Number theory, 2024-2025

Qing Liu*

November 28, 2024

Contents

*based on lecture notes of Olivier Brinon and of Pascal Autissier

1 Valued fields

In this chapter, K denotes a field.

1.1 Absolute values

Definition 1.1 An *absolute value* on K is a map $|\ |: K \to \mathbb{R}_+$ such that:
(a) $\forall x \in K, |x| = 0$ if and only if $x = 0$;
(b) $\forall (x, y) \in K^2, |xy| = |x||y|$;
(c) $\forall (x, y) \in K^2, |x + y| \leqslant |x| + |y|$ (triangle inequality).
A field endowed with an absolute value is called a *valued field*.

Remark 1.2 Let $|\ |$ be an absolute value on K. By (a) and (b), $|\ |: K^* \to \mathbb{R}_+^*$ is a group homomorphism. For any $x \in K$, as $|-x|^2 = |(-x)^2| = |x|^2$, we have $|-x| = |x|$.

Example 1.3
1. The *trivial* absolute value on K is given by $|0|_0 = 0$ and $|x|_0 = 1$ for all $x \in K^*$.
2. The usual absolute value on $\mathbb{C}$. It will be denoted by $|\ |_\infty$.

A way to produce absoulte values is by using valuations.

Definition 1.4 A *valuation (of rank one)* on K is a map $v : K^* \to \mathbb{R}$ such that

1. $v(xy) = v(x) + v(y)$ for all $x, y \in K^*$ (in particular $v(1) = 0$);
2. if $x + y \neq 0$, then
$$v(x + y) \geq \min\{v(x), v(y)\}.$$

It is convenient to extend v to $K \to \mathbb{R} \cup \{+\infty\}$ by taking 0 to $+\infty$. Then the above conditions hold for all $x, y \in K$.

Example 1.5 For any prime number p, we have the p-adic valuation v_p on $\mathbb{Q}^*$ defined by $v_p(r) = k$ if $r = p^k a/b$ with $a, b \in \mathbb{Z} \setminus p\mathbb{Z}$,

Lemma 1.6. *Fix a real number $0 < t < 1$. If $v : K \to \mathbb{R} \cup \{+\infty\}$ is a valuation, then $x \mapsto t^{v(x)}$ is an absolute value on K.*

Over $\mathbb{Q}$, usually the absoulte value associated to the p-adic valuation is defined by $|x|_p = (1/p)^{v_p(x)}$. This is the *p-adic absolute value.*

Definition 1.7 A absolute value $|\ |$ on K is *ultrametric* if for all $x, y \in K$ we have the (ultrametric) inequality

$$|x + y| \leq \max\{|x|, |y|\}.$$

This is stronger than the triangular inequality.

The usual absolute value $|\ |_\infty$ on $\mathbb{R}$ is not ultrametric, while the absolute value (including the trivial one) defined by a valuation as above is ultrametric.

Proposition 1.8. *There is a one-to-one correspondance between the valuations and the ultrametric absolute values on K :*

$$v \mapsto (1/2)^v, \quad |\ | \mapsto -(\ln 2)^{-1} \ln |.|$$

Definition 1.9 Let $(K, |.|)$ be a valued field. Then K is said to be *archimedean* if for any $x \in K^*$ and for any $c \in \mathbb{R}$, there exists $n \in \mathbb{N}$ such that $|nx| \geq c$. (We really mean $|nx|$, not $n|x|$).

Proposition 1.10. *Consider an absolute value $|\ |$ on K. Then the following properties are equivalent:*

1. *the absolute value $|\ |$ is not archimedean;*
2. *the set $\{|n.1_K| \mid n \in \mathbb{Z}\} \subset \mathbb{R}$ is bounded;*
3. *$|n.1_K| \leq 1$ for all $n \in \mathbb{Z}$;*
4. *$|\ |$ is ultrametric.*

   So the absolute values are either archimedean or ultrametric.

Proof. (1) $\Longrightarrow$ (2). There exists $x_0 \in K^*$ and $c > 0$ such that for all $n \in \mathbb{N}$, we have $|nx_0| \leq c$. So $|\pm n.1_K| \leq c/|x_0|$.

(2) $\Longrightarrow$ (3). Fix $n \in \mathbb{Z}$. As the sequence $(|n.1_K|^m)_m = (|n^m.1_K|)_m$ is bounded, we have $|n.1_K| \leq 1$.

(3) $\Longrightarrow$ (4). Let $x, y \in K$ with $|x| \leq |y|$ and $y \neq 0$. Dividing the ultrametric inequality (to prove) by $|y|$, we can suppose $y = 1$ and $|x| \leq 1$. We need to show that

$$|1 + x| \leq 1.$$

For all $n > 0$, we have

$$|1 + x|^n = |(1 + x)^n| = |\sum_{0 \leq k \leq n} \binom{n}{k} x^k| \leq \sum_{0 \leq k \leq n} 1 = n + 1.$$

By making $n \to +\infty$, this implies that $|1 + x| \leq 1$. The implications (4) $\Longrightarrow$ (3) $\Longrightarrow$ (2) $\Longrightarrow$ (1) are immediate. □

Proposition 1.11. *Suppose that $|\ |$ is ultrametric.*

1. *If $|x| \neq |y|$, then $|x + y| = \max\{|x|, |y|\}$.*
2. *Any point b in a disc*

   $$D(a, r) := \{x \in K \mid |x - a| \leq r\}$$

   is a center of the disc, meaning that $D(a, r) = D(b, r)$.
3. *If two discs in K intersect each other, then one of them is included in the other one.*
4. *The set $\mathcal{O}_{(K,|\ |)} := D(0, 1)$ is a subring of K and $\mathfrak{m}_{(K,|\ |)} := \{x \in K \mid |x| < 1\}$ is the unique maximal ideal of $\mathcal{O}_{(K,|\ |)}$.*

Proof. (1) Assume $|x| < |y|$, then $|y| = |x + y - x| \leqslant \max(|x + y|, |x|)$. But $|y| > |x|$, so the maximum on the right-hand side is $|x+y|$, therefore $|y| \leq |x+y|$, whence $|y| = |x + y|$.

(2) If $x \in D(a, r)$, then

$$|x - b| = |(x - a) + (a - b)| \leq \max\{|x - a|, |a - b|\} \leq r.$$

Conversely, as $|b-a| \leq r$, we have $a \in D(b,r)$ and $D(a,r) \subseteq D(b,r)$.

(3) Suppose that $b \in D(a,r) \cap D(a',r') \neq \emptyset$ and $r \leq r'$. Then $D(a',r') = D(b,r') \subseteq D(b,r) = D(a,r)$.

(4) As $\mathcal{O}_{(K,|\ |)}$ contains $0, 1 \in K$, is stable by multiplication, and by addition (here we use the ultrametric property), it is a subring of K. It is clear $\mathfrak{m}_{(K,|\ |)}$ is an ideal of $\mathcal{O}_{(K,|\ |)}$. As the elements of $\mathcal{O}_{(K,|\ |)} \setminus \mathfrak{m}_{(K,|\ |)}$ are all invertible in $\mathcal{O}_{(K,|\ |)}$ ($|x| = 1$ implies that $|x^{-1}| = 1$), $\mathfrak{m}_{(K,|\ |)}$ is maximal and is the unique one. □

Definition 1.12 Whe the ultrametric absolute value is given by a valuation v, we also denote $\mathcal{O}_{(K,|\ |)}$ and $\mathfrak{m}_{(K,|\ |)}$ respectively by $\mathcal{O}_v$, $\mathfrak{m}_v$. We call $\mathcal{O}_v = \{x \in K \mid v(x) \geq 0\}$ the valuation ring of K and we have $\mathfrak{m}_v = \{x \in K \mid v(x) > 0\}$. The quotien $\mathcal{O}_v/\mathfrak{m}_v$ is called the *residue field* of v.

