noting that none of the a_{e_i} or b_{γ_i} are zero, and hence that all c_i are zero.

Without loss of generality, we may assume $w(c_1 b_{\gamma_1})$ is minimum among $\{ w(c_i b_{\gamma_i}) : 1 \leq i \leq \ell \}$. We may also assume $c_i \neq 0$, since otherwise all c_i are zero and the claim holds.

Claim 4.61. *$w(c_i b_{\gamma_i}) > w(c_1 b_{\gamma_1})$ for all i such that $\gamma_i \neq \gamma_1$.*

Proof. If $w(c_i b_{\gamma_i}) = w(c_1 b_{\gamma_1})$, then $\gamma_1 - \gamma_i = w(c_i) - w(c_1) \in \Gamma_v$. But $\gamma_1 \neq \gamma_i$ come from G, and thus represents distinct cosets of Γ_v in Γ_w, a contradiction. □ Claim 4.61

Suppose for contradiction that

$$w(d) > \min_{1 \leq i \leq \ell} w(c_i a_{e_i} b_{\gamma_i}) = w(c_{i_0} a_{e_{i_0}} b_{\gamma_{i_0}})$$

for some i_0. Then

$$\frac{d}{c_{i_0} a_{e_{i_0}} b_{\gamma_{i_0}}} \in \mathcal{M}_w$$

and

$$\frac{d}{c_{i_0} b_{\gamma_{i_0}}} \in \mathcal{M}_w$$

since $a_{e_{i_0}} \in \mathcal{O}_w$. Then

$$\frac{d}{c_1} b_{\gamma_1} \in \mathcal{M}_w$$

since $w(c_{i_0}b_{\gamma_{i_0}}) \geq w(c_1 b_{\gamma_1})$. But

$$\underbrace{\frac{d}{c_1 b_{\gamma_1}}}_{\in \mathcal{M}_w} = \sum_{\substack{i \\ \gamma_i = \gamma_1}} \frac{c_i a_{e_i}}{c_1} + \sum_{\substack{i \\ \gamma_i \neq \gamma_1}} \underbrace{\frac{c_i b_{\gamma_i}}{c_1 b_{\gamma_1}}}_{\in \mathcal{M}_w} \underbrace{a_{e_i}}_{\in \mathcal{O}_w}$$

Hence

$$\sum_{\substack{i \\ \gamma_i = \gamma_1}} \frac{c_i}{c_1} a_{e_i} \in \mathcal{M}_w$$

But

$$\frac{c_i}{c_1} = \frac{c_i b_{\gamma_i}}{c_1 b_{\gamma_1}} \in \mathcal{O}_w$$

for i such that $\gamma_i = \gamma_1$ since $w(c_i b_{\gamma_i} \geq w(c_1 b_{\gamma_1})$. Note also that $\frac{c_i}{c_1} \in \mathcal{O}_w \cap K = \mathcal{O}_v$, so

$$\overline{\left(\frac{c_i}{c_1}\right)} \in \overline{K}_v$$

Taking residues, we then find that

$$\sum_{\substack{i \\ \gamma_i = \gamma_1}} \overline{\left(\frac{c_i}{c_1}\right)} e_i = 0$$

since $\overline{a_{e_i}} = e_i$, and the coefficients are not all zero since

$$\overline{\left(\frac{c_1}{c_1}\right)} = 1$$

But this contradicts $\overline{K}_v$-linear independence of E. □ Proposition 4.60

Proposition 4.62. *Suppose $(K, \mathcal{O}_v) \subseteq (L, \mathcal{O}_w)$ is an extension of valuations with L/K algebraic. Then $\overline{L}_w/\overline{K}_v$ is algebraic and Γ_w/Γ_v is a torsion grape.*

Proof. Suppose $\gamma \in \Gamma_w$; say $\gamma = w(a)$ for $a \in L$. Then $K(a)/K$ is a finite extension; so we may apply the previous proposition to the extension $(K, \mathcal{O}_v) \subseteq (K(a), \mathcal{O}_w \cap K(a))$. (Note that $\mathcal{O}_w \cap K(a)$ is indeed the valuation ring of $w \restriction K(a)$.) So $w(K(a)^\times)/\Gamma_v$ is finite; say of order N. Then $N\gamma \in \Gamma_v$, and $\gamma + \Gamma_v$ is torsion in Γ_w/Γ_v. So Γ_w/Γ_v is torsion.

Suppose now that $\overline{a} \in \overline{L}_w$, so $a \in \mathcal{O}_w$. Now, a is algebraic over K, so $K(a)/K$ is a finite extension; so, again by the previous proposition, we get that $\overline{K(a)}_w/\overline{K}_v$ is finite. So $\overline{a}$ is algebraic over $\overline{K}_v$. So $\overline{L}_w$ is an algebraic extension of $\overline{K}_v$. □ Proposition 4.62

The following lemma will be useful later:

Lemma 4.63 (3.2.8)**.** *Suppose $(K, \mathcal{O}_v) \subseteq (L, \mathcal{O}_{w_1})$ and $(K, \mathcal{O}_v) \subseteq (L, \mathcal{O}_{w_2})$ with L an algebraic extension of K. If $\mathcal{O}_{w_1} \subseteq \mathcal{O}_{w_2}$, then $\mathcal{O}_{w_1} = \mathcal{O}_{w_2}$.*

Proof. Suppose $\mathcal{O}_v \subseteq \mathcal{O}_{w_1} \subseteq \mathcal{O}_{w_2}$. Then

$$\underbrace{\mathcal{O}_v/(\mathcal{M}_{w_2} \cap \mathcal{O}_v)}_{\mathcal{O}_v/\mathcal{M}_v = \overline{K}_v} \subseteq \mathcal{O}_{w_1}/(\mathcal{M}_{w_2} \cap \mathcal{O}_{w_1}) \subseteq \underbrace{\mathcal{O}_{w_2}/\mathcal{M}_{w_2}}_{\overline{L}_{w_2}}$$

Let $R = \mathcal{O}_{w_1}/(\mathcal{M}_{w_2} \cap \mathcal{O}_{w_2})$; so $\overline{K}_v \subseteq R \subseteq \overline{L}_{w_2}$. But $\overline{L}_{w_2}/\overline{K}_v$ is algebraic by the previous proposition; so R is a field. (Indeed, if $a \in R$, then a is algebraic over $\overline{K}_v$, so $\overline{K}_v[a] = \overline{K}_v(a)$, and $a^{-1} \in R$.)

Claim 4.64. *R is a valuation subring of $\overline{L}_{w_2}$.*

Proof. Suppose $\overline{a} \in \overline{L}_{w_2}$ with $a \in \mathcal{O}_{w_2}$. If $a \in \mathcal{O}_{w_1}$, then $\overline{a} \in R$. If $a \notin \mathcal{O}_{w_1}$, then $a^{-1} \in \mathcal{O}_{w_1}$; so $\overline{a^{-1}} = \overline{a}^{-1} \in R$. □ Claim 4.64

So $R = \overline{L}_{w_2}$, since $\overline{L}_{w_2} = \mathrm{Frac}(R) = R$. Suppose $a \in \mathcal{O}_{w_2}$. Then by the above there is $b \in \mathcal{O}_{w_1}$ and $x \in \mathcal{M}_{w_2}$ such that $a = b + x$. But now $x \in \mathcal{M}_{w_2}$ then $x^{-1} \notin \mathcal{O}_{w_2}$; in particular, we get that $x^{-1} \notin \mathcal{O}_{w_1}$, and $x \in \mathcal{O}_{w_1}$. (In fact $x \in \mathcal{M}_{w_1}$.) So $a = b + x \in \mathcal{O}_{w_1}$. So $\mathcal{O}_{w_2} \subseteq \mathcal{O}_{w_1}$. □ Lemma 4.63

Proposition 4.65. *Suppose $(K, \mathcal{O}_v) \subseteq (L, \mathcal{O}_w)$ where $L = K^{\mathrm{alg}}$. Then*

1. $\overline{L}_w = \left(\overline{K}_v\right)^{\mathrm{alg}}$.
2. $\Gamma_w = \mathrm{div}(\Gamma_v)$ *is the* divisible hull *of* Γ_v*; i.e.*
   (a) Γ_w/Γ_v *is torsion.*
   (b) Γ_w *is divisible.*

Equivalently, every map of Γ_v to a divisible abelian grape factors through the embedding $\Gamma_v \hookrightarrow \Gamma_w$.

Proof. 1. We already know that $\overline{L}_w/\overline{K}_v$ is algebraic; it then suffices to check that $\overline{L}_w$ is algebraically closed. Suppose $P(x)$ is a non-zero polynomial over $\overline{L}_w$; we may assume it is monic, say

$$P(x) = x^n + \alpha_1 x^{n-1} + \cdots + \alpha_{n-1}x + \alpha_n$$

with $\alpha_1, \ldots, \alpha_n \in \overline{L}_w$ and $\alpha_i = \overline{a_i}$ for $a_i \in \mathcal{O}_w$.

Consider

$$Q(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \in \mathcal{O}_w[x]$$

Since L is algebraically closed, we get that $Q(x)$ has a root in $\mathcal{O}_w$. Since $Q(x)$ is monic and has coefficients in $\mathcal{O}_w$ and since $\mathcal{O}_w$ is integrally closed in L we get that $Q(x)$ has a root in $\mathcal{O}_w$; say $b \in \mathcal{O}_w$ has

$$b^n + a_1 b^{n-1} + \cdots + a_{n-1}b + a_n = 0$$

Taking residues, we find that

$$\overline{b}^n + \overline{a_1}\overline{b}^{n-1} + \cdots + \overline{a_n} = 0$$

So $P(\overline{b}) = 0$ and $\overline{b} \in \overline{L}_w$. So $\overline{L}_w = \left(\overline{K}_v\right)^{\mathrm{alg}}$.

2. We already know that $\Gamma_w/\Gamma_v$is torsion. Suppose $\gamma \in \Gamma_w$ and $n > 0$. Write $\gamma = w(a)$ where $a \in L^\times$. Since L is algebraically closed, there is $b \in L^\times$ such that $b^n = a$; then $\gamma = w(a) = w(b^n) = nw(b)$. So $w(b) \in \Gamma_w$ and $nw(b) = \gamma$. So Γ_w is divisible. □ Proposition 4.65

Our next goal is to count the number of extensions of v from K to a finite extension L.

Recall: K^{sep} is the set of $a \in K^{\mathrm{alg}}$ such that the minimal polynomial of a over K is a separable polynomial. Note that in characteristic 0 we have $K^{\mathrm{sep}} = K^{\mathrm{alg}}$.

Fact 4.66. *In characteristic* $\mathrm{char}(K) = p > 0$ *we have that $K^{\mathrm{alg}}/K^{\mathrm{sep}}$ is a purely inseparable extension: if $a \in K^{\mathrm{alg}}$ then $a^{p^n} \in K^{\mathrm{sep}}$ for some $n \geq 0$.*

Definition 4.67. Suppose L/K is an algebraic extension. Then L is of *finite separable degree* if $(L \cap K^{\mathrm{sep}})/K$. In this case we set

$$[L : K]_{\mathrm{sep}} = [L \cap K^{\mathrm{sep}} : K]$$

Example 4.68. Consider

$$L = \bigcup_{n \geq 0} K^{\left(\frac{1}{p^n}\right)} = K^{\mathrm{per}}$$

the *perfect hull* of K. Then L/K is algebraic of finite separable degree since $L \cap K^{\mathrm{sep}} = K$. But L/K is not finite.

Lemma 4.69 (3.2.6)**.** *Suppose K is a field with finitely many valuation subrings $\mathcal{O}_1, \ldots, \mathcal{O}_n$. Suppose $\mathcal{O}_i \not\subseteq \mathcal{O}_j$ for $i \neq j$. Let $R = \mathcal{O}_1 \cap \cdots \cap \mathcal{O}_n$. Let $P_i = \mathcal{M}_i \cap R$. Then*

1. $\mathcal{O}_i = R_{P_i}$ *for* $i \in \{1, \ldots, n\}$.

2. *$P_1, \dots, P_n$ are the distinct maximal ideals of R.*

Proof. We check part (1).

Fix $i \in \{1, \dots, n\}$. Then $\mathcal{O}_i$ and R_{P_i} are subrings of K.

If $x \in R \setminus P_i$, then $x \in \mathcal{O}_i \setminus \mathcal{M}_i$; hence $\frac{1}{x} \in \mathcal{O}_i$. Hence $R_{P_i} \subseteq \mathcal{O}_i$.