Example 1.13 The valuation ring of $\mathbb{Q}$ for the p-adic valuation is the localization $\mathbb{Z}_{p\mathbb{Z}}$ and the residue field is $\mathbb{F}_p$.

Exercise 1.14 Let $(K,|\ |)$ be a valued field of positive characteristic. Show that $|\ |$ is ultrametric.

Definition 1.15 An absolute value $|\ |$ on K induces a distance on K: $(x,y) \mapsto |x-y|$. It defines a topology on K. The absolute value is then a continous map $K \to \mathbb{R}$.

Two absolute values are said to be *equivalent* when they define the same topology on K.

Proposition 1.16. *Two absolute values $|\ |_1$ and $|\ |_2$ on K are equivalent if and only if there exists $s \in \mathbb{R}_+^*$ such that $|\ |_2 = |\ |_1^s$.*

Proof. The if part is easy.

Suppose that $|\ |_1$ and $|\ |_2$ are equivalent. Let $x \in K^*$, then $\lim_{n\to+\infty} x^n = 0$ if and only if $|x|_1 < 1$ (resp. $|x|_2 < 1$). Therefore

$$|x|_1 < 1 \Longleftrightarrow |x|_2 < 1.$$

This implies at once that $|\ |_1$ trivial is equivalent to $|\ |_2$ trivial. Moreover, for all $x \in K$,

$$|x|_1 \geq 1 \Longleftrightarrow |x|_2 \geq 1.$$

This implies that for all $x, y \in K$

$$|x|_1 \geq |y|_1 \Longleftrightarrow |x|_2 \geq |y|_2.$$

(divid by y if $y \neq 0$).

Suppose that $|\ |_1$ is not trivial. Let $t \in K^*$ with $|t| \neq 1$. We can suppose $|\ | < |t|_1 < 1$ (take $1/t$ otherwise). Then $0 < |t|_2 < 1$. Let $s > 0$ be such that $|t|_2 = |t|_1^s$. We are going to show that $|x|_2 = |x|_1^s$ for all $x \in K^*$.

Fix $x \in K^*$ with $|x|_1 < 1$. We have $|x|_1 = |t|_1^\lambda$ for some $\lambda > 0$. Let $(a_n/b_n)_n$ be a descreasing sequence of rational number tending to λ with $a_n, b_n > 0$. We have $|x|_1 \geq |t|_1^{a_n/b_n}$, hence $|x^{b_n}|_1 \geq |t^{a_n}|_1$, so

$$|x^{b_n}|_2 \geq |t^{a_n}|_2, \quad \text{and} \quad |x|_2 \geq |t|_2^{a_n/b_n}.$$

Taking the limit $n \to +\infty$ we get $|x|_2 \geq |t|_2^\lambda$. Using an inscreasing sequence of rational numbers going to λ we get $|x|_2 \leq |t|_2^\lambda$. Therefore

$$|x|_2 = |t|_2^\lambda = (|t|_1^s)^\lambda = (|t|_1^\lambda)^s = |x|_1^s.$$

□

Remark 1.17 If $|\ |$ is an absolute value on K, then $|\ |^s$ is an absolute value on K if $s \leq 1$ (convexity). If $s > 1$ this is still true if $|\ |$ is ultrametric, but false in general otherwise (*e.g.* $|\ |_\infty$ on $\mathbb{R}$).

Over $\mathbb{Q}$, we have the usual absolute value and the p-adic ones. Are there others ?

Theorem 1.18 (Ostrowski)**.** *A non-trivial absolute value $|\ |$ on $\mathbb{Q}$ is equivalent either to the usual absolute value $|\ |_\infty$ or to a p-adic absolute value.*

Proof. (1) Suppose $|\ |$ is archimedean. Let us first show that $|a| > 1$ for all integers $a \geq 2$.

Let $a, b \geq 2$ be integers. For all $n \geq 1$, write a^n in the basis b

$$a^n = c_\ell b^\ell + ... + c_1 b + c_0, \quad 0 \leq c_i \leq b-1,\ c_\ell \neq 0.$$

We have $b^\ell \leq a^n \leq b^{\ell+1}$. So when n goes to $+\infty$, $\ell \sim (\ln a / \ln b)n$ (for the usual topology). We also have

$$|a|^n = |a^n| \leq (\max_{0 \leq i \leq b-1} \{|i|\}) \max\{|b|^\ell, 1\}(\ell + 1).$$

Taking $n \to +\infty$, this implies that $|b| > 1$ if $|a| > 1$. As $|\ |$ is archimedean, $|a| > 1$ for some $a \geq 2$. Thus $|b| > 1$ for all $b \geq 2$. Moreover the above inequality (with $n \to +\infty$) implies that $|a| \leq |b|^{\ln a / \ln b}$, hence

$$|a| = |b|^{\ln a / \ln b}$$

by symmetry. So $|a| = |2|^{\ln a / \ln 2}$. Comparing with $|a|_\infty = 2^{|a|_\infty / \ln 2}$, if we put $s = \ln|2| / \ln 2$, we get

$$|a| = |a|_\infty^s$$

for all integers $a \geq 2$. This extends immediately to all $r \in \mathbb{Q}$.

(2) Now suppose that $|\ |$ is ultrametric. Let A be the valuation ring $\mathcal{O}_{(\mathbb{Q},|\ |}$ with it maximal ideal $\mathfrak{m} = \{x \in K \mid |x| < 1\}$. We have $\mathbb{Z} \subseteq A$ (Proposition 1.10). The intersection $Z \cap \mathfrak{m}$ is a prime ideal of $\mathbb{Z}$.

If $\mathbb{Z} \cap \mathfrak{m} = \{0\}$, then $|k| = 1$ for all non-zero $k \in \mathbb{Z}$, hence $|\ |$ is trivial. So there exists a prime number p such that $\mathbb{Z} \cap \mathfrak{m} = p\mathbb{Z}$. If $k \in \mathbb{Z} \setminus \{0\}$ is prime to p, then $ak + bp = 1$ for some $a, b \in \mathbb{Z}$. As $bp \in p\mathbb{Z} \subseteq \mathfrak{m}$, we have $|bp| < 1$ and

$$|ak| = |1 - bp| = 1.$$

So $|k| = 1$. In general, write $k = p^r k'$ with $r = v_p(k)$ and k' prime to p, then $|k| = |p|^r |k'| = |p|^r$. Let s be such that $|p| = (|p|_p)^s$, then $|k| = (|k|_p)^s$. Again this extends immediately to all rational numbers. □

Definition 1.19 For the record, a *place* of K is an equivalence class of non-trivial absolute values on K. This terminology is often used for number fields. A *finite place* (resp. *infinite place*) corresponds to an ultrametric absolute value (resp. archimedean one).

Ostrowski's theorem says that the finite places of $\mathbb{Q}$ are the p-adic ones and the only infinite place is given by the usual absolute value.

1.2 Complete valued fields

Assume K is endowed with an absolute value $|\ |$. As we already saw with $\mathbb{R}$, the fact that it is complete is a fondamental fact to do analysis.

Recall the following definitions: a sequence $(x_n)_{n\in\mathbb{N}}$ with values in K is a *Cauchy sequence* if for every $\varepsilon \in \mathbb{R}_+^*$ there exists $N \in \mathbb{N}$ such that for all $m \geqslant N$ and $n \geqslant N$, we have $|x_n - x_m| < \varepsilon$. Convergent sequences are Cauchy sequences.

Definition 1.20 A value field K is *complete* if all Cauchy sequences are convergent.

Example 1.21 The field $\mathbb{Q}$ is not complete for the archimedean absolute value $|\ |_\infty$, nor for the p-adic absolute values (see exercise).

Proposition 1.22. *Given a valued field $(K, |\ |)$, there exists a complete valued field $(\widehat{K}, |\ |)$ and a ring homomorphism $\iota : K \to \widehat{K}$ such that $|\iota(x)| = |x|$ for all $x \in K$ and $\iota(K)$ is dense in $\widehat{K}$.*

Proof. Let $\mathcal{C}(K) \subset K^{\mathbb{N}}$ be the set of the Cauchy sequences with values in K. It is easy to check that it is a subring. Denote by $\mathfrak{m} \subset \mathcal{C}(K)$ the set of the sequences K that converge to 0. This is an ideal in $\mathcal{C}(K)$. Let $\widehat{K} = \mathcal{C}(K)/\mathcal{I}(K)$, and let $\iota : K \to \widehat{K}$ be the map defined by $\iota(x) = \pi\big((x)_{n\in\mathbb{N}}\big)$ where $\pi : \mathcal{C}(K) \to \widehat{K}$ is quotient map, so $\iota(x)$ is the class of the constant sequence $(x)_n$. It is straightforward to check that ι is a innjective ring homomorphism.

Let us show that $\widehat{K}$ **is a field**. Let $\underline{x} = (x_n)_{n\in\mathbb{N}} \in \mathcal{C}(K) \smallsetminus \mathfrak{m}$. We have to show that $\pi(\underline{x}) \in \widehat{K}$ is invertible. By hypothesis, there exists $\varepsilon_0 > 0$ such that for all $N \in \mathbb{N}$, there exists $n \geqslant N$ such that $|x_n| \geqslant \varepsilon_0$. As $\underline{x}$ is Cauchy, there exists $N_0 \in \mathbb{N}$ such that $n \geqslant N_0$ and $m \geqslant N_0 \ \Rightarrow\ |x_n - x_m| < \varepsilon_0/2$. So $|x_n| \geq \varepsilon_0/2$ for all $n \geq N_1$ for N_1 big enough. As any finite sequence belongs to $\mathfrak{m}$, we can modify the first N_1-th termes of $\underline{x}$ without changing its class in the quotient. Thus we can suppose that $|x_n| \geq \varepsilon_0/2$ holds for all n. It is straightforward to check that $\underline{y} := (x_n^{-1})_{n\in\mathbb{N}}$ is a Cauchy sequence in K. As $\underline{x}\underline{y} = 1$, $\underline{x}$ is invertible in the quotient.

Now we define an **absolute value on** $\widehat{K}$. Let $\underline{x} = (x_n)_{n\in\mathbb{N}} \in \mathcal{C}(K)$. For all n, m in $\mathbb{N}$, we have

$$-|x_n - x_m| \leq |x_n| - |x_m| \leq |x_n - x_m|$$

by the trangular inequalities. This implies that $(|x_n|)_{n\in\mathbb{N}}$ is a Cauchy sequence in $\mathbb{R}$. The limit $\lim_n |x_n| \in \mathbb{R}$ depends only on $\pi(\underline{x})$. Define

$$|\pi(\underline{x})| = \lim_n |x_n| \in \mathbb{R}_+.$$

It is easy to check that this defines an absolute value en $\widehat{K}$ and that $|\iota(x)| = |x|$ for all $x \in K$.

Let us show that $\iota(K)$ **is dense in** $\widehat{K}$**.** Let $\underline{x} = (x_n)_{n\in\mathbb{N}} \in \mathcal{C}(K)$. Let $\varepsilon \in \mathbb{R}_+^*$: there exists $N \in \mathbb{N}$ such that $|x_n - x_m| < \varepsilon$ for all $n, m \geq N$. Consider the constant sequence $\iota(x_N) = (\tau(x_N))_n$. We have

$$|\iota(x_N) - \pi(\underline{x})| = \lim_{n\to+\infty} |x_N - x_n| \leq \varepsilon.$$

Therefore $\iota(K)$ is dense in $\widehat{K}$.

It remains to prove that $(\widehat{K}, |\ |)$ **is complete**. Let $(\xi_m)_{m\in\mathbb{N}}$ be a Cauchy sequence in $\widehat{K}$. We use Cantor's diagonal method. Concretely, for $m \in \mathbb{N}$, choose $x_m \in K$ (by density of K in $\widehat{K}$) such that $|\xi_m - \iota(x_m)| < 1/(m+1)$. For all $n, m \geq 0$, we have

$$|x_n - x_m| = |\iota(x_n) - \iota(x_m)| \leq |\iota(x_n) - \xi_n| + |\xi_n - \xi_m| + |\xi_m - \iota(x_m)|.$$

This implies easily that $(x_n)_n$ is Cauchy. Finally, let $\alpha := \pi((x_n)_n) \in \widehat{K}$. Then for all $m \geq 0$ we have

$$|\iota(x_m) - \alpha| = \lim_{n\to+\infty} |x_m - x_n|$$

and

$$|\xi_m - \alpha| \leq |\xi_m - \iota(x_m)| + |\iota(x_m) - \alpha|.$$

So $|\xi_m - \alpha|$ is as small as we want provided m is big enough. In other words $(\xi_m)_m$ converges to α. □

Definition 1.23 The valued field $(\widehat{K}, |\ |)$ is called the *completion* of $(K, |\ |)$.

Remark 1.24 The construction of $\widehat{K}$ (more precisely the definition of the absolute value on $\widehat{K}$) relies on the completeness of $\mathbb{R}$. The construction of $\mathbb{R}$ is done in a smilar way, except for the definition of its absolute value. Instead, it is constructed as an ordered field. See Proposition 1.34

Definition 1.25 Let $(K, |\ |_K)$, $(L, |\ |_L)$ be valued fields. A ring homomorphism $f : K \to L$ is called a *homomorphism of valued fields* if $|f(x)|_L = |x|_K$ for all $x \in K$.

Proposition 1.26 (Universal property)**.** *Let $(L, |\ |)$ be a complete valued field and let $f : K \to L$ be a homorphism of valued fields. Then there exists a unique homomorphism of valued fields $\widehat{f} : \widehat{K} \to L$ such that $f = \widehat{f} \circ \iota$. Moreover f is an isomorphism if and only if $f(K)$ is dense in L.*

In particular the completion $(\widehat{K}, |\ |)$ is unique up to unique isomorphism (of valued fields).

Proof. Exercise. □

Remark 1.27 If $|\ |$ is ultrametric, one can also complete K by the process of formal completion. Namely, consider the valuation ring $\mathcal{O}_K$ of $(K, |\ |)$. Fix $t \in K$ with $0 < |t| < 1$ and consider the inverse limit

$$\widehat{\mathcal{O}}_K := \varprojlim \mathcal{O}_K / t^n \mathcal{O}_K.$$

This is an integral domain (use the fact $\cap_n t^n \mathcal{O}_K = \{0\}$). If $\underline{x} = (\bar{x}_n)_n \in \widehat{\mathcal{O}}_K$ ($x_n \in \mathcal{O}_K$ and $\bar{x}_n$ is its image in $\mathcal{O}_K/t^n\mathcal{O}_K$) is non-zero, say $x_{n_0} \notin t^{n_0}\mathcal{O}_K$ (equivalently, $v(x_{n_0}) < n_0 v(t)$), define $\hat{v}(\underline{x}) = v(x_{n_0})$. This is independent of the choice of n_0 and of x_{n_0}.