For the converse, suppose $a \in \mathcal{O}_i$. Let

$$J = \{\, 1 \le j \le n : a \in \mathcal{O}_j \,\}$$

So $i \in J$. Choose a prime p such that

- $p > \operatorname{char}(K)$
- $p > \operatorname{char}(\overline{K}_j)$ for $j \in J$ (where $\overline{K}_j$ is the residue field corresponding to $\mathcal{O}_j$)
- $\operatorname{res}_j(a)$ is not a primitive p^{th} root of unity in $\overline{K}_j$ for any $j \in J$.

Let $b = 1 + a + a^2 + \cdots + a^{p-1}$; so $b \in \mathcal{O}_j$ for all $j \in J$. We will show that $\frac{a}{b}, \frac{1}{b} \in R$.

Claim 4.70. *For $j \in J$ we have $b \in \mathcal{O}_j^\times$.*

Proof. If $\operatorname{res}_j(a) = 1$, then $\operatorname{res}_j(b) = p \neq 0$ in $\overline{K}_j$; so $b \notin \mathcal{M}_j$, as desired.

Suppose then that $\operatorname{res}_j(a) \neq 1$. Then

$$\operatorname{res}_j(b) = 1 + \operatorname{res}_j(a) + \cdots + \operatorname{res}_j(a)^{p-1}$$

So

$$\operatorname{res}_j(b)(1 - \operatorname{res}_j(a)) = 1 - \operatorname{res}_j(a)^p$$

and

$$\operatorname{res}_j(b) = \frac{1 - \operatorname{res}_j(a)^p}{1 - \operatorname{res}_j(a)} \neq 0$$

by choice of p. □ Claim 4.70

Hence $b^{-1} \in \mathcal{O}_j$ for all $j \in J$.

Suppose $j \notin J$. Then $a \notin \mathcal{O}_j$, and $a^{-1} \in \mathcal{M}_j$; hence

$$1 + a^{-1} + a^{-2} + \cdots + a^{-p+1} \notin \mathcal{M}_j$$

But now

$$b^{-1} = \frac{1}{1 + a + \cdots + a^{p-1}} = \frac{a^{-p+1}}{a^{-p+1} + a^{-p+2} + \cdots + a^{-1} + 1}$$

But $a^{-1} \in \mathcal{O}_j$, so $a^{-p+1} \in \mathcal{O}_j$; so

$$\frac{1}{1 + a^{-1} + \cdots + a^{-p+1}} \in \mathcal{O}_j$$

and $b^{-1} \in \mathcal{O}_j$.

Similar arguments show that $\frac{a}{b} \in R$. But now $b \in \mathcal{O}_i^\times$, so $\frac{1}{b} \in \mathcal{O}_i \setminus \mathcal{M}_i$; so $\frac{1}{b} \in R \setminus P_i$, and $b = \frac{1}{b^{-1}} \in R_{P_i}$. So

$$a = \underbrace{\frac{a}{b}}_{\in R} \underbrace{b}_{} \in R_{P_i} \in R_{P_i}$$

□ Lemma 4.69

Corollary 4.71 (3.2.7)**.** *With the setup of the previous lemma, consider the map*

$$\begin{aligned} R &\to \overline{K}_1 \times \cdots \times \overline{K}_n \\ a &\mapsto (\operatorname{res}_1(a), \dots, \operatorname{res}_n(a)) \end{aligned}$$

where $\operatorname{res}_i \colon \mathcal{O}_i \to \overline{K}_i$. Then this map is surjective.

Proof. By part (2) of the lemma, we get that if $i \neq j$ then P_i and P_j are distinct maximal ideals of R. So $P_i + P_j = R$. By the Chinese remainder theorem, we then get that

$$\begin{aligned} R &\to R/P_1 \times \cdots \times R/P_n \\ a &\mapsto (\pi_1(a), \ldots, \pi_n(a)) \end{aligned}$$

is surjective, where $\pi_i \colon R \to R/P_i$ is the quotient map. But $R/P_i \cong R_{P_i}/P_i R_{P_i} \cong \mathcal{O}_i/\mathcal{M}_i = \overline{K}_i$, and this isomorphism preserves the quotient maps. □ Corollary 4.71

Theorem 4.72 (3.2.9)**.** *Suppose $(K, \mathcal{O}_v)$ is a valued field and L/K is an algebraic extension of finite separable degree. Then there are at most $[L:K]_{\text{sep}}$ extensions of v to L, up to equivalence.*

Proof. By a previous lemma, we know $\mathcal{O}_i \not\subseteq \mathcal{O}_j$ if $i \neq j$. So the corollary yields $R \to \overline{L}_1 \times \cdots \times \overline{L}_n$ is surjective, where $R = \mathcal{O}_1 \cap \cdots \cap \mathcal{O}_n$. For $i \in \{1, \ldots, n\}$, let $c_i \in R$ be such that

$$\operatorname{res}_j(c_i) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

Then each c_i is algebraic over K. So if $p = \operatorname{char}(K)$ then there is an $\ell \geq 0$ such that each $c_i^{p^\ell} \in K^{\text{sep}} \cap L$. Let $d_i = c_i^{p^\ell} \in R$. Note

$$\operatorname{res}_j(d_i) = \operatorname{res}_j(c_i^{p^\ell}) = \operatorname{res}_j(c_i)^{p^\ell} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

(If $\operatorname{char}(K) = 0$ we instead let $d_i = c_i$, which is already separably algebraic.)

Claim 4.73. *$d_1, \ldots, d_n$ are K-linearly independent.*

Proof. Toward a contradiction, suppose $a_1 d_1 + \cdots + a_n d_n = 0$ where $a_1, \ldots, a_n \in K$ are not all 0. We may assume

$$v(a_1) = \min_{1 \leq i \leq n} v(a_i)$$

Write

$$d_1 = -\frac{a_2}{a_1} d_2 - \frac{a_3}{a_1} d_3 - \cdots - \frac{a_n}{a_1} d_n$$

For $j > 1$, we have $\operatorname{res}_1(d_j) = 0$; hence $d_j \in \mathcal{M}_1$ for each $j > 1$. Hence for $j \geq 1$, we have

$$v\left(\frac{a_j}{a_1}\right) = v(a_j) - v(a_1) \geq 0$$

So $\frac{a_j}{a_1} \in \mathcal{O}_v \subseteq \mathcal{O}_1$, and $d_1 \in \mathcal{M}_1$. But this contradicts our assumption that $\operatorname{res}_1(d_1) = 1 \neq 0$. □ Claim 4.73

Hence $[L:K]_{\text{sep}} = [L \cap K^{\text{sep}} : K] \geq n$. □ Theorem 4.72

Corollary 4.74. *Suppose $(K, \mathcal{O}_v)$ is a valued field and L/K is a purely inseparable extension. Then there is a unique extension of v to L.*

Proof. "Purely inseparable" exactly means that $[L:K]_{\text{sep}} = 1$. □ Corollary 4.74

Theorem 4.75 (Conjugacy theorem (3.2.15))**.** *Suppose L/K is a normal algebraic extension and v is a valuation on K. If v_1, v_2 extend v to L then there is $\sigma \in \operatorname{Aut}(L/K)$ such that $\sigma \mathcal{O}_{v_1} = \mathcal{O}_{v_2}$.*

Remark 4.76.

1. Recall that L/K is *normal* if L is the spliotting field of a (not necessarily finite) set of polynomials over K; equivalently, if whenever $f \in K[x]$ is irreducible and has a root in L then all the roots of f are in L.
2. We let $\operatorname{Aut}(L/K)$ be the grape of field automorphisms of L that act as the identity on K.

3. If w extends v to L and $\sigma \in \mathrm{Aut}(L/K)$, then $\sigma\mathcal{O}_w \subseteq L$ is a valuation subring, and $\sigma\mathcal{O}_w \cap K = \mathcal{O}_w \cap K = \mathcal{O}_v$; i.e. $(L, \sigma\mathcal{O}_w)$ is a valuation extending v. (In fact, $(L, \mathcal{O}_w) \cong (L, \sigma\mathcal{O}_w)$ via σ.) So $\mathrm{Aut}(L/K)$ acts on the set of extensions of v to L; the conjugacy theorem says that the action is transitive.

4. In particular, all extensions of v to a normal algebraic L/K are isomorphic. So the residue degree and ramification index of such extensions are invariant: they depend only on L/K, and not on the particular extension of v to L.

Proof of Theorem 4.75.

Case 1. We first check the case where L/K is Galois; i.e. normal, finite, and separable. Let

$$\begin{aligned}
\mathcal{O}_1 &= \mathcal{O}_{v_1} \\
\mathcal{O}_1 &= \mathcal{O}_{v_2} \\
G &= \mathrm{Aut}(L/K) \\
H_1 &= \mathrm{stab}(\mathcal{O}_1) \\
&= \{\, \sigma \in G : \sigma\mathcal{O}_1 = \mathcal{O}_1 \,\} \\
H_2 &= \mathrm{stab}(\mathcal{O}_2)
\end{aligned}$$

so G is a finite grape. Write

$$G = \bigcup_{i=1}^{n} H_1\sigma_i^{-1} = \bigcup_{j=1}^{m} H_2\tau_j^{-1}$$

as the union of distinct cosets of H_1 and H_2 (with $\sigma_i, \tau_j \in G$). We will show that for some $1 \le i \le n$ and some $1 \le j \le m$ we have $\tau_j^{-1}\sigma_i\mathcal{O}_1 = \mathcal{O}_2$.

Now, note that $\tau_j^{-1}\sigma_1\mathcal{O}_1 = \mathcal{O}_2$ if and only if $\sigma_i\mathcal{O}_1 = \tau_j\mathcal{O}_2$; by Lemma 4.63 this occurs if and only if $\sigma_i\mathcal{O}_1 \subseteq \tau_j\mathcal{O}_2$ or $\tau_j\mathcal{O}_2 \subseteq \sigma_i\mathcal{O}_1$. Suppose for contradiction that for all i and j we have $\sigma_i\mathcal{O}_1 \not\subseteq \tau_j\mathcal{O}_2$ and $\tau_j\mathcal{O}_2 \not\subseteq \sigma_i\mathcal{O}_1$.

Claim 4.77. *For all $1 \le i < i' \le n$ we have $\sigma_i\mathcal{O}_1 \not\subseteq \sigma_{i'}\mathcal{O}_1$. Similarly, For all $1 \le j < j' \le m$ we have $\tau_j\mathcal{O}_2 \not\subseteq \tau_{j'}\mathcal{O}_2$.*

Proof. Again by Lemma 4.63, if $\sigma_i\mathcal{O}_1 \subseteq \sigma_{i'}\mathcal{O}_1$, then $\sigma_i\mathcal{O}_1 = \sigma_{i'}\mathcal{O}_1$; hence $\sigma_{i'}^{-1}\sigma_i\mathcal{O}_1 = \mathcal{O}_1$, and $\sigma_{i'}^{-1}\sigma_i \in H$. But this contradicts our assumption that i and i' represent distinct cosets of H. □ Claim 4.77

Let

$$R = \bigcap_{i=1}^{n} \sigma_i\mathcal{O}_1 \cap \bigcap_{j=1}^{m} \tau_j\mathcal{O}_2$$

Then by Corollary 4.71, since these extensions of $\mathcal{O}_v$ are all incompatible, we get that

$$R \to \left(\prod_{i=1}^{n} \sigma_i\mathcal{O}_1/\sigma_i\mathcal{M}_1\right) \times \left(\prod_{i=1}^{n} \tau_j\mathcal{O}_2/\tau_j\mathcal{M}_2\right)$$

(the product of the residue maps) is surjective. Pick $a \in R$ such that $a - 1 \in \sigma_i\mathcal{M}_i$ for $i \in \{\, 1, \ldots, n \,\}$ and $a \in \tau_j\mathcal{M}_2$ for $j \in \{\, 1, \ldots, m \,\}$.

Now, suppose $\sigma \in G$; so for some $i \in \{\, 1, \ldots, n \,\}$ and some $\rho \in H_1$ we have $\sigma = \rho \circ \sigma_i^{-1}$; likewise we write $\sigma = \eta \circ \tau_j^{-1}$ for some $j \in \{\, 1, \ldots, m \,\}$ and some $\eta \in H_2$. But then

$$\sigma(a-1) \in \sigma(\sigma_i\mathcal{M}_1) = \rho \circ \sigma_i^{-1}(\sigma_i\mathcal{M}_1) = \rho\mathcal{M}_1 = \mathcal{M}_1$$

and

$$\sigma(a) \in \sigma(\tau_j\mathcal{M}_2) = (\eta \circ \tau_j^{-1})\tau_j\mathcal{M}_2 = \eta\mathcal{M}_2 = \mathcal{M}_2$$

So $\sigma(a-1) \in \mathcal{M}_1$ and$\sigma(a) \in \mathcal{M}_2$ for all $\sigma \in G$. But

$$\prod_{\sigma \in G} \sigma(a) \in \mathcal{M}_2 \cap K = \mathcal{M}_v$$

since

$$\prod_{\sigma \in G} \sigma(a) \in L^G$$

since L/K is Galois we get that $L^G = K$. But

$$\prod_{\sigma \in G} \sigma(a) \in \underbrace{(\mathcal{M}_1 + 1)}_{\text{multiplicatively closed}} \cap K = (\mathcal{M}_1 \cap K) + 1 = \mathcal{M}_v + 1$$

a contradiction since $1 \notin \mathcal{M}_v$.