It is immediate to check that $\hat{v}$ satisfies the conditions of a valuation (except that $\widehat{\mathcal{O}}_K$ is not a field), hence extends to a valuation on $\widehat{K} := \mathrm{Frac}(\widehat{\mathcal{O}}_K)$. One checks that $\widehat{\mathcal{O}}_K$ is actually the valuation ring of $\widehat{K}$. Similarly to before we prove that any Cauchy sequence in in $\widehat{\mathcal{O}}_K$ is convergent and $\widehat{K}$ is complete.

Definition 1.28 Let p be a prime number. The completion of $\mathbb{Q}$ with respect to the p-adic absolute value is denoted by $\mathbb{Q}_p$. It is called the field of *p-adic numbers*. Its valuation ring $\mathbb{Z}_p$ is called the ring of *p-adic integers*.

Remark 1.29 As a fun fact, over a complete ultrametric valued field, a series $\sum_{n\geq 0} a_n$ converges if and only if a_n converges to 0 !

Exercise 1.30 Find the radius of convergence of $\exp(z) := \sum_{n\geq 0} z^n/n!$ in $\mathbb{Q}_p$.

Exercise 1.31 (p-adic expansion) Show that for any $x \in \mathbb{Z}_p$, there is a unique sequence $(a_n)_{n\geq 0}$ with $a_n \in \mathbb{N}$ and $0 \leq a_n \leq p-1$ such that

$$x = a_0 + a_1 p + a_2 p^2 + \dots.$$

Remark 1.32 A way to construct ultrametric valued fields is the following. Let A be a commutative noetherian integral domain. Let $\mathfrak{m} \subset A$ be a maximal ideal generated by one element $t \neq 0$. Then the t-adic valuation is defined similarly to the p-adic valuation. Let $a \in A$ non-zero, then there exists a biggest integer n such that $a \in t^n A$ and $a \notin t^{n+1}A$ (exercise, using Nakayama's lemma). Put $v_{\mathfrak{m}}(a) = n$. We check that this defines a valuation on $\mathrm{Frac}(A)$, therefore an ultrametric absolute value $2^{-v_{\mathfrak{m}}}$ on $\mathrm{Frac}(A)$.

Construction of $\mathbb{R}$. Recall that an *ordered field* is a field K endowed with an order $\leq$, compatible with addition and multiplication by positive elements: if $x \leq y$, then

1. $x + z \leq y + z$;
2. $xz \leq yz$ if moreover $z \geq 0$.

We will only work with *totally* ordered field. Such a field is said to be *archimedean* is for any positive element a and for any $b \in K$, there exists $n \in \mathbb{N}$ such that $na \geq b$. The field $\mathbb{Q}$ is naturally a totally ordered archimedean field.

On a totally ordered field, we can have the notion of intervals, and we define a topology for which the open subsets are the union of open intervals. We define Cauchy sequences $(x_n)_n$ by replacing the $|x_n - x_m| < \epsilon$ with $-a < x_n - x_m < a$ for arbitrary $a \in K_+^*$.

Lemma 1.33. *Let K be a totally ordered archimedean field.*

1. *For any $a \in K$, if $a > 0$, then $-a < 0$.*
2. *For any $a \in K$, we have $a^2 \geq 0$.*
3. *The field K has characteristic 0, and the canonical inclusion $\mathbb{Q} \to K$ is compatible with the structure of ordered fields, is continuous with dense image.*
4. *A sequence $(x_n)_n$ in K is Cauchy if and only if for any $r \in \mathbb{Q}_+^*$, we have $-r < x_n - x_m < r$ for all n, m big enough. In particular, if $x_n \in \mathbb{Q}$, then $(x_n)_n$ is Cauchy for $|\ |_\infty$ if and only if it is Cauchy in K with the ordered topology.*

Proof. (1) This is because $a + (-a) = 0$ and the sum of two positive element is positive.

(2) If $a \geq 0$, then this comes from the definition. Otherwise $-a > 0$ and $a^2 = (-a)^2$.

(3) If $\mathrm{char}(K) = p > 0$, then $\mathbb{N}.1_K$ is a finite set, hence bounded, so K would not be archimedean. For the compatibility if the orders on K and $\mathbb{Q}$, it is enough to show that $1_K > 0$. This is just because 1_K is a square.

Any morphism of totally ordered fields is continuous because the pre-image of an open interval is an open interval.

Let (a, b) be a non-empty open interval. Fix an $n_0 \in \mathbb{N}$ such that $n_0.1_K > b - a$. Consider the set $\{m \in \mathbb{N} \mid m.(n_0.1_K)^{-1} > a\}$. It is non-empty because K is archimedean. Let ℓ be its minimum. Then $\ell(n_0.1_K)^{-1} \in (a, b)$.

(4) is a consequence of the density of $\mathbb{Q}$ in K. □

A construction of the field of real numbers is given by the proposition below.

Proposition 1.34. *There is a totally ordered complete archimedean field.*

Proof. Define $\mathcal{C}(\mathbb{Q})$ as the ring of Cauchy sequences in $(\mathbb{Q}, |\ |_\infty)$, $\mathcal{I}(\mathbb{Q})$ the maximal ideal of the rational sequences converging to 0, and the field $\widehat{\mathbb{Q}} = \mathcal{C}(\mathbb{Q})/\mathcal{I}(\mathbb{Q})$ as before. Let $\pi : \mathcal{C}(\mathbb{Q}) \to \widehat{\mathbb{Q}}$ be the quotient map.

Let us define an **order** on $\widehat{\mathbb{Q}}$. We define

$$\pi((a_n)_n) \geq \pi((b_n)_n)$$

if there is equality or if there exists $r \in \mathbb{Q}_+^*$ such that $a_n \geq b_n + r$ for all n big enough. It is easy to check that this is actually an order and makes $\widehat{\mathbb{Q}}$ an ordered field. Note that if $a_n \geq b_n$ for all n big enough, then $\pi((a_n)_n) \geq \pi((b_n)_n)$. Indeed, we can suppose that they are not equal. Then $(a_n - b_n)_n$ is a Cauchy sequence in $\mathbb{Q}_+$ which does not converge to 0. So there exists $r_0 \in \mathbb{Q}_+^*$ such that $a_n - b_n \geq r_0$ for n big enough.

The above order is **total**. It is enough to show that any non-zero element $\pi((a_n)_n)$ is either > 0 or < 0. As $(a_n)_n$ is Cauchy and does not converge to 0, there is $\epsilon_0 \in \mathbb{Q}_+^*$ such that for all n big enough we have $a_n \geq \epsilon$ or $a_n \leq -\epsilon_0$. But if n is big enough $-\epsilon_0 < a_n - a_m < \epsilon_0$, so they all have the same sign, say > 0. Therefore $a_n \geq \epsilon_0$ for all n big enough. This means that $\pi((a_n)_n) > 0$. Similarly $\widehat{\mathbb{Q}}$ is **archimedean**.