Case 2. We now check the case where L/K is finite and normal (though not necessarily separable). We then get an intermediate extension $K \subseteq L \cap K^{\text{sep}} \subseteq L$ with $L \cap K^{\text{sep}}/K$ Galois. Suppose $\mathcal{O}_1$ and $\mathcal{O}_2$ are valuation subrings of L such that $\mathcal{O}_1 \cap K = \mathcal{O}_2 \cap K = \mathcal{O}_v$. Let

$$\mathcal{O}_1' = \mathcal{O}_1 \cap (L \cap K^{\text{sep}})$$
$$\mathcal{O}_2' = \mathcal{O}_2 \cap (L \cap K^{\text{sep}})$$

By the previous case there is $\sigma \in \text{Aut}(L \cap K^{\text{sep}}/K)$ such that $\sigma\mathcal{O}_1' = \mathcal{O}_2'$.

But the restriction map $\text{Aut}(L/K) \to \text{Aut}(L \cap K^{\text{sep}}/K)$ is actually an isomorphism, and in particular is surjective. Another way to see surjectivity: suppose $a \in L$. Then for some n we have $a^{p^n} \in L \cap K^{\text{sep}}$; we then send $a \mapsto (\sigma(a^{p^n}))^{p^{-n}}$. (One can check that this is actually an isomorphism, though we only need surjectivity.)

So we can lift $\sigma \in \text{Aut}(L \cap K^{\text{sep}}/K)$ to $\widetilde{\sigma} \in \text{Aut}(L/K)$. Now, $\widetilde{\sigma}(\mathcal{O}_1) \subseteq L$ is a valuation subring, and

$$\widetilde{\sigma}(\mathcal{O}_1) \cap (L \cap K^{\text{sep}}) = \widetilde{\sigma}(\mathcal{O}_1 \cap 9L \cap K^{\text{sep}}) = \sigma(\mathcal{O}_1 \cap L \cap K^{\text{sep}} = \sigma\mathcal{O}_1' = \mathcal{O}_2'$$

But now $\mathcal{O}_2$ and $\widetilde{\sigma}(\mathcal{O}_1)$ are two extensions of $\mathcal{O}_2'$, and $L/L \cap K^{\text{sep}}$ is purely inseparable; so $\mathcal{O}_2 = \widetilde{\sigma}(\mathcal{O}_1)$.

Case 3. We now merely suppose that L/K is normal and algebraic (not necessarily finite or separable). Suppose $\mathcal{O}_1$ and $\mathcal{O}_2$ are valuation subrings of L with $\mathcal{O}_1 \cap K = \mathcal{O}_2 \cap K = \mathcal{O}_v$. Let

$$\mathcal{F} = \{\, (F, \sigma) : K \subseteq F \subseteq L, F/K \text{ normal}, \sigma \in \text{Aut}(F/K), \sigma(\mathcal{O}_1 \cap F) = \mathcal{O}_2 \cap F \,\}$$

Now, $K, \text{id}) \in \mathcal{F}$, so $\mathcal{F} \neq \emptyset$. One checks that every chain in $\mathcal{F}$ has an upper bound; by Zorn's lemma, there is a maximal $(F, \sigma) \in \mathcal{F}$. If $F = L$, then we are done. Suppose towards a contradiction that $F \neq L$; let $a \in L \setminus F$. Let $p(x)$ be the minimal polynomial of a over F; let N be the splitting field of $p(x)$ over F. We can extend σ to $\widetilde{\sigma} \in \text{Aut}(L/K)$ such that $\widetilde{\sigma}(N) = N$. (First extend σ to $\widehat{\sigma} \in \text{Aut}(K^{\text{alg}}/K)$ by uniqueness of $F^{\text{alg}} = K^{\text{alg}}$; since L/K is normal, we get $\widehat{\sigma}(L) = L$, and we let $\widetilde{\sigma} = \widehat{\sigma} \restriction L$. But now $\widetilde{\sigma}(N)$ is the splitting field of $p^\sigma(x) = p(x)$ over F (where p^σ is obtained from p by applying σ to the coefficients of p), which is just N.)

Let $\mathcal{O}_1' = \widetilde{\sigma}^{-1}(\mathcal{O}_2 \cap N)$, which is a valuation subring of N. Note also that $\mathcal{O}_1' = \widetilde{\sigma}^{-1}(\mathcal{O}_2 \cap N)$ extends $\widetilde{\sigma}^{-1}(\mathcal{O}_2 \cap F) = \sigma^{-1}(\mathcal{O}_1 \cap F) = \mathcal{O}_1 \cap F$. But $\mathcal{O}_1 \cap N$ also extends $\mathcal{O}_1 \cap F$; hence, by the previous case, we get $\tau \in \text{Aut}(N/F)$ such that $\tau(\mathcal{O}_1 \cap N) = \mathcal{O}_1'$.

Consider now $\widetilde{\sigma} \circ \tau$; note that

$$\widetilde{\sigma} \circ \tau(\mathcal{O}_1 \cap N) = \widetilde{\sigma}(\mathcal{O}_1') = \mathcal{O}_2 \cap N$$

Furthermore, since $\widetilde{\sigma} \in \text{Aut}(N/K)$ and $\tau \in \text{Aut}(N/F)$, we get that $\widetilde{\sigma} \circ \alpha t \in \text{Aut}(N/K)$. So $(N, \widetilde{\sigma} \circ \tau) \in \mathcal{F}$ and $(F, \sigma) < (N, \widetilde{\sigma} \circ \tau)$ since $\widetilde{\sigma} \circ \tau \restriction F = \sigma$, contradicting the maximality of (F, σ) in $\mathcal{F}$. So $F = L$. □ Theorem 4.75

4.1 Fundamental inequality

Suppose L/K is normal and finite; suppose v is a valuation on K. By the conjugacy theorem, we get that all extensions of v to L have the same residue degree and ramification index, since they are conjugate under $\mathrm{Aut}(L/K)$.

Definition 4.78. We call this ramification index e the *ramification index of L/K with respect to v*. We call the residue degree f the *residue degree of L/K with respect to v*.

Let r be the number of non-equivalent extensions of v to L.
We know:

$$\begin{aligned} e &\leq [L:K] \\ f &\leq [L:K] \\ ef &\leq [L:K] \\ r &\leq [L:K]_{\text{sep}} \end{aligned}$$

Theorem 4.79 (Fundamental inequality)**.** *Suppose L/K is Galois and v is a valuation on K. Then $ref \leq [L:K]$.*

In fact, one can do better (though we won't show it):

Fact 4.80. *If L/K is Galois and in characteristic 0 then $ref = [L:K]$. If L/K is Galois and in characteristic p then $refp^n = [L:K]$ (where n is an invariant called the* defect*).*

Proposition 4.81 (3.3.1)**.** *Suppose (K,v) is a valued field. Suppose L/K is Galois (in particular, finite); let $G = \mathrm{Aut}(L/K)$. Let w be an extension of v to L. Let $H = \mathrm{stab}(\mathcal{O}_w) = \{\, \sigma \in G : \sigma\mathcal{O}_w = \mathcal{O}_w \,\} \leq G$; let $F = L^H = \{\, a \in L : \sigma(a) = a \text{ for all } \sigma \in H \,\}$. Then*

1. *w is the unique extension of $w \restriction F$ to L.*
2. *$w \restriction F$ is an immediate extension of v.*

Proof.

1. Let w' be another extension of $w \restriction F$ to L. Since L/F is normal, the conjugacy theorem yields some $\sigma \in \mathrm{Aut}(L/F) = H$ such that $\sigma\mathcal{O}_w = \mathcal{O}_{w'}$. But $H = \mathrm{stab}(\mathcal{O}_w)$. So $\mathcal{O}_{w'} = \mathcal{O}_w$.

2. **Residue fields** We first show that $(F, w \restriction F)$ has the same residue field as (K,v). Suppose $a \in \mathcal{O}_{w\restriction F} = \mathcal{O}_w \cap F$. We want $c \in \mathcal{O}_v$ such that $\overline{a} = \overline{c}$; i.e. such that $a - c \in \mathcal{M}_w$.
   Let $w = w_1, w_2, \ldots, w_r$ be the non-equivalent extensions of v to L. Let

$$\begin{aligned} \mathcal{O}_i &= \mathcal{O}_{w_i} \\ \mathcal{O}_i' &= \mathcal{O}_{w_i} \cap F \end{aligned}$$

   Now, perhaps $\mathcal{O}_i' = \mathcal{O}_j'$ for some $i \neq j$ (though necessarily $\mathcal{O}_i \neq \mathcal{O}_j$ for $i \neq j$). However:

   Claim 4.82. *$\mathcal{O}_j' \neq \mathcal{O}_1'$ for $j \neq 1$.*

   Proof. Well, $\mathcal{O}_1' = \mathcal{O}_w \cap F = \mathcal{O}_{w\restriction F}$. If $\mathcal{O}_j' = \mathcal{O}_1'$ then $w_j \restriction F = w \restriction F$. So w_j and w both extend $w \restriction F$, and $j = 1$ by part (1). □ Claim 4.82

   It follows that there is

$$b \in \bigcap_{i=1}^{r} \mathcal{O}_i'$$

   such that

   - $b - a \in \mathcal{M}_{w_1} = \mathcal{M}_w$.
   - $b \in \mathcal{M}_{w_j}$ for $j \in \{\, 2, \ldots, r \,\}$.

Note that b is not yet our desired c since we don't have $b \in \mathcal{O}_v$; we just have that b is in every extension of $\mathcal{O}_v$ to F.

Let $b = b_1, b_2, \dots, b_\ell$ be the distinct conjugates of b under G; let

$$c = b_1 + b_2 + \cdots + b_\ell \in L^G = K$$

since L/K is Galois.

Claim 4.83. *$b_j \in \mathcal{M}_w$ for all $j \in \{2, \dots, \ell\}$.*

Proof. Fix $j \in \{2, \dots, \ell\}$. Let $\tau \in G$ satisfy $\tau(b) = b_j$. Since $b \in F = L^H$ and $b \neq \tau(b)$, we get that $\tau \notin H$. So $\tau^{-1} \notin H$, and $\tau^{-1}(\mathcal{O}_w) = \mathcal{O}_{w_i}$ for some $i \in \{2, \dots, r\}$. So $\tau\mathcal{O}_{w_i} = \mathcal{O}_w$; so $\tau\mathcal{M}_{w_i} = \mathcal{M}_w$. But $b \in \mathcal{M}_{w_i}$; so $\tau(b) \in \mathcal{M}_w$, and $b_j \in \mathcal{M}_w$. ☐ Claim 4.83

So

$$c = \underbrace{b_1}_{\in \mathcal{M}_w} + \underbrace{b_2 + \cdots + b_\ell}_{\in \mathcal{M}_w} \in \mathcal{O}_w \cap K = \mathcal{O}_v$$

So

$$a - c = \underbrace{a - b_1}_{\in \mathcal{M}_w} - \underbrace{b_2 - \cdots - b_\ell}_{\in \mathcal{M}_w} \in \mathcal{M}_w$$

Hence $(F, w \restriction F)$ and (K, v) have the same residue field.

Value grapes We now show that $\Gamma_{w \restriction F} = \Gamma_v$. It suffices to show that the non-negative elements are the same. Let $a \in \mathcal{O}_w \cap F$; we want $c \in K$ with $w(a) = w(c)$.

As before, we can find $b \in \mathcal{O}_w \cap F$ with

(a) $b - 1 \in \mathcal{M}_w$.

(b) $\tau(b) \in \mathcal{M}_w$ for all $\tau \in G \setminus H$.

So for all $\tau \in G \setminus H$ we have $w(\tau(b)) > 0$.

Claim 4.84. *There is $N > 0$ such that $w(b^N a) \neq w(\tau(b^N a))$ for any $\tau \in G \setminus H$.*

Proof. Well, $w(b^N a) = Nw(b) + w(a) = w(a)$. Since $b - 1 \in \mathcal{M}_w$, we get that $b \notin \mathcal{M}_w$, and $w(b) = 0$. Now

$$w(\tau(b^N a)) = Nw(\tau(b)) + w(\tau(a))$$

But $G \setminus H$ is finite and $w(\tau(b)) \neq 0$, so there is such an N. ☐ Claim 4.84

Consider $b_1 = b^N a, b_2, \dots, b_\ell$ the distinct conjugates of $b^N a$ under G.