It remains to show the completeness. Let $\phi : \mathbb{Q} \to \widehat{\mathbb{Q}}$ be the morphism $r \mapsto \pi((r)_n)$ (constant sequence). By the above lemma, $\phi(\mathbb{Q})$ is dense in $\widehat{\mathbb{Q}}$. Let $(Y_n)_n$ be a Cauchy sequence in $\widehat{\mathbb{Q}}$. For any $n \geq 0$, take $r_n \in \mathbb{Q}$ such that $-1/(n+1) < Y_n - \phi(r_n) < 1/(n+1)$. As $(Y_n)_n$ is Cauchy, this implies easily that $(r_n)_n$ is Cauchy in $\mathbb{Q}$. Let $\ell = \pi((r_n)_n)$. We have $Y_n \to \ell$ similarly to the proof of Proposition 1.22. □

Proposition 1.35. *If K_1, K_2 are complete totally ordered archimedean fields, there exists a unique isomorphism $f : K_1 \to K_2$ of ordered fields.*

Proof. Any element $x \in K_1$ is the limit of a Cauchy sequene $(r_n)_n$ in $\mathbb{Q}$. But $(r_n)_n$ is also a Cauchy sequence in K_2, so we can define $f(x) = \lim_n r_n$ in K_2. This is a ring homomorphism. We get an inverse of f by symmetry.

Let us show that f is compatible with the orders on K_1, K_2, that is, f is increasing. Let $x, y \in K_1$ with $x - y \geq 0$. By the lemma below, $x - y = z^2$ for some $z \in K_1$, so $f(x) - f(y) = f(z^2) = f(z)^2 \geq 0$ and f is strictly increasing. Note that the pre-image of an open interval is then an open interval, hence f is continuous. □

Lemma 1.36. *Let K be a field as in the above proposition. Let $a \in K$ with $a \geq 0$. Then $a = b^2$ for some $b \in K$.*

Proof. One can suppose $a > 0$. Consider the set $S = \{x \in K \mid x > 0,\ x^2 \leq a\}$. As K is complete, there exists $b = \sup S$. If $b < a^2$, then $(b(1 + /n))^2 \leq a^2$ for $n \gg 0$. But $b < b(1 + 1/n)$ and $b(1 + 1/n) \in S$, contradiction. So $b \geq a^2$. Similarly $b \leq a^2$. So $b = a^2$. □

1.3 Normed vector spaces

Definition 1.37 Let $(K, |\ |)$ be a valued field. Let V be a K-vector space. A *norm* on V is a function $\|\ \| : V \to \mathbb{R}_+$ such that

(a) $\forall v \in V,\ \|v\| = 0$ if and only if $v = 0$;

(b) $\forall \lambda \in K,\ \forall v \in V,\ \|\lambda v\| = |\lambda| \|v\|$;

(c) (Triangle inequality) $\forall (v, w) \in V^2,\ \|v + w\| \leqslant \|v\| + \|w\|$.

The pair $(V, \|\ \|)$ is then called a *normed vector space.*

Example 1.38 1. If $(L, |\ |)$ is a valued field and $K \subset L$ a subfield, endowed with the restriction of $|\ |$, then the absolute value $|\ |$ endows L with a normed vector space structure.

2. Let X be a set and let $\mathcal{B}(X, K)$ be the space of bounded functions on X with values in K. For all $f \in \mathcal{B}(X, K)$, put

$$\|f\|_\infty = \sup_{x \in X} |f(x)|.$$

Then $(\mathcal{B}(X, K), \|\ \|_\infty)$ is a normed vector space over K.

As a special case ($X = \{1, 2, \ldots, n\}$),

$$(x_1, \cdots, x_n) \mapsto \max_{1 \leq i \leq n} |x_i|$$

is a norm on K^n.

Example 1.39 (Gauss norm) Let K be a *ultrametric* valued field with valuation ring $\mathcal{O}_K$ and residue field k. Fix $n \geq 0$ and consider $K[X]$ as a K-vector space. Define

$$\|\sum_{i \geq 0} a_i X^i\| := \max_{i \geq 0} |a_i|.$$

This is clearly a norm. We claim that this norm is multiplicative. Indeed, it is enough to show that $\|FG\| = 1$ if $\|F\| = \|G\| = 1$.

We have a ring homomorphism $\mathcal{O}_K[X] \to k[X]$ defined by reducing the coefficients of $P(X) \in \mathcal{O}_K[X]$ modulo the ideal $\mathfrak{m}_K$. Then $\|F\| = 1$ is equivalent to say that $F(X) \in \mathcal{O}_K[X]$ and that its image $\bar{F}(X) \in k[X]$ is non-zero. Now the claim results from the fact that $k[X]$ is an integral domain.

The multiplicativity of the Gauss norm allows us to extend it to an absolute value on $K(X)$, whose restriction on K is the initial absolute value.

Definition 1.40 Let $(V, \|\ \|)$ be a normed K-vector space. Then $\|\ \|$ induces a distance on V: $(x, y) \mapsto \|x - y\|$. In what follows, V will always be endowed with this metric space structure. Assuming that K is complete, we say that $(V, \|\ \|)$ is a *Banach space* if $(V, \|\ \|)$ is complete.

Proposition 1.41. *If $(K, |\ |)$ is complete, then so is $(\mathcal{B}(X, K), \|\ \|_\infty)$.*

Proof. Let $(f_n)_n$ be a Cauchy sequence in $(\mathcal{B}(X, K), \|\ \|_\infty)$. For any $x \in X$, the sequence $(f_n(x))_{n \in \mathbb{N}}$ is Cauchy in K, hence converges to a limit $f(x) \in K$. As $(f_n)_n$ is normally (in the sens of the norm) Cauchy, it converges normally to f. □

Definition 1.42 Let V be a K-vector space. Two norms $\|\ \|_1, \|\ \|_2$ on V are said to be *equivalent* if they define the same topology on V.

If there exist constants c, c' in $\mathbb{R}_+^*$ such that

$$c'\|x\|_1 \leqslant \|x\|_2 \leqslant c\|x\|_1, \quad \forall x \in V$$

then the two norms are clearly equivalent.

Exercise 1.43 Show that the converse of the above property holds if the absolute value $|\ |$ on K is non-trivial.

The following theorem is well-known for real vector spaces of finite dimension.

Theorem 1.44. *Let $(K, |\ |)$ be a complete valued field. Let V be a K-vector space of finite dimension. Then all norms on V are equivalent. In particular $(V, \|\ \|)$ is Banach for any norm.*

Proof. Let $e_1, \dots, e_n$ be a basis of V. We saw that $(V, \|\ \|_\infty)$ is Banach for the norm

$$\|x\|_\infty = \max_{1 \leq i \leq n} \{|a_i|\}$$

if $x = \sum_{1 \leq i \leq n} a_i e_i$.

Let $\|\ \|$ be a norm on V. By the triangle inequality,

$$\|x\| \leq \max_{1 \leq i \leq n} \{|a_i|\} (\sum_{1 \leq i \leq n} \|e_i\|) = (\sum_{1 \leq i \leq n} \|e_i\|) \|x\|_\infty.$$

To prove the inverse inequality (with a different constant) we proceed by induction on n. We can suppose $n \geq 2$. For any $i \leq n$, define V_i as the subspace of V generated by the e_j, $j \neq i$. By induction hypothesis, V_i with the restriction of $\|\ \|$ is complete, hence is closed in $(V, \|\ \|)$. As $0 \notin \cup_{1 \leq i \leq n} (e_i + V_i)$, there exists $\varepsilon_0 > 0$ such that this union is disjoint from $\{x \in V \mid \|x\| < \varepsilon_0\}$.

Let $x \in V \smallsetminus \{0\}$ and suppose, say, $\|x\|_\infty = |a_1|$. Then $a_1^{-1} x \in e_1 + V_1$, thus $\|a_1^{-1} x\| \geq \varepsilon_0$ and $\|x\| \geq \varepsilon_0 |a_1| = \varepsilon_0 \|x\|_\infty$, and we are done. □

Exercise 1.45 Let K be a complete valued field, then any linear map between normed vector spaces of finite dimension over K is continuous, and is open if it is surjective. (*Hints:* choose suitable bases of the vector spaces).

1.4 Hensel's lemma

Over a complete ultrametric valued field, there are several forms of Hensel's lemma. They transform a approximated decomposition of a polynomial into an exact decomposition.

Theorem 1.46 (Hensel's lemma, strong form)**.** *Let K be a complete ultrametric field with valuation ring $\mathcal{O}_K$ and residue field k. Let $P(X) \in \mathcal{O}_K[X]$. Suppose that $\bar{P}(X) \in k[X]$ can be decomposed as*

$$\bar{P}(X) = f(X) g(X), \quad \gcd(f(X), g(X)) = 1.$$

Then there exist $F(X), G(X) \in \mathcal{O}_K[X]$ such that

$$P(X) = F(X) G(X),$$

and

$$\bar{F}(X) = f(X),\ \bar{G}(X) = g(X),\ \deg F(X) = \deg f(X).$$

Moreover, such a decomposition is unique up to multiplication by $\mathcal{O}_K^*$.

Proof. Note that $\deg \bar{P}(X)$ can be smaller than $\deg P(X)$.

Let $d = \deg P(X)$ and $m = \deg f(X)$. For any $r \geq 0$, denote by

$$\mathcal{O}_K[X]_r = \{F(X) \in \mathcal{O}_K[X] \mid \deg F \leq r\}.$$

Lift $f(X), g(X)$ respectively to $F_0(X), G_0(X) \in \mathcal{O}_K[X]$ keeping the degrees. In particular the leading coefficient of $F_0(X)$ belong to $\mathcal{O}_K^*$ (units of $\mathcal{O}_K$).

Let $t \in \mathfrak{m}_K \smallsetminus \{0\}$ be such that

$$P(X) - F_0(X)G_0(X) \in t\mathcal{O}_K[X]$$

and

$$1 \in F_0(X)\mathcal{O}_K[X] + G_0(X)\mathcal{O}_K[X] + t\mathcal{O}_K[X]$$

(recall that $\gcd(f(X), g(X)) = 1$).

(1) *First approximation.* We are going to approximate F_0, G_0 by $F_1 = F_0 + tV_1$, $G_1 = G_0 + tU_1$, such that $P - F_1G_1 \in t^2\mathcal{O}_K[X]$. We have

$$P - F_1G_1 = (P - F_0G_0) - t(U_1F_0 + V_1G_0) - t^2U_1V_1.$$

Let $E_0 = t^{-1}(P - F_0G_0) \in \mathcal{O}_K[X]_d$. Then what we need are U_1, V_1 such that

$$E_0 - (U_1F_0 + V_1G_1) \in t\mathcal{O}_K[X], \quad \deg U_1 \leq d - m, \ \deg V_1 \leq m. \tag{1}$$

The conditions on the degrees of U_1, V_1 are to insure that the limits we will consider exist in $\mathcal{O}_K[X]$. We have

$$E_0 \in (F_0, G_0) + t\mathcal{O}_K[X].$$

Using Euclidian division by F_0 (whose leading coefficient is invertible in $\mathcal{O}_K$), we can find $V_1 \in \mathcal{O}_K[X]_m$ such that

$$E_0 \in V_1G_0 + F_0\mathcal{O}_K[X] + t\mathcal{O}_K[X]$$

As $E_0 - V_1G_0$ has degree $\leq d$, we can find $U_1 \in \mathcal{O}_K[X]_{d-m}$ such that $E_0 - (U_1F_0 + V_1G_0) \in t\mathcal{O}_K[X]$. The polynomials U_1, V_1 satisfy the conditions in (1) above. This implies that

$$P - F_1G_1 \in t^2\mathcal{O}_K[X],$$

$\deg F_1 = m$, $\deg G_1 \leq d - m$ and $\bar{F}_1 = f$, $\bar{G}_1 = g$.

(2) *Induction.* The same arguments show that there exist $U_2 \in \mathcal{O}_K[X]_{d-m}, V_2 \in \mathcal{O}_K[X]_m$ such that

$$t^{-2}(P - F_1G_1) \in U_2F_1 + V_2G_1 + t\mathcal{O}_K[X],$$

Put

$$F_2 = F_1 + t^2V_2, \quad G_2 = G_1 + t^2U_2.$$

Then

$$P - F_2G_2 \in t^3\mathcal{O}_K[X]$$

$\deg F_2 = m$, $\deg G_2 \leq d - m$ and $\bar{F}_2 = f$, $\bar{G}_2 = g$. In this way we construct inductively two sequences

$$U_n(X) \in \mathcal{O}_K[X]_{d-m}, \quad V_n(X) \in \mathcal{O}_K[X]_m$$

such that if

$$F_n := F_0 + tV_1 + t^2V_2 + \cdots + t^nV_n, \quad G_n := G_0 + tU_1 + t^2U_2 + \cdots + t^nU_n,$$

then

$$P - F_n G_n \in t^{n+1} \mathcal{O}_K[X],$$

$\deg F_n = m$, $\deg G_n \leq d - m$ and $\bar{F}_n = f$, $\bar{G}_n = g$.

(3) *Proof of the existence.* The sequence $(F_n)_n$ in $\mathcal{O}_K[X]_m$ converges to some $F(X) \in \mathcal{O}_K[X]$ for the Gauss norm (Example 1.39). Similarly for $(G_n)_n$ and we get a decomposition $P(X) = F(X)G(X)$ as desired.

(4) *Uniqueness.* Suppose $P(X) = F(X)G(X) = \Phi(X)\Gamma(X)$ with $\deg \Phi(X) = m$ and $\bar{\Phi}(X) = f(X)$. Without loss of generalities we can suppose that F and Φ are monic. If $F \neq \Phi$, then $\Phi = F + H$ with $\deg H < m$ and $H \in \mathfrak{m}_K[X]$. Let $s \in K^*$ be such that $|s| = \|H\|$ the Gauss norm (Example 1.39) of H. Then $H = sR$ with $\deg R < m$ and $\bar{R}(X) \neq 0$. Then $F(G - \Gamma) = -sR\Gamma$. This implies that the Gauss norm $\|G - \Gamma\| = |s|$ and $f(X) \mid \bar{R}(X)g(X)$. This is impossible as $\deg \bar{R}(X) < m$ and $g(X)$ is prime to $f(X)$. □

Corollary 1.47. *Let $(K, |\ |)$ be ultrametric and complete. Let*

$$P(X) = \sum_{0 \le i \le d} a_i X^i \in K[X]$$

be an irreducible polynomial of degree d. Then

$$\max_{0 \le i \le d} \{|a_i|\} = \max\{|a_0|, |a_d|\}.$$

Proof. Suppose that for some $1 \le i_0 < d$ we have $|a_{i_0}| > |a_0|, |a_d|$. Consider $Q(X) = a_{i_0}^{-1} P(X) \in \mathcal{O}_K[X]$. Then $\bar{Q}(X) = X^r g(X)$ with $0 < r < d$ and $g(X)$ prime to X. By Hensel's lemma, $Q(X)$ is divisible by a $F(X) \in \mathcal{O}_K[X]$ of $\deg F(X) = r < d$. This implies that $P(X)$ itself is reducible, contradiction. □

Corollary 1.48 (Hensel's lemma, basic form)**.** *Let K be a complete ultrametric valued field with valuation ring $\mathcal{O}_K$ and residue field k. Let $P(X) \in \mathcal{O}_K[X]$. Suppose that $\bar{P}(X) \in k[X]$ has a simple zero $\lambda \in k$. Then $P(X)$ has a unique zero $\alpha \in \mathcal{O}_K$ such that $\bar{\alpha} = \lambda$.*