Case 1. Assume $w(b_j) \geq w(b_1$ for all $j > 1$. Fix $j > 1$; write $b_j = \tau(b_1)$ with $\tau \in G$. Then $\tau \notin H$ since $b_1 = b^N a \in F = L^H$. Then

$$w(b_j) = w(\tau(b_1)) = w(\tau(b^N a)) \neq w(b_1)$$

by the claim. So $w(b_j) > w(b_1)$ for all $j \in \{2, \dots, r\}$. Let

$$c = b_1 + b_2 + \cdots + b_\ell \in K = L^G$$

Then

$$v(c) = w(c) = w(b_1 + b_2 + \cdots + b_n) = w(b_1) = w(b^N a) = Nw(b) + w(a) = w(a)$$

and we are done.

Case 2. Suppose $t > 0$ of the b_j have $w(b_j) < w(b_1)$. Let

$$c = \left(\sum_{1 \leq i_1 < \cdots < i_{t+1} \leq \ell} b_{i_1} \cdots b_{i_{t+1}} \right) \left(\sum_{1 \leq i_1 < \cdots < i_t} b_{i_1} \cdots b_{i_t} \right)^{-1} \in K$$

Then G fixes c since ite permutes the $b_1, \dots, b_\ell$. An argument is given in the text that $w(c) = w(a)$. ☐ Proposition 4.81

Aside 4.85 (Correction to question 4 on assignment). Suppose L/K is a Galois extension of degree n. By the primitive element theorem, we may take $L = K(a)$. Let $P(x) \in K[x]$ be irreducible with $P(a) = 0$. Suppose v is a valuation on K; we may assume $P \in \mathcal{O}_v[x]$. If $\overline{P} \in \overline{K}_v[x]$ is irreducible and of degree n then $e(L/K) = 1$ and v has a unique extension to L.

Proof of Theorem 4.79. Let $\mathcal{O}_1, \dots, \mathcal{O}_r$ be the non-equivalent extensions of $\mathcal{O}_v$ to L. Let $H = \mathrm{stab}(\mathcal{O}_1) \leq G = \mathrm{Aut}(L/K)$. For each $i \in \{1, \dots, r\}$ we let $\sigma_i \in G$ be such that $\sigma_i \mathcal{O}_1 = \mathcal{O}_i$. (These exist by the conjugacy theorem.)

Claim 4.86. *$\sigma_1, \dots, \sigma_r$ are distinct representatives of the cosets of H in G.*

Proof. Suppose $\sigma \in G$; then $\sigma\mathcal{O}_1 = \mathcal{O}_i$ for some $i \in \{1, \dots, r\}$. So $\sigma_i^{-1}\sigma\mathcal{O}_1 = \mathcal{O}_1$, and $\sigma_i^{-1}\sigma \in H$; so $\sigma \in \sigma_i H$. So

$$G = \bigcup_{i=1}^{r} \sigma_i H$$

Furthermore, if $i \neq j$ then

$$\sigma_i \mathcal{O}_1 = \mathcal{O}_i \neq \mathcal{O}_j = \sigma_j \mathcal{O}_1$$

So $\sigma_j^{-1}\sigma_i \notin H$, and $\sigma_i H \neq \sigma_j H$. □ Claim 4.86

Let $F = L^H$. We have a chain of valued fields $(K, \mathcal{O}_v) \subseteq (F, \mathcal{O}_1 \cap F) \subseteq (L, \mathcal{O}_1)$. (Since L/F is normal, $e(L/F)$ and $f(L/F)$ make sense with respect to $\mathcal{O}_1 \cap F$.) We know that

$$e(L/F)f(L/F) \leq [L : F] = |H| = \frac{|G|}{r} = \frac{[L : K]}{r}$$

so

$$re(L/F)f(L/F) \leq [L : K]$$

But by the previous proposition we have that $(F, \mathcal{O}_1 \cap F) \supseteq (K, \mathcal{O}_v)$ is an immediate extension; so

$$e(L/K) = e(L/F)$$
$$f(L/K) = f(L/F)$$

and $ref \leq [L : K]$. □ Theorem 4.79

5 Henselizations

Some remarks:

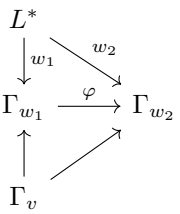
Remark 5.1.

1. Suppose $(K, \mathcal{O}_v) \subseteq (L, \mathcal{O}_w)$. This means that $\mathcal{O}_w \cap K = \mathcal{O}_v$; hence we get $\varphi\colon \Gamma_v \to \Gamma_w$ such that the following diagram commutes:

$$\begin{array}{ccc} K^* & \xrightarrow{\subseteq} & L^* \\ \downarrow{\scriptstyle v} & & \downarrow{\scriptstyle w} \\ \Gamma_v & \xrightarrow{\varphi} & \Gamma_w \end{array}$$

   We identify Γ_v with its image under φ in order to view $\Gamma_v \leq \Gamma_w$; after this identification we get $w \restriction K = v$.

2. Suppose (L, w_1) and (L, w_2) are both extensions of (K, v). Then Γ_{w_1} and Γ_{w_2} both contain Γ_v as a subgrape, and $w_1 \restriction K = v = w_2 \restriction K$. Then w_1 and w_2 being equivalent means $\mathcal{O}_{w_1} = \mathcal{O}_{w_2}$; i.e. we have an isomorphism $\varphi\colon \Gamma_{w_1} \to \Gamma_{w_2}$ of divisible abelian grapes such that the following diagram commutes:



TODO 4. *Parse the following.*

When $L = K^{\mathrm{alg}}$ there is a unique canonical isomorphism of ordered abelian grapes $\varphi\colon \Gamma_{w_1} \to \Gamma_{w_2}$ such that $\varphi \restriction \Gamma_v = \mathrm{id}$ since $\Gamma_{w_1} = \div(\Gamma_v)$ (plus torsion-free). So if $\sigma \in \Gamma_{w_1}$ then there is n such that $n\gamma \in \Gamma_v$; then $n\varphi(\gamma) = \varphi(n\gamma) = n\gamma$. But in Γ_{w_2} there is a unique γ' such that $n\gamma' = n\gamma$; so $\varphi(\gamma) = \gamma'$.

Definition 5.2. (K, v) is *Henselian* if v has a unique (up to equivalence) extension to K^{alg}.

Remark 5.3.

1. This is equivalent to requiring that for any finite extension L/K, there is a unique extension of v to L.
2. If (K, v) is Henselian and (L, w) is an algebraic extension of (K, v) then (L, w) is Henselian.
3. Since the number of non-equivalent extensions is bounded by the separable degree, we get that (K, v) is Henselian if annd only if v has a unique extension to K^{sep}. (In general, any valuation on K^{sep} extends uniquely to K^{alg} because $[K^{\mathrm{alg}} : K^{\mathrm{sep}}]_{\mathrm{sep}} = 1$.)
4. Every separably closed valued field is Henselian. The converse is false: we'll see that $\mathbb{Q}_p$ is Henselian but not algebraically closed. (In characteristic 0, separably closed is equivalent to algebraically closed.) Note that the value grape of $\mathbb{Q}_p$ is $\mathbb{Z}$, which is not divisible; this is a quick proof that $\mathbb{Q}_p$ is not divisible.

Theorem 5.4 (4.1.3)**.** *Suppose (K, v) is a valued field. Then the following are equivalent:*

1. *(K, v) is Henselian.*
2. *Hensel's lemma holds: given $P \in \mathcal{O}_v[x]$ and $a \in \overline{K}_v$ such that $\overline{P}(\alpha) = 0$ and $\overline{P}'(\alpha) \neq 0$, there is $a \in \mathcal{O}_v$ with $\overline{a} = \alpha$ and $P(a) = 0$.*
3. *Hensel-Rychik holds: given $P \in \mathcal{O}_v[x]$ and $b \in \mathcal{O}_v$ such that $v(P(b)) > 2v(P'(b))$, there is $a \in \mathcal{O}_v$ such that $P(a) = 0$ and $v(b - a) > v(P'(b))$.*
4. *Hensel-Rychik holds for separable polynomial $P \in \mathcal{O}_v[x]$.*

Corollary 5.5. *Suppose (K, v) is Henselian and $F \subseteq K$ has $F^{\mathrm{sep}} \cap K = F$. (i.e. F is separable closed in K.) Then $(F, v \restriction F)$ is Henselian.*

So $(\mathbb{Q}_p, v_p)$ is Henselian, and $\mathbb{Q}^{\mathrm{alg}} \cap \mathbb{Q}_p$ is Henselian as it is algebraically closed in $\mathbb{Q}_p$. This is an example of a classical Henselian valued field that is not complete.

Lemma 5.6. *Suppose $(K, \mathcal{O}_v)$ is a value sfield and $P \in \mathcal{O}_v[x]$. Then there are $P_1, \ldots, P_m \in \mathcal{O}_v[x]$ irreducible in $K[x]$ such that $P = P_1 \cdots P_m$.*

Proof. Let $P = P_1 \cdots P_m$ be the irreducible decomposition of P in $K[x]$. For each i let $b_i \in K$ be the coefficient of Q_i of least value. So $Q_i = b_i \widehat{Q}_i$ where $\widehat{Q}_i \in \mathcal{O}_v[x]$. So

$$P = \underbrace{b_1 b_2 \cdots b_m \widehat{Q}_1}_{P_1} \underbrace{\widehat{Q}_2}_{P_2} \cdots \underbrace{\widehat{Q}_m}_{P_m}$$

It remains to check that $b_1 \cdots b_m \in \mathcal{O}_v$. But

$$v(b_1, \ldots, b_m) = v(b_1) + \cdots + v(b_m) = w(Q_1) + \cdots + w(Q_m) = w(Q_1 Q_2 \cdots Q_m) = w(P) = v(a) \geq 0$$

where w is the Gaussian extension of v to $K(x)$ and $a$is a coefficient of P of least value; in particular, since $a \in \mathcal{O}_v$, we get that $v(a) \geq 0$. □ Lemma 5.6

Proof of Theorem 5.4.

(1) ⟹ (2) Supposef (K, v) is Henselian. We show that Hensel's lemma holds. Suppose $P \in \mathcal{O}_v[x]$ and $\alpha \in \overline{K}_v$ satisfy $\overline{P}(\alpha) = 0$ and $\overline{P}'(\alpha) \neq 0$. We wish to find $a \in \mathcal{O}_v$ such that $\overline{a} = \alpha$ and $P(a) = 0$. By the lemma we may assume that $P(x)$ is irreducible in $K[x]$. We will prove that $\deg(P) = 1$.

Factor $P(x)$ in K^{alg}:

$$P(x) = c \prod_{i=1}^{n} (x - b_i)$$

where $c \in \mathcal{O}_v$ is the leading coefficient of P and $b_1, \ldots, b_n$ are the roots of P in K^{alg}. By Henselianity there is a unique extension $\widehat{v}$ of v to K^{alg}.

Claim 5.7. $b_1, \ldots, b_n \in \mathcal{O}_{\widehat{v}}$.

Proof. Well, $b_1, \ldots, v_n$ are conjugate by $\text{Aut}(K^{\text{alg}}/K)$. Fix $i, j \in \{1, \ldots, n\}$; pick $\sigma \in \text{Aut}(K^{\text{alg}}/K)$ such that $b_i = \sigma b_j$. Then

$$\widehat{v}(b_i) = \widehat{v}(\sigma b_j) = (\widehat{v} \circ \sigma)(b_j) = \widehat{v}(b_j)$$

since $\widehat{v} \circ \sigma$ and $\widehat{v}$ are equivalent by Henselianity (since they're both extensions of v to K^{alg}) and have the same value grape; by a previous remark about extensions to K^{alg}, this forces equality. So

$$\widehat{v}(b_1) = \widehat{v}(b_2) = \cdots = \widehat{v}(b_n) \in \Gamma_{\widehat{v}}$$

Let $\gamma = \widehat{v}(b_1)$. Let $b \in K^{\text{alg}}$ satisfy $b^n = c$. Since $v(c) \geq 0$, we get that $\widehat{v}(b) = \frac{1}{n} v(c) \geq 0$, and hence that $b \in \mathcal{O}_{\widehat{v}}$. But now

$$P(x) = b^n \prod_{i=1}^{n} (x - b_i) = \prod_{i=1}^{n} (\underbrace{bx}_{\in \mathcal{O}_{\widehat{v}}} - b b_i)$$

Subclaim 5.8. $b b_i \in \mathcal{O}_{\widehat{v}}$.