Corollary 1.49. *Let $(K, |\ |)$ is a complete ultrametric valued field with valuation ring $\mathcal{O}_K$. Let $P(X) \in \mathcal{O}_K[X]$. Assume that $|P(\alpha)| < |P'(\alpha)|^2$ for some $\alpha \in \mathcal{O}_K$. Then there exists a unique $\widetilde{\alpha} \in \mathcal{O}_K$ such that $P(\widetilde{\alpha}) = 0$ and $|\widetilde{\alpha} - \alpha| < |P'(\alpha)|$.*

Proof. Let $\lambda = P'(\alpha)$. The Taylor expansion at α gives

$$P(X + \alpha) = P(\alpha) + \lambda X + X^2 R(X),\ R(X) \in \mathcal{O}_K[X].$$

Consider the polynomial

$$H(X) = \lambda^{-2} P(\lambda X + \alpha) = \lambda^{-2} P(\alpha) + X + X^2 S(X),\ S(X) \in \mathcal{O}_K[X].$$

So 0 is a simple root of $\bar{H}(X)$. By Hensel's lemma (basic form), $H(X)$ has a unique zero $t \in \mathfrak{m}_K$. Hence $\tilde{\alpha} := \lambda t + \alpha$ is the unique zero of $P(X)$ with $|\tilde{\alpha} - \alpha| < |\lambda| = |P'(\alpha)|$. □

Example 1.50 Let $n \ge 2$ be prime to p. Then $\mathbb{Z}_p \to \mathbb{Z}_p$, $x \mapsto x^n$, induces a (multiplicative) group automorphism of $1 + p\mathbb{Z}_p \subset \mathbb{Z}_p^*$.

Example 1.51 Considering $X^{p-1} - 1$, we see that $\mathbb{Z}_p$ contains all $(p-1)$-th roots of unity.

Remark 1.52 The example of $P(X) = X^2 - p \in \mathbb{Z}_p[X]$, which does not have zeros in $\mathbb{Z}_p$, shows that Hensel's lemma is false without condition on $P'(X)$.

Multiple variables Hensel's lemma.

Proposition 1.53. *Let $(K, |\ |)$ be a complete ultrametric valued field, let $\mathcal{O}_K$ be the corresponding valuation ring. Let $F(X, Y) \in \mathcal{O}_K[X, Y]$. Denote by $Z(F) = \{(x, y) \in K^2 \mid F(x, y) = 0\}$ the zero locus of $F(X, Y)$. Suppose that for some $(a, b) \in k^2$, we have $\bar{F}(a, b) = 0$ and $\bar{F}'_X(a, b) \ne 0$ (partial derivative w.r.t. X). Then we have a bijection*

$$\mathfrak{m}_K \to Z_{(a,b)} := \{(x, y) \in \mathcal{O}_K^2 \mid F(x, y) = 0,\ \bar{x} = a, \bar{y} = b\}.$$

Proof. Let $\tilde{a}, \tilde{b}$ be respective liftings of a, b in $\mathcal{O}_K$. For any $t \in \mathfrak{m}_K$, consider the polynomial $P_t(X) = F(X, \tilde{b} + t) \in \mathcal{O}_K[X]$. Then $\bar{P}'_t(a) = \bar{F}'_X(a, b) \neq 0$. By Hensel's lemma (basic form), there exists a unique $x_t \in \mathcal{O}_K$ such that

$$F(x_t, \tilde{b} + t) = 0, \quad \bar{x}_t = a.$$

So $t \mapsto (x_t, \tilde{b}+t)$ defines an injective map from $\mathfrak{m}_K$ into $Z_{(a,b)}$. Let $(x, y) \in Z_{(a,b)}$. Let $t = y - \tilde{b} \in \mathfrak{m}_K$. As $F(x, \tilde{b} + t) = 0 = F(x_t, \tilde{b} + t)$ and $\bar{a}$, Hensel's lemma says that $x = x_t$ and (x, y) is the image of t. This implies the surjectivity. □

Remark 1.54 The bijection is in fact an analytic function. We also have easily a similar result for more than two variables.

Example 1.55 Let $p > 3$. Let $F(X, Y) = Y^2 + X^3 + 1 + p \in \mathbb{Q}_p[X, Y]$. Then $\{(x, y) \mid F(x, y) = 0$ is a the disjoint union of the $Z_{(a,b)}$'s, where the $(a, b) \in \mathbb{F}_p^2$ are the zeros of $\bar{F}(X, Y) \in \mathbb{F}_p[X, Y]$, and each $Z_{(a,b)}$ is in bijection with $\mathfrak{m}_K$. Indeed, at each (a, b), at least one of $\bar{F}'_X$, $\bar{F}'_Y$ is non-zero.

1.5 Extensions of absolute values

Let $(K, |\ |)$ be an ultrametric valued field, and L be an extension of K. The aim of this subsection is to extend the absolute value on K to L.

Recall that if L/K is a finite extension of degree n of fields (we forget about absolute for a moment), then for any $\alpha \in L$, the norm $N_{L/K}(\alpha)$ is defined as the determinant of the (K-linear) multiplication-by-α map $L \to L$.

Proposition 1.56. *Let L/K be an extension of degree n.*

1. *If $\alpha \in K$ then $N_{L/K}(\alpha) = \alpha^n$.*
2. *If $\alpha, \beta \in L$, then $N_{L/K}(\alpha\beta) = N_{L/K}(\alpha)N_{L/K}(\beta)$.*
3. *If E is a subextension of L, then*

$$N_{L/K}(\alpha) = N_{E/K}(N_{L/E}(\alpha)).$$

In particular

$$N_{L/K}(\alpha) = N_{K[\alpha]/K}(\alpha)^{[L:K[\alpha]]}.$$

4. *If $X^d + a_{d-1}X^{d-1} + \cdots + a_0 \in K[X]$ is the minimal polynomial of α over K, then $N_{K[\alpha]/K}(\alpha) = (-1)^d a_0$.*

Proof. These are classical results on fields extensions. They are all easy except the transitivity property (3). The special case $E = K[\alpha]$ in (3) (the only one we need later) will be done in TD (exercise session). □

Theorem 1.57. *Let $(K, |\ |)$ be a complete ultrametric valued field, let L/K be an extension of degree n. Then $|\ |$ extends uniquely to an absolute value on L, which is given by*

$$\alpha \mapsto |N_{L/K}(\alpha)|^{1/n}$$

for all $\alpha \in L$.

Proof. (1) **Existence.** The only property to check is the ultrametric inequality. As we already observed, this amongs to showing that $|N_{L/K}(1+\alpha)| \leq 1$ if $|N_{L/K}(\alpha)| \leq 1$. By 1.56(3), we can suppose $L = K[\alpha]$. Let

$$P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in K[X]$$

be the minimal polynomial of α over K. Then $|a_0| = |\alpha|^n \leq 1$. By Corollary 1.47, $P(X) \in \mathcal{O}_K[X]$. The minimal polynomial of $1+\alpha$ is $P(X-1) \in \mathcal{O}_K[X]$, therefore $|N_{L/K}(1+\alpha)| \leq 1$.

(2) **Uniqueness** Let $|\ |_1, |\ |_2$ be two absolute values on L extending that of K. They are then equivalent (Theorem 1.44). So there exists $s > 0$ such that $|\ |_2 = |\ |_1^s$ (Proposition 1.16). Restricting to K we get $s = 1$ if $|\ |$ is non-trivial on K.