Proof. Note that $c b_1 \cdots b_n$ is the constant term of $P \in \mathcal{O}_v[x]$ and $c \in \mathcal{O}_v$. So

$$0 \leq \widehat{v}(c b_1 \cdots b_n) = \widehat{v}(c) + \widehat{v}(b_1) + \cdots + \widehat{v}(b_n) = v(c) + n\gamma = n\widehat{v}(b) + n\gamma = n(\widehat{v}(b) + \gamma)$$

So $\widehat{v}(b) + \gamma \geq 0$. So

$$\widehat{v}(b b_i)\widehat{v}(b) + \widehat{v}(b_i) = \widehat{v}(b) + \gamma \geq 0$$

and $b b_i \in \mathcal{O}_{\widehat{v}}$. □ Subclaim 5.8

We can now take residues to find that

$$\overline{P}(x) = \prod_{i=1}^{n} (\overline{b} x - \overline{b b_i})$$

Since $\overline{P}$ is not constant, we get that $\overline{b} \neq 0$. So $b \in \mathcal{O}_{\widehat{v}}^{\times}$. So $b_i = \frac{1}{b} \cdot b b_i \in \mathcal{O}_{\widehat{v}}$. □ Claim 5.7

Taking residues, we find

$$\overline{P}(x) = \overline{c} \prod_{i=1}^{n} (x - \overline{b_i})$$

So $\overline{b_1}, \ldots, \overline{b_n}$ are the roots of $\overline{P}$ in $\overline{K}_v^{\text{alg}}$; say $\alpha = \overline{b_1}$.

Claim 5.9. *Any factor G of $\overline{P}$ in $\overline{K}_v[x]$ must have α as a root.*

Proof. Let u be a root of G; so $u = \overline{b_i}$. Let $\sigma \in \mathrm{Aut}(K^{\mathrm{alg}}/K)$ be such that $\sigma b_i = b_1$. Lift G to $g \in \mathcal{O}_v[x]$. Then

$$g(b_1) = g(\sigma b_i) = \sigma g(b_i) \in \sigma \mathcal{M}_{\widehat{v}} = \mathcal{M}_{\widehat{v}\circ\sigma} = \mathcal{M}_{\widehat{v}}$$

since $g \in K[x]$ and $\sigma \in \mathrm{Aut}(K^{\mathrm{alg}}/K)$. So

$$\overline{g(b_i)} = \overline{g}(\overline{b_i}) = G(u) = 0$$

So $g(b_i) \in \mathcal{M}_{\widehat{v}}$. But $\widehat{v} \circ \sigma = \widehat{v}$. So $g(b_1) \in \mathcal{M}_{\widehat{v}}$. So

$$G(\alpha) = \overline{g}(\overline{b_1}) = \overline{g(b_1)} = 0$$

□ Claim 5.9

Hence

$$\overline{P} = \overline{c} \prod_{i=1}^{n} (x - \alpha)$$

where $\alpha \in \overline{K}_v$. But α is a simple root, so $n = 1$. So $P = c(x - b)$ for some $c, b \in \mathcal{O}_v$ and $P(b) = 0$. So $\overline{P} = \overline{c}(x - \overline{b})$ with $\overline{b} = \alpha$.

□ Theorem 5.4

TODO 5. *Missing stuff*

We saw that given a value sfiel $\mathrm{s}(K, v)$ we can extend v to w on K^{sep}. If we then let $K^h = \mathrm{Fix}(\mathrm{stab}(\mathcal{O}_w))$ and $v^h = w \restriction K^h$, then (K^h, v^h) is the *Henselization*. This satisfies a universal property: if $(K', v') \supseteq (K, v)$ is Henselian then there is a unique embedding $f \colon K^h \to K'$ such that $f(\mathcal{O}_v) = \mathcal{O}_{v'} \cap f(L)$ and $f \restriction K = \mathrm{id}$. In diagram:

$$\begin{array}{ccc} (K^h, v^k) & \xrightarrow{f} & (K', v') \\ \subseteq\uparrow & \nearrow_{\subseteq} & \\ (K, v) & & \end{array}$$

Proposition 5.10. *Henselizations are immediate.*

Proof. We wish to show that (K^h, v^h) is an immediate extension of (K, v).

TODO 6. *"an"?*

Recall that $v^h = w \restriction K^h$ where w is an extension of v to K^{sep}.
Suppose $L \subseteq K^{\mathrm{sep}}$ is a finite Galois extension of K. We then have the following diagram:

$$\begin{array}{ccc} K^{\mathrm{sep}} & \xleftarrow{\subseteq} & L \\ \subseteq\uparrow & & \subseteq\uparrow \\ K^h & & K^h \cap L \\ \subseteq\uparrow & \nearrow_{\subseteq} & \\ K & & \end{array}$$

We let $H = \mathrm{Aut}(L/K)$; so $\mathrm{stab}_H(\mathcal{O}_{w\restriction L}) = \{\, \sigma \in H : \sigma \mathcal{O}_{w\restriction L} = \mathcal{O}_{w\restriction L} \,\}$.

Claim 5.11. $\mathrm{stab}_H(\mathcal{O}_{w\restriction L}) = \{\, \sigma \restriction L : \sigma \in \mathrm{stab}(\mathcal{O}_w) \leq \mathrm{Aut}(K^{\mathrm{sep}}/K) \,\}$.

Proof.

($\supseteq$) Well, L/K is normal, so for any $\sigma \in \mathrm{Aut}(K^{\mathrm{sep}}/K)$ we have $\sigma(L) = L$. If $\sigma \in \mathrm{stab}(\mathcal{O}_w)$ then $\sigma \restriction L \in H = \mathrm{Aut}(L/K)$ and $(\sigma \restriction L)(\mathcal{O}_{w\restriction L}) = (\sigma \restriction L)(\mathcal{O}_w \cap L) = \mathcal{O}_w \cap L$.

($\subseteq$) Suppose $\tau \in H$ has $\tau\mathcal{O}_{w\restriction L} = \mathcal{O}_{w\restriction L}$. Extend τ to $\sigma \in \mathrm{Aut}(K^{\mathrm{sep}}/K)$.sNow $\sigma\mathcal{O}_w$ is another extension of $\mathcal{O}_{w\restriction L}$. By the conjugacy theorem there is $\rho \in \mathrm{Aut}(K^{\mathrm{sep}}/L)$ such that $\rho\sigma\mathcal{O}_w = \mathcal{O}_w$; hence $\rho\sigma \in \mathrm{stab}(\mathcal{O}_w)$. But $(\rho\sigma)\restriction L = \sigma\restriction L = \tau$. □ Claim 5.11

By the claim, it follows that $K^h \cap L = \mathrm{Fix}(\mathrm{stab}(\mathcal{O}_{w\restriction L}))$, since $K^h = \mathrm{Fix}(\mathrm{stab}(\mathcal{O}_w))$. By a previous proposition, we get that $(K^h \cap L, w\restriction(K^h \cap L))$ is an immediate extension of (K, v). (Note that $w\restriction(K^h \cap L) = v^h \restriction L$.)

But any growth in the residue field or value grape from (K, v) to (K^h, v^h) would be witnessed by a finite extension. So (K^h, v^h) is an immediate extension of (K, v). □ Proposition 5.10

Example 5.12. Consider $(\mathbb{Q}, v_p) \subseteq (\mathbb{Q}^h, v_p^h) \subseteq (\mathbb{Q}^{\mathrm{alg}} \cap \mathbb{Q}_p, v_p) \subseteq (\mathbb{Q}_p, v_p)$. In fact $\mathbb{Q}^h = \mathbb{Q}^{\mathrm{alg}} \cap \mathbb{Q}_p$.

6 p-adically closed fields

We now abandon the textbook. A good reference for this material is "Formally p-adic fields" by Prestel and Roquette.

The goal is to understand $\mathbb{Q}_p$ axiomatically or abstractly.

Allegorically, $\mathbb{C}$ is an instance of an algebraically closed field: a field that has no proper algebraic extensions. An intrinsic (in fact, first-order) characterization is that every non-constant polynomial has a root.

Consider also separably closed fields: those that have no proper algebraic separable extension. This too has an intrinsic first-order axiomatization.

Also in this vein, we have that $\mathbb{R}$ is an instance of a real closed field. We first define a *formally real field* to be a field that admits a linear ordering compatible with the field structure; we then define a real closed field to be a field with no proper algebraic formally real field extension. A result of Tarski yields an intrinsic first-order axiomatization.

Can we do a similar study on p-adic fields? It turns out we can.

Definition 6.1. Fix a prime p. A valued field (K, v) is *formally p-adic* or *p-valued* if

1. $\overline{K}_v = \mathbb{F}_p$.
2. $v(p)$ is the least positive element of Γ_v.

Note that this definition is first-order.

Proposition 6.2. *The second condition is equivalent to requiring that $\mathcal{M}_v = p\mathcal{O}_v$.*

Proof.

($\Longrightarrow$) Suppose $0 \neq a \in \mathcal{M}_v$. By the second condition we have $v(a) \geq v(p)$. Hence $v(a) = v(p) + v(b)$ for some $b \in \mathcal{O}_v$, and $a = ubp$ for some $u \in \mathcal{O}_v^\times$; so $a \in (p)\mathcal{O}_v$.

($\Longleftarrow$) Suppose $\mathcal{M}_v = (p)\mathcal{O}_v$; suppose $a \in K$ has $v(a) > 0$. Then $a \in \mathcal{M}_v$, and $a = bp$ for some $b \in \mathcal{O}_v$; so $v(a) = v(b) + v(p) \geq v(p)$. So $v(p)$ is indeed the least positive element of Γ_v. □ Proposition 6.2

Remark 6.3. If (K, v) is a p-valued field, then $\mathrm{char}(K) = 0$. Indeed, if we had $\mathrm{char}(K) = p$, then $p = 0$ and $v(p) = \infty$, contradicting the second condition; if we had $\mathrm{char}(K) = q$ for $q \neq p$, then following the maps $\mathbb{Z} \to \mathcal{O}_v \to \mathbb{F}_p$, we find that $\overline{q} = 0$ in $\mathbb{F}_p$, a contradiction.

Fact 6.4. *In general for a valued field we have $(\mathrm{char}(K), \mathrm{char}(\overline{K}_v))$ must take one of the following forms: $(0, 0)$, (p, p), or $(0, p)$.*

Example 6.5.

1. $(\mathbb{Q}, v_p)$.
2. $(\mathbb{Q}_p, v_p)$.

3. Suppose (K, v) is a p-valued field. Extend v to w on $K(x)$ with $\Gamma_w = \Gamma_v \oplus \mathbb{Z}$ with the lexicographical ordering, and with $w(x) = (0, 1)$; then we have $\Gamma_v \hookrightarrow \Gamma_w$ by $\gamma \mapsto (\gamma, 0)$. So, by earlier results, we get that $\overline{K}_w = \overline{K}_v = \mathbb{F}_p$ and $w(p) = (v(p), 0)$ is the least possible element of Γ_w. So $(K(x), w)$ is a non-classical p-valued field.

4. Every immediate extension of a p-valued field is p-valued.

5. Any restriction of a p-valued field is p-valued.

Suppose (K, v) is p-valued. Let $\mathbb{Z}v(p)) = \langle v(p) \rangle \leq \Gamma_v$; this is a copy of $\mathbb{Z}$ in Γ_v.

Lemma 6.6. *$\mathbb{Z}v(p))$ is convex in Γ_v.*

Proof. Suppose $nv(p) < \gamma < (n+1)v(p)$ for some $\gamma \in \Gamma_v$. Then $0 < \gamma - nv(p) < v(p)$, contradicting the requirement that $v(p)$ be the least positive element of Γ_v. □ Lemma 6.6

Definition 6.7. A p-valued field (K, v) is *p-adically closed* if (K, v) has no proper p-valued algebraic extension.

This is exactly in analogy with algebraically closed fields and real closed fields, and somewhat in analogy with separably closed fields.

Remark 6.8. These exist by Zorn's lemma. Indeed, let $\mathcal{S}$ be the set of all p-valued algebraic, ordered by inclusion. This is closed under unions of chains; by Zorn's lemma there is a maximal element, which will be p-adically closed.

We'd like a first-order (intrinsic) axiomatization.

Proposition 6.9. *Every p-adically closed field is Henselian.*

Proof. Suppose (K, v) is p-adically closed. Let (K^h, v^h) be its Henselization. This is an immediate algebraic extension, and hence is p-valued. Since (K, v) is p-adically closed, we get that $K^h = K$; i.e. (K, v) is Henselian. □ Proposition 6.9

Remark 6.10. (K, v) is p-valued. Then $\mathbb{Z}v(p)$ is a convex subgrape. So $\Gamma_v/\mathbb{Z}v(p)$ has an induced ordering. (One checks that $\gamma + \mathbb{Z}v(p) \leq \alpha + \mathbb{Z}v(p)$ if and only if $\gamma \leq \alpha$ is well-defined and endows $\Gamma_v/\mathbb{Z}v(p)$ with the structure of an ordered abelian grape.) For example, if $\Gamma_v = \mathbb{Z}$, then $\Gamma_v/\mathbb{Z}v(p) = \{ 0 \}$.

We will show that if (K, v) is p-adically closed then $\Gamma_v/\mathbb{Z}v(p)$ is divisible.

Lemma 6.11. *Suppose (K, v) is p-valued. Suppose L/K is a finite extension and w is an extension of v to L. Then*

1. *Γ_w has only finitely many positive elements $\leq v(p)$. (Say j-many.)*

2. *Let $\pi \in L$ be such that $w(\pi)$ is the least positive element of Γ_w. (This exists by part (1).) Then $\mathbb{Z}w(\pi) \cap \Gamma_v = \mathbb{Z}v(p)$. So $\Gamma_v/\mathbb{Z}v(p) \hookrightarrow \Gamma_w/\mathbb{Z}w(\pi)$.*

3. *$e(\mathcal{O}_w/\mathcal{O}_v) = [\Gamma_w : \Gamma_v] = j \cdot [\Gamma_w/\mathbb{Z}w(\pi) : \Gamma_v/\mathbb{Z}v(p)]$.*

Proof.

1. If $0 < \beta < \beta' \leq v(p)$, then $0 < \beta' - \beta < \beta' \leq v(p)$; so $\beta' - \beta \notin \Gamma_v$, and $\beta + \Gamma_v \neq \beta' + \Gamma_v$. Hence the number of positive elements of Γ_w that are $\leq v(p)$ is at most $[\Gamma_w : \Gamma_v]$; in particular, we get that there are finitely many such elements.

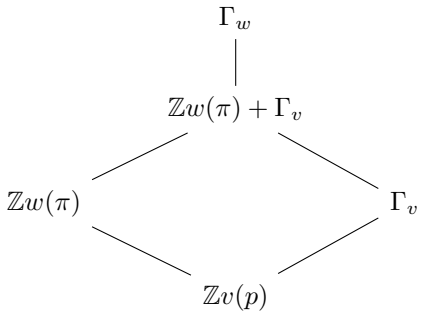
2. Since $w(\pi)$ is least positive, we have seen that $\mathbb{Z}w(\pi)$ is convex in Γ_w. But $v(p) \not> \mathbb{Z}w(\pi)$; so $v(p) \in \mathbb{Z}w(\pi)$, and $v(p) = kw(\pi)$ for some $k > 0$. So $\mathbb{Z}v(p) \subseteq \mathbb{Z}w(\pi) \cap \Gamma_v$.

   For the converse, suppose $\gamma \in \mathbb{Z}w(\pi) \cap \Gamma_v$. Then $-k\gamma \leq \gamma \leq k\gamma$. But $-k\gamma, k\gamma \in k\mathbb{Z}w(\pi) = \mathbb{Z}v(p)$. So, by convexity of $\mathbb{Z}v(p)$ in Γ_v, we get that $\gamma \in \mathbb{Z}v(p)$.

   So $\mathbb{Z}w(\pi) \cap \Gamma_v = \mathbb{Z}v(p)$, as desired.

3. Note that $w(\pi), 2w(\pi), \ldots, kw(\pi) = v(p)$ are precisely the positive elements of Γ_w that are $\leq v(p)$, by convexity of $\mathbb{Z}w(\pi)$ in Γ_w. So $j = k$.

   By part (2), we get an induced embedding $\Gamma_v/\mathbb{Z}v(p) \hookrightarrow \Gamma_w/\mathbb{Z}w(\pi)$. We thus get the following lattice:



   By the second isomorphism theorem, we get that

$$(\mathbb{Z}w(\pi) + \Gamma_v)/\Gamma_v \cong \mathbb{Z}w(\pi)/\mathbb{Z}v(p) \cong \mathbb{Z}w(\pi)/j\mathbb{Z}w(\pi)$$

   so $[\mathbb{Z}w(\pi) + \Gamma_v : \Gamma_v] = [\mathbb{Z}w(\pi) : j\mathbb{Z}w(\pi)] = j$. By the third isomorphism theorem we get

$$\Gamma_w/(\mathbb{Z}w(\pi) + \Gamma_v) \cong \Big(\Gamma_w/\mathbb{Z}w(\pi)\Big)/\Big((\mathbb{Z}w(\pi) + \Gamma_v)/\mathbb{Z}w(\pi)\Big) \cong \Big(\Gamma_w/\mathbb{Z}w(\pi)\Big)/\Big(\Gamma_v/\mathbb{Z}v(p)\Big)$$

   Hence $[\Gamma_w : \mathbb{Z}w(\pi) + \Gamma_v] = [\Gamma_w/\mathbb{Z}w(\pi) : \Gamma_v/\mathbb{Z}v(p)]$. So

$$e(\mathcal{O}_w/\mathcal{O}_v) = [\Gamma_w : \Gamma_v] = [\Gamma_w : \Gamma_w/(\mathbb{Z}w(\pi) + \Gamma_v)][\Gamma_w/(\mathbb{Z}w(\pi) + \Gamma_v) : \Gamma_v] = j[\Gamma_w/\mathbb{Z}w(\pi) : \Gamma_v/\mathbb{Z}v(p)]$$

   as desired. □ Lemma 6.11

Proposition 6.12. *Suppose (K, v) is p-adically closed. Then $\Gamma_v/\mathbb{Z}v(p)$ is divisible.*

Proof. Suppose not; we will construct a proper algebraic p-valued extension of (K, v).

Exercise 6.13. $\Gamma_v/\mathbb{Z}v(p)$ is not q-divisible for some prime q.

Pick $v(c) + \mathbb{Z}v(p) \in \Gamma_v/\mathbb{Z}v(p)$ such that there is no $\alpha \in \Gamma_v/\mathbb{Z}v(p)$ with $q\alpha = v(c) + \mathbb{Z}v(p)$. (Here $c \in K$.) Consider $L = K(t)$ where $t^q = c$. Extend v to w on L. Note that $qw(t) = w(c) = v(c)$; so $w(t) \in \Gamma_w \setminus \Gamma_v$.

Now L/K is a proper algebraic extension; we show that (L, w) is p-valued. By Lemma 6.11, we have that $j = |\{\, \gamma \in \Gamma_w : 0 < \gamma \leq v(p) \,\}|$ is finite. Letting $\pi \in L$ be such that $w(\pi)$ is the least positive element of Γ_w, we get that $\mathbb{Z}v(p) = j\mathbb{Z}w(\pi)$ and $\mathbb{Z}w(\pi) \cap \Gamma_v = \mathbb{Z}v(p)$; furthermore that $[\Gamma_w : \Gamma_v] = j[\Gamma_w/\mathbb{Z}w(\pi) : \Gamma_v/\mathbb{Z}v(p)]$.

Claim 6.14. *$j = 1$; so $w(\pi) = v(p)$ is the least positive element of Γ_w.*

Proof. In $\Gamma_w/\mathbb{Z}w(\pi)$, we have

$$\begin{aligned} q(\underbrace{w(t) + \mathbb{Z}w(\pi)}_{\alpha}) &= qw(t) + \mathbb{Z}w(\pi) \\ &= v(c) + \mathbb{Z}w(\pi) \\ &= v(c) + \mathbb{Z}v(p) \\ &\in \Gamma_v/\mathbb{Z}v(p) \end{aligned}$$

$\Gamma_v/\mathbb{Z}v(p) \subseteq \Gamma_w/\mathbb{Z}v(\pi)$, with $q\alpha$ on the left and α on the right.

TODO 7. *What?*

Since $\alpha \neq 0$ in $\Big(\Gamma_w/\mathbb{Z}w(\pi)\Big)/\Big(\Gamma_v/\mathbb{Z}v(p)\Big)$. But $q\alpha = 0$; so $\Big(\Gamma_w/\mathbb{Z}w(\pi)\Big)/\Big(\Gamma_v/\mathbb{Z}v(p)\Big)$ has an element of order q (represented by α). So

$$jq \leq j[\Gamma_w/\mathbb{Z}w(\pi) : \Gamma_v/\mathbb{Z}v(p)] = [\Gamma_w : \Gamma_v] \leq [L : K] = q$$

So $j = 1$, as desired. □ Claim 6.14

So $w(\pi) = v(p)$ is the least positive element of Γ_w. But $e(\mathcal{O}_w/\mathcal{O}_v) = [\Gamma_w : \Gamma_v] = [L : K]$. So $[\overline{K}_w : \overline{K}_v] = 1$. So $\overline{K}_w = \overline{K}_v = \mathbb{F}_p$. So (L, w) is p-valued. □ Proposition 6.12

Theorem 6.15. *Suppose (K, v) p-valued. Then (K, v) is p-adically closed if and only if it is Henselian and $\Gamma_v/\mathbb{Z}v(p)$ is divisible.*

Proof.

($\implies$) By Proposition 6.9 and Proposition 6.12.

□ Theorem 6.15

TODO 8. *Missing stuff. (Mostly proof of the above.)*

Example 6.16.

1. $(\mathbb{Q}_p, v_p)$ is p-adically closed: it's p-valued, it's Henselian by completeness, and $\Gamma_{v_p}/\mathbb{Z}v(p) = \mathbb{Z}/\mathbb{Z} = 0$ is divisible.
2. $(\mathbb{Q}, v_p)^h = (\mathbb{Q}_p \cap \mathbb{Q}^{\text{alg}}, v_p)$ is p-adically closed: it's p-valued as the restriction of a p-valued field, it's Henselian as it is algebraically closed in $\mathbb{Q}_p$ (which is Henselian), and $\Gamma_{v_p} = \mathbb{Z}$.
3. Let
$$K = \bigcup_{m>0} \underbrace{\mathbb{Q}_p\left(\left(t^{\frac{1}{m}}\right)\right)}_{\text{Laurent series}}$$
These are the *Puiseaux series over* $\mathbb{Q}_p$. We extend v_p on $\mathbb{Q}_p$ to K by
$$v\left(\sum_{i=n}^{\infty} a_i t^{\frac{i}{m}}\right) = \left(\frac{n}{m}, v_p(a_n)\right) \in \mathbb{Q} \times \mathbb{Z}$$
where $a_n \neq 0$ and $\mathbb{Q} \times \mathbb{Z}$ is given the lexicographical ordering.
   - This is p-valued. Indeed, $v(p) = (0, v_p(p)) = (0, 1)$ is the least positive element of $\mathbb{Q} \times \mathbb{Z}$. Further observe that
   $$\sum_{i=n}^{\infty} a_i t^{\frac{i}{m}} \in \mathcal{O}_v$$
   if and only if $n > 0$ or $n = 0$ and $a_{\in}\mathcal{O}_{v_p} = \mathbb{Z}_p$; similarly,
   $$\sum_{i=n}^{\infty} a_i t^{\frac{i}{m}} \in \mathcal{M}_v$$
   if and only if $n > 0$ or $n = 0$ and $a_n \in \mathcal{M}_{v_p} = p\mathbb{Z}_p$. Hence $\mathcal{O}_v/\mathcal{M}_v = \mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$.
   - $\Gamma_v/\mathbb{Z} = \mathbb{Q}$ is divisible.
   - It is Henselian. To see this, one examines the following diagram:
   $$\begin{array}{ccc} \mathbb{Q}_p\left(\left(t^{\frac{1}{m}}\right)\right) & \xrightarrow{\text{res}_w} & \mathbb{Q}_p \\ & \searrow^{\text{res}_v} & \downarrow{\scriptstyle \text{res}_{v_p}} \\ & & \mathbb{F}_p \end{array}$$
   where
   $$w\left(\sum_{i=n}^{\infty} a_i t^{\frac{i}{m}}\right) = n$$

We now generalize the second example to:

Proposition 6.17. *If (L, w) is p-adically closed and $K \subseteq L$ is relatively algebraically closed, then $(K, w \restriction K)$ is p-adically closed.*

We first need another tool: p-adic expansions in p-valued fields.

Suppose (K, v) is p-valued and $a \in \mathcal{O}_v$. Let $a_0 = \overline{a} \in \mathbb{F}_p$; we regard $0 \leq a_0 \leq p-1$. So $a - a_0 \in \mathcal{O}_v$, and in particular

$$\overline{a - a_0} = \overline{a} - \overline{a_0} = \overline{a} - a_0 = 0$$

and $a - a_0 = \mathcal{M}_v = (p)\mathcal{O}_{v_p}$. So $\frac{a-a_0}{p} \in \mathcal{O}_v$. Let

$$a_1 = \overline{\left(\frac{a - a_0}{p}\right)} \in \mathbb{F}_p$$

Then

$$\overline{\left(\frac{a - a_0}{p} - a_1\right)} = 0$$

and

$$v\left(\frac{a - a_0 - a_1 p}{p}\right) \geq v(p)$$

so $v(a - a_0 - a_1 p) \geq 2v(p)$.

In general for any m we get $a_0, \ldots, a_{m-1} \in \mathbb{F}_p$ such that $v(a - a_0 - a_1 p - a_2 p^2 - \cdots - a_{m-1}p^{m-1}) \geq mv(p)$. So the $\sum_{i=1}^{m-1} a_i p^i$ are successively better approximations to a as $m \to \infty$. If we squint hard enough, we can kind of pretend that we're approximating elements of $\mathcal{O}_v$ by p-adic integers:

$$\mathbb{Z}_p \ni \sum_{i=0}^{\infty} a_i p^i \approx a \in \mathcal{O}_v$$

Lemma 6.18. *Suppose (K, v) is p-valued and (L, w) is a p-valued Henselian extension. Suppose $a \in L$ and $n \in \mathbb{N}$ such that $w(a) \in \Gamma_v$. Then there is $c \in K$ and $u \in \mathcal{O}_w^\times$ such that $a = cu^n$.*

Proof. By assumption we have $w(a) = w(b) \in \Gamma_v$ for some $b \in K$. If we prove $\frac{a}{b} = cu^n$ for some $c \in K$ then $a = bcu^n$, and $bc \in K$, so we're done.

We may thus assume that $a \in \mathcal{O}_w^\times$. Let $c \in \mathbb{Z}$ be such that $w(a - c) \geq mv(p)$ (where we fix m such that $mv(p) > 2v(n)$). We identify $\mathbb{Z}$ with $\mathbb{Z}v(p) \subseteq \Gamma_v \subseteq \Gamma_w$; i.e. we normalize so that $v(p) = 1$. So $w(a - c) \geq m > 2v(n)$; so

$$w\left(\frac{a}{c} - 1\right) = w\left(\frac{a - c}{c}\right) = w(a - c) - w(c) = w(a - c) \geq m$$

(since $c = \sum_{i=0}^{m-1} a_i p^i$ and $a_0 = \overline{a} \neq 0$ since $a \in \mathcal{O}_w^\times$; so $v(c) = 0$ since $p \nmid c$.) Let $p(x) = x^n - \frac{a}{c}$. Then

$$\begin{aligned} w(p(1)) &\geq m \\ &> 2v(p'(1)) \\ w(p'(1)) &= v(n) \end{aligned}$$

By Hensel-Rychik in (L, w), we now get a root $u \in \mathcal{O}_w$ with $\overline{u} = \overline{1} = 1$ and $u \in \mathcal{O}_w^\times$; in particular, $u^n = \frac{a}{c}$. □ Lemma 6.18

Corollary 6.19. *Suppose (K, v) is p-valued and (L, w) is a p-valued Henselian extension. Suppose further that K is relatively algebraically closed in L. Then Γ_w/Γ_v is torsion-free.*

Proof. Suppose $b \in L$ satisfies $nw(b) \in \Gamma_v$; i.e. $w(b)$ is n-torsion in Γ_w/Γ_v. Let $a = b^n \in L$; so $w(a) = nw(b) \in \Gamma_v$. By the previous lemma, we get that $a = cu^n$ for some $c \in K$ and some $u \in \mathcal{O}_w^\times$ with $w(u) = 0$. So $b^n = cu^n$, and $\left(\frac{b}{u}\right)^n = c \in K$. So $\frac{b}{u} \in L \cap K^{\mathrm{alg}} = K$; so $w(b) = w(b) - w(u) = w\left(\frac{b}{u}\right) \in \Gamma_v$. □ Corollary 6.19

Corollary 6.20. *Suppose (L, w) is p-adically closed, $K \subseteq L$, and $K^{\mathrm{alg}} \cap L = K$. Then $(K, w \restriction K)$ is p-adically closed.*

Proof. Let $v = w \restriction K$. Then (K, v) is p-valued as a restriction of (L, w); it is Henselian since (L, w) is and $K^{\text{alg}} \cap L = K$. It remains to check divisibility of $\Gamma_v/\mathbb{Z}$. But $\Gamma_w/\mathbb{Z}$ is divisible, and

$$\Big(\Gamma_w/\mathbb{Z}\Big)/\Big(\Gamma_v/\mathbb{Z}\Big) \cong \Gamma_w/\Gamma_v$$

which is torsion-free.

Claim 6.21. *If G is a divisible abelian grape, $H \leq G$, and G/H is torsion free, then H is divisible.*

Proof. Suppose $h \in H$. By divisibility of G there is $g \in G$ with $ng \in H$. So g is torsion in G/H, and G/H is torsion-free; so $g \in H$. So H is n-divisible. □ Claim 6.21

So $\Gamma_v/\mathbb{Z}$ is divisible. □ Corollary 6.20

7 Completeness and decidability of $\mathbb{Q}_p$

Let ACF_0 be the axioms of algebraically closed fields of characteristic 0.

Fact 7.1 (Tarski, Completeness of ACF_0)**.** *Suppose σ is a first-order statement. Then σ is true in $\mathbb{C}$ if and only if σ is a consequence of* ACF_0.

In particular, if σ is true in $\mathbb{C}$, then it is true in every algebraically closed field of characteristic 0.

Let RCF be the axioms of real closed fields.

Fact 7.2 (Tarski)**.** *Suppose σ is a first-order statement. Then σ is true in $\mathbb{R}$ if and only if σ is a consequence of* RCF.

We get a similar fact for separably closed fields of characteristic p, SCF_p; this is due to Ersov.

From these facts, we get *decidability* of $\mathbb{C}$ and $\mathbb{R}$; i.e. given a first-order statement, one can decide whether it is true in $\mathbb{C}$ or not. Likewise with $\mathbb{R}$.

Gödel's incompleteness theorem implies that the sae is not true of $(\mathbb{Z}, 0, 1, +, -, \times)$.

We will explain how the axios of p-adically closed fields is a complete axiomatization of $\mathbb{Q}_p$.

First, a vague description of first-order statements in a valued field (K, v):

- Finitary.
- Involve:
  - $+, -, \times, 0, 1$ in K.
  - $+, -, \times, 0, 1$ in $\overline{K}_v$.
  - $+, -, <, 0$ in Γ_v.
  - v and res_v.
- Allow quantifying over elements (*not* subsets) of K, $\overline{K}_v$, and Γ_v.
- Allow logical operations: $\wedge$, $\vee$, $\neg$, $\to$, and $\leftrightarrow$.

Example 7.3. We want axioms saying $\Gamma_v/\mathbb{Z}$ is divisible. (We have normalized $v(p) = 1$ here.) Fix $m \geq 1$; we want σ_m asserting that $\Gamma_v/\mathbb{Z}$ is m-divisible. We let

$$\sigma_m = (\forall \gamma \in \Gamma_v)(\exists \lambda \in \Gamma_v)((m\lambda - \gamma = 0) \vee (m\lambda - \gamma = 1) \vee \cdots \vee (m\lambda - \gamma = (m-1)))$$

Claim 7.4. *$\Gamma_v/\mathbb{Z}$ is m-divisible if and only if σ_m holds.*

Proof.

($\Longleftarrow$) Clear.

($\Longrightarrow$) Suppose $\Gamma_v/\mathbb{Z}$ is m-divisible. Suppose $\gamma \in \Gamma_v$; pick $\lambda' \in \Gamma$ such that $m\lambda' - \gamma = n = qm + r$ for some q and some $0 \leq r < m$. Then $m(\lambda' - q) - \gamma = r$ and $0 \leq r < m$; so we may take $\lambda = \lambda' - q \in \Gamma_v$.

□ Claim 7.4

Hence $\{ \sigma_m : m \geq 1 \}$ expresses divisibility of Γ_v.

Example 7.5. We want to axiomatize being p-valued:

- $(v(p) > 0) \wedge \nexists\, \gamma (0 < \gamma < v(p))$.
- $\forall x (\mathrm{res}_v(x) = 0 \vee \mathrm{res}_v(x) = 1 \vee \cdots \vee \mathrm{res}_v(x) = p - 1)$.
- $p = 0$ in $\overline{K}_v$.

Example 7.6. Suppose (K, v) is p-valued; we wish to express that (K, v) is Henselian. For $m \geq 1$, we will pick τ_m to express that for every polynomial $p \in \mathcal{O}_v[x]$ of degree m and every simple root $\overline{p} \in \overline{K}_v[x]$ there is a lifting of the siple root to a root of p in $\mathcal{O}_v$. Then (K, v) will be Henselian if and only if $\{ \tau_m : m \geq 1 \}$ holds.

We define τ_m to be the following statement:

$$
\begin{aligned}
&\forall a_0, \ldots, a_m \in K \\
&\forall \alpha \in \overline{K}_v \\
&\Big(\bigwedge_{i=0}^{m} v(a_i) \geq 0 \\
&\wedge a_m \neq 0 \\
&\wedge \overline{a_m} \alpha^m + \cdots + \overline{a_0} = 0 \\
&m\overline{a_m} \alpha^{m-1} + \cdots + \overline{a_1} \neq 0 \Big) \\
&\to \exists b \in K \\
&\Big(\overline{b} = \alpha \wedge a_m b^m + \cdots + a_0 = 0 \Big)
\end{aligned}
$$

Hence being a p-adically closed valued field is first-order axiomatizable in the language of valued fields.

We now introduce ultraproducts of valued fields. Suppose (K_i, v_i) are valued fields for $i < \omega$. We might hope to define a product by

$$
\begin{aligned}
K' &= \prod_{i<\omega} K_i \\
\Gamma' &= \prod_{i<\omega} \Gamma_i \\
v' &: (K')^\times \to \Gamma'
\end{aligned}
$$

But K' is not an integral domain, Γ' is not an ordered abelian grape, and v' is not a valuation.

However, if we mod out be the equivalence relation of being "almost everywhere equal", then we do get a valued field. We make this precise with the following definition:

Definition 7.7. An *ultrafilter* on ω is some $\mathcal{F} \subseteq \mathcal{P}(\omega)$ satisfying:

1. $\emptyset \notin \mathcal{F}$ and $\omega \in \mathcal{F}$.
2. If $U, V \in \mathcal{F}$ then $U \cap V \in \mathcal{F}$.
3. If $U \in \mathcal{F}$ and $V \supseteq U$ then $V \in \mathcal{F}$.
4. If $U \in \mathcal{F}$ then one of U or $\omega \setminus U$ lies in $\mathcal{F}$.

If we omit the final axiom, we get the definition of a *filter* on ω. We say an ultrafilter is *non-principal* if it contains the Fréchet filter.

Exercise 7.8. An ultrafilter is principal if and only if it does not contain a singleton.

Example 7.9. The Fréchet filter is given by $U \in \mathcal{F}$ if and only if $\omega \setminus U$ is finite.

Exercise 7.10. The ultrafilters are precisely the maximal filters under $\subseteq$.

So, by Zorn's lemma, there is an ultrafilter on ω containing the Fréchet filter; i.e. there is a non-principal ultrafilter on ω.

We are now in a position to define ultraproducts of valued fields. Suppose (K_i, v_i) are valued fields for $i < \omega$. Fix an ultrafilter $\mathcal{U} \subseteq \mathcal{P}(\omega)$. Define

$$\begin{aligned} K^* &= \prod_{\mathcal{U}} K_i \\ &= \prod_{i<\omega} K_i/\sim \end{aligned}$$

where $(a_i : i < \omega) \sim (b_i : i < \omega)$ if $\{ i < \omega : a_i = b_i \} \in \mathcal{U}$. We call K^* the *ultraproduct* of the (K_i, v_i) (with respect to $\mathcal{U}$). Then K^* is a field under

$$\begin{aligned} 0 &= [(0, 0, \ldots)] \\ 1 &= [(1, 1, \ldots)] \\ [(a_i : i < \omega)] + [(b_i : i < \omega)] &= [(a_i + b_i : i < \omega)] \\ [(a_i : i < \omega)] \cdot [(b_i : i < \omega)] &= [(a_i b_i : i < \omega)] \end{aligned}$$

To see that addition is well-defined, suppose

$$\begin{aligned} [(a_i : i < \omega)] &= [(a'_i : i < \omega)] \\ [(b_i : i < \omega)] &= [(b'_i : i < \omega)] \end{aligned}$$

Then $I = \{ i < \omega : a_i = a'_i \} \cap \{ i < \omega : b_i = b'_i \} \in \mathcal{U}$ as the intersection of elements of $\mathcal{U}$. But for $i \in I$ we have $a_i + b_i = a'_i + b'_i$; so $[(a_i + b_i : i < \omega)] = [(a'_i + b'_i : i < \omega)]$.

Remark 7.11. Every non-zero element of K^* is invertible. Indeed, if $[(a_i : i < \omega)] \neq 0$ then $I = \{ i < \omega : a_i = 0 \} \notin \mathcal{U}$, and $\omega \setminus I \in \mathcal{U}$. Now let

$$b_i = \begin{cases} a_i^{-1} & \text{if } i \notin I \\ 0 & \text{else} \end{cases}$$

Then $[(b_i : i < \omega)][(a_i : i < \omega)] = [(a_i b_i : i < \omega)]$. But for $i \in \omega \setminus I$ we have $a_i b_i = a_i a_i^{-1} = 1$. So, since $\omega \setminus I \in \mathcal{U}$, we get that $[(a_i b_i : i < \omega)] = 1$. So $[(b_i : i < \omega)] = [(a_i : i < \omega)]^{-1}$.

We similarly get that $\Gamma^* = \prod_{\mathcal{U}} \Gamma_i$ is an ordered abelian grape, where $[(\gamma_i : i < \omega)] < [(\lambda_i : i < \omega)]$ if $\{ i < \omega : \gamma_i < \lambda_i \} \in \mathcal{U}$.

Remark 7.12. Γ^* is linearly ordered. Indeed, if $[(\gamma_i : i < \omega)], [(\lambda_i : i < \omega)] \in \Gamma^*$, then one of $\{ i < \omega : \gamma_i < \lambda_i \}$ and $\{ i < \omega : \gamma_i \geq \lambda_i \}$ is in $\mathcal{U}$. Hence either $[(\gamma_i : i < \omega)] < [(\lambda_i : i < \omega)]$ or $[(\gamma_i : i < \omega)] \geq [(\lambda_i : i < \omega)]$.

We also have

$$\begin{aligned} v^* \colon K^* \setminus \{ 0 \} &\to \Gamma^* \\ [(a_i : i < \omega)] &\mapsto [(\gamma_i : i < \omega)] \end{aligned}$$

where

$$\gamma_i = \begin{cases} v(a_i) & \text{if } a_i \neq 0 \\ 0 & \text{else} \end{cases}$$

This defines a valuation on K^*; one can check that

$$\begin{aligned} \mathcal{O}_{v^*} &= \prod_{\mathcal{U}} \mathcal{O}_{v_i} \\ \overline{K^*}_{v^*} &= \prod_{\mathcal{U}} \overline{K}_{v_i} \end{aligned}$$

We thus get a valued field (K^*, v^*).

We now come to ultrapowers:

Definition 7.13. Suppose (K, v) is a valued field. We define the *ultrapower* of (K, v) to be

$$(K, v)^{\mathcal{U}} = \prod_{\mathcal{U}} (K, v)$$

i.e. the ultraproduct with $(K_i, v_i) = (K, v)$.

If (K, v) is p-adically closed, then so is (K, v^*). One could check the axioms; this also follows from the following:

Theorem 7.14 (Łoś's theorem)**.** *Suppose (K_i, v_i) are valued fields for $i < \omega$. Let (K^*, v^*) be the ultraproduct with respect to some ultrafiilter $\mathcal{U}$. Suppose σ is any first-order statement about valued fields. Then σ holds in (K^*, v^*) if and only if $\{ i < \omega : \sigma \text{ holds in } (K_i, v_i) \} \in \mathcal{U}$.*

Then $(K, v)^{\mathcal{U}}$ is p-adically closed since being p-adically closed is first-order axiomatizable.

Remark 7.15. Suppose (K, v) is a valued field; let $(K^*, v^*) = (K, v)^{\mathcal{U}}$. Then there is an embedding $(Kv) \subseteq (K^*, v^*)$ where

$$\begin{aligned} K &\hookrightarrow K^* \\ a &\mapsto [(a : i < \omega)] \\ \Gamma_v &\hookrightarrow \Gamma_{v^*} \\ \gamma &\mapsto [(\gamma : i < \omega)] \end{aligned}$$

Under this identification we get $\mathcal{O}_{v^*} \cap K = \mathcal{O}_v$.

Remark 7.16. Suppose $n < \omega$. Let $\mathcal{U} = \{ I \subseteq \omega : n \in I \}$; this is a principal ultrafilter. Then

$$\prod_{\mathcal{U}} (K_i, v_i) \cong (K_n, v_n)$$

and in particular

$$(K, v)^{\mathcal{U}} \cong (K, v)$$

Recall that $\mathcal{U}$ is non-principal if and only if all cofinite sets are in $\mathcal{U}$; the intuition is that if $\mathcal{U}$ is non-principal then $(K, v) \subseteq (K^*, v^*)$ is a *very* rich extension.

In particular, one can prove:

Fact 7.17 (Embedding theorem)**.** *Suppose $(K, v) \subseteq (L, w)$ are p-adically closed fields. Let $\mathcal{U}$ be a non-principal ultrafilter on ω. Consider the ultrapower of (L, w):*

$$(K, v) \subseteq (L, w) \subseteq (L, w)^{\mathcal{U}}$$

Then for any countable p-valued extension (K', v') of (K, v), there is an embedding $(K', v') \hookrightarrow (L, w)$ over (K, v).

The proof uses p-valued field theory plus basic model-theoretic properties of non-principal ultraproducts (namely saturation).

Theorem 7.18 (Completeness of the theory of p-adically closed fields)**.** *Suppose σ is a first-order sentence in the language of valued fields, then σ is either true in every p-adically closed field or false in every p-adically closed field.*

Sketch of proof. Suppose (L_1, v_1) and (L_2, v_2) are p-adically closed; normalize so $v_1(p) = v_2(p) = 1$. Suppose σ is true in (L_1, v_1). We want to show that σ is true in (L_2, v_2). Since $\mathrm{char}(L_1) = \mathrm{char}(L_2) = 0$, we get that $\mathbb{Q} \subseteq L_1 \cap L_2$, with $v_1 \restriction \mathbb{Q} = v_2 \restriction \mathbb{Q} = v_p$.

Consider $K_1 = \mathbb{Q}^{\mathrm{alg}} \cap L_1$ with $w_1 = v_1 \restriction K_1$; so $(\mathbb{Q}, v_p) \subseteq (K_1, w_1) \subseteq (L_1, v_1)$.

Claim 7.19. *$(K_1, w_1) \supseteq (\mathbb{Q}, v_p)$ is immediate.*

Proof. Both are p-valued, so both residue fields are $\mathbb{F}_p$. Since $K_1/\mathbb{Q}$ is algebraic, we get that $\Gamma_{w_1}/\Gamma_{v_1} = \Gamma_w/\mathbb{Z}$ is torsion. By Proposition 6.17, since K_1 is algebraically closed in L_1 and L_1 is p-adically closed, we get that K_1 is p-adically closed; so $\Gamma_w/\mathbb{Z}$ is divisible. So $\Gamma_w/\mathbb{Z}$ is trivial, and $\Gamma_w = \mathbb{Z}$. □ Claim 7.19

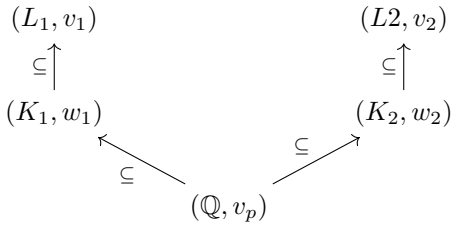
Claim 7.20. *(K_1, w_1) is a Henselization of $(\mathbb{Q}, v_p)$.*

Proof. Well, (K_1, w_1) is Henselian as it is p-adically closed. By the universal property, we have

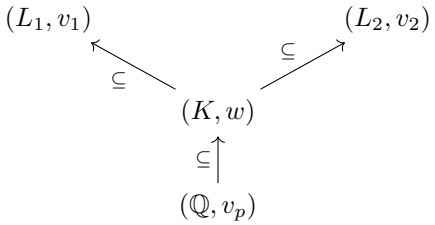
$$(\mathbb{Q}, v_p) \subseteq (\mathbb{Q}^h, v_p^h) \subseteq (K_1, w_1)$$

Since $(\mathbb{Q}, v_p) \subseteq (K_1, w_1)$ is an immediate and algebraic extension, we get that so too is $(\mathbb{Q}^h, v_p^h) \subseteq (K_1, w_1)$. By **??**, every p-valued Henselian field has no proper immediate algebraic extensions. So $\mathbb{Q}^h = K_1$. □ Claim 7.20

We now have the following diagram:



with $K_1 = \mathbb{Q}^{\text{alg}} \cap L_i$ are both Henselizations of $(\mathbb{Q}, v_p)$. So, by uniqueness of Henselizations, we may assume the following picture:



with K, L_1, L_2 all p-adically closed; so $K_1 = K_2 = K = \mathbb{Q}^{\text{alg}} \cap L_1 = \mathbb{Q}^{\text{alg}} \cap L_2$.

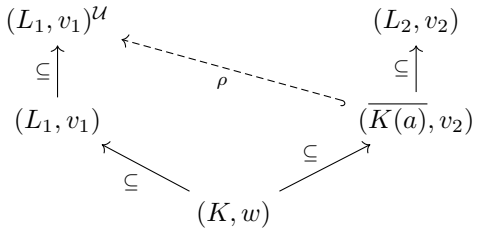
We now begin to wave our hands. Suppose σ is of the for $\forall x \exists y \varphi(x, y)$, where $\varphi(x, y)$ is "quantifier-free"; i.e. is an algebraic valued-field-theoretic condition on x and y.

Example 7.21. $\varphi(x, y)$ might be

- $v(P(x, y)) > v(Q(x, y))$ where P and Q are polynomials over $\mathbb{Q}$,
- $(v(P(x, y)) \geq 0) \wedge R(\text{res}(P(x, y))) = 0$ where $R \in \mathbb{F}_p[z]$, or
- $P(x, y) \neq 0$.

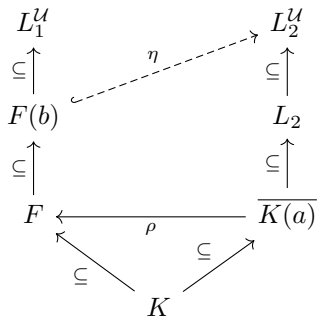
We assume $\forall x \exists y \varphi(x, y)$ holds in (L_1, v_1); we wish to show it holds in (L_2, v_2).

Suppose $a \in L_2$; we wish to show $\exists y \varphi(a, y)$ holds in (L_2, v_2). Let $\overline{K(a)} = K(a)^{\text{alg}} \cap L_2$; this is a countable p-valued extension of (K, w), so we can apply the embedding theorem. Namely, we have ρ as in the following diagram:



where $\mathcal{U}$ is any non-principal ultrafilter. Since $\forall x \exists y \varphi(x, y)$ holds in (L_1, v_1), Łoś's theorem yields that it also holds in $(L_1, v_1)^{\mathcal{U}}$. In particular, $\exists y \varphi(\rho(a), y)$ holds in $(L_1, v_1)^{\mathcal{U}}$. So there is $b \in L_1^{\mathcal{U}}$ such that $(\rho(a), b)$ satisfy $\varphi(x, y)$ in $(L_1, v_1)^{\mathcal{U}}$.

Now let $F = \rho(\overline{K(a)})$; so F is p-adically closed. Consider now $F(b)$, which is a countable p-valued extension of F. We may again apply the embedding theorem to get η as in the following diagram:



Now $(\rho(a), b)$ satisfy $\varphi(x, y)$ in $(F(b), v_1)$; so $(\eta(\rho(a)), \eta(b)) = (a, \eta(b))$ satisfy $\varphi(x, y)$ in $(L_2, v_2)^{\mathcal{U}}$; i.e. $\exists y \varphi(a, y)$ holds in $(L_2, v_2)^{\mathcal{U}}$. So, by Łoś's theorem, we get that $\exists y \varphi(a, y)$ holds in (L_2, v_2). So $\forall x \exists y \varphi(x, y)$ holds in (L_2, v_2).

If φ has more alternating quantifiers, one needs more applications of the embedding theorems.

□ Theorem 7.18

Corollary 7.22. *Any first-order sentence true in $\mathbb{Q}_p$ is a consequence of the axioms of p-adically closed fields.*

Proof. By Gödel's completeness theorem of first-order logic, if σ holds in every p-adically closed field, then it can be proven from the axioms. □ Corollary 7.22

Hence, like $\mathbb{C}$ and $\mathbb{R}$, we see that $\mathbb{Q}_p$ is a decidable theory.