Otherwise, the trivial absolute value on L is an extension of $|\ |$ to L. So $|\ |_i$ is equivalent to the trivial absolute value, thus is trivial as well. □

Corollary 1.58. *Let $(K, |\ |)$ be a complete ultrametric absolute value. Let K^c be an algebraic closure of K. Then $|\ |$ extends uniquely to an absolute value $|\ |_c$ to K^c.*

Proof. For any $\alpha \in K^c$, define $|\alpha|_c = |N_{K[a]/K}(\alpha)|^{1/[K[\alpha]:K]}$. As we saw above, we have $|\alpha|_c = |\alpha|_L$ for any finite extension L containing α. This easily implies the corollary. □

Remark 1.59 Suppose K is ultrametric and complete. By construction, if $\alpha \in K^c$, then all conjuguates of α have the same absolute value $|\alpha|_c$.

Exercise 1.60 Let $(K, |\ |)$ be as in Theorem 1.57. Let $\alpha \in K^c$ with minimal polynomial $\sum_{0 \leq i \leq n} a_i X^i \in K[X]$. Show that $|a_i|^n \leq |a_0|^{n-i}$ for all $i \geq 0$.

Next we study the extension of absolute values when K is not necessarily complete (*e.g.* a number fields).

Proposition 1.61. *Let $(K, |\ |_K)$ be an ultrametric valued field. Let L/K be an algebraic extension. Then $|\ |_K$ extends to an absolute value on L. Moreover, if L/K is finite, then there are at most $[L:K]$ distinct such extensions.*

Proof. Let $(\widehat{K}, |\ |_{\widehat{K}})$ be the completion of $(K, |\ |_K)$. Let $(\widehat{K})^c$ be an algebraic closure of $\widehat{K}$ and let K^c be the algebraic closure of K in $(\widehat{K})^c$. Then K^c is an algebraic closure of K.

The absolute value $|\ |_K$ extends uniquely to an absolute value $|\ |_c$ on $(\widehat{K})^c$. As L is algebraic over K, there exists an embedding $\sigma : L \to K^c \subset \widehat{K}^c$ (as extensions of K). Then $\alpha \mapsto |\sigma(\alpha)|_c$ defines an absolute value on L extending $|\ |_c$.

Suppose now that L/K is finite. Let us show that any extension $|\ |_L$ of $|\ |_K$ is obtained as above for some embbeding $\sigma : L \to K^c$. Let $(\widehat{L}, |\ |_{\widehat{L}})$ be the completion of $(L, |\ |_L)$. Consider K' the topological closure of K in $\widehat{L}$, endowed with the restriction of $|\ |_{\widehat{L}}$. This is a completion of $(K, |\ |_K)$. Let us show that $\widehat{L}$ is finite over K'. Indeed, the compositum $LK' \subseteq \widehat{L}$ is finite over K', hence is complete (for the topology induced by that of $\widehat{L}$), therefore closed in $\widehat{L}$. But it is also dense in $\widehat{L}$ because it contains L. So we get $\widehat{L} = LK'$ is finite over K'.

By the uniqueness of the completion we have an isomorphism of value fields $\phi : K' \simeq \widehat{K}$. As $\widehat{L}$ is algebraic over K', we have a commutative diagram

$$\begin{array}{ccccc} L & \longrightarrow & \widehat{L} & \xrightarrow{\tau} & (\widehat{K})^c \\ \uparrow & & \uparrow & & \uparrow \\ K & \longrightarrow & K' & \xrightarrow{\phi} & \widehat{K} \end{array}$$

where the no-name arrows are inclusions. On the extension $\tau(\widehat{L})$ of $\widehat{K}$, the map $\tau(x) \mapsto |x|_{\widehat{L}}$ defines an absolute value extending $|\ |_{\widehat{K}}$. By the uniqueness property, $|x|_{\widehat{L}} = |\tau(x)|_c$ for all $x \in \widehat{L}$. Let $\sigma = \tau|_L$, then $|x|_L = |\sigma(x)|_c$ and we are done. □

Proposition 1.62. *Let $(K, |\ |)$ be an ultrametric valued field. Let Ω/K be any field extension. Then $|\ |$ extends to an absolute value on Ω.*

Proof. Let $\{x_i\}_{i\in I}$ be a transcendental basis of Ω over K (the existence is proved by the axiom of choice). Define the multi-variable Gauss norm by

$$\| \sum_{\nu\in\mathbb{N}^I} a_\nu \underline{x}^\nu \| = \max_{\nu\in\mathbb{N}^I} |a_\nu|.$$

Like in the one-variable case, this norm is multiplicative (because $k[x_i]_i$ is an integral domain). So it defines an absolute value on $K(x_i)_i$ extending that of K. Now we are reduced to the case of the algebraic extension $\Omega/K(x_i)_i$ which was treated in the above proposition. □

The proposition below says that two polynomials with close coefficients have close roots. We include the archimedean case (over $\mathbb{C}$).

Proposition 1.63 (Continuity of roots)**.** *Let $(K, |\ |)$ be a valued field. Endow $K[X]$ with the norm $\|\sum_i a_i X^i\| = \sum_i |a_i|$ and extend $|\ |$ to some $|\ |_c$ over an algebraic closure K^c of K (if K is archimedean, take $\mathbb{C}$ instead of K^c).*

Let $P(X) \in K[X]$ be a monic polynomial of degree n. For all $\varepsilon > 0$, there exists a constant $\delta > 0$ depending on $P(X)$ and on ε, such that for any monic polynomial $Q(X) \in K[X]$ of degree n, if $\|P - Q\| < \delta$, then for any root $\alpha \in K^c$ of $P(X)$, there exists a root $\beta \in K^c$ of Q such that $|\beta - \alpha| < \varepsilon$.

Proof. (1) Let $\alpha \in K^c$ be a root of $P(X)$, then $|\alpha|_c \le \|P\|$. Indeed, we can suppose $|\alpha|_c \ge 1$ because $\|P\| \ge 1$. We have

$$|\alpha|_c^n \le \sum_{0\le i\le n-1} |a_i||\alpha|_c^i \le \sum_{0\le i\le n-1} |a_i||\alpha|_c^{n-1} \le \|P\||\alpha|_c^{n-1}.$$

Thus $|\alpha|_c \le \|P\|$.

(2) Let $\alpha \in K^c$ be a root of $P(X)$. We have

$$|Q(\alpha)|_c = |(Q-P)(\alpha)|_c \le \|P - Q\| \max\{1, |\alpha|_c^n\} \le \|P - Q\|\|P\|^n.$$

Now $|Q(\alpha)|_c$ is the product of the $|\alpha - \beta|_c$'s on all the roots (counted with multiplicity) of $Q(X)$ in K^c, therefore one of them satisfies $|\alpha - \beta|_c \le \|P - Q\|^{1/n}\|P\|$. So we can take any $\delta \le (\varepsilon/\|P\|)^n$. □

When working in p-adic analytic theory, we need the ground field to be complete. Sometimes we also want it to be algebraically closed. The natural way to construct such a field is to take the algebraic closure of the completion of an ultrametric valued field.

Corollary 1.64. *Let $(K, |\ |)$ be an ultrametric valued field. Let K^c be an algebraic closure of K, endowed with an extension $|\ |_c$ of $|\ |$, and let $\widehat{K^c}$ be its completion. Then $\widehat{K^c}$ is algebraically closed.*

Proof. Let Ω be an algebraic closure of $\widehat{K^c}$ endowed with an extension of $|\ |_c$, that we still denote by $|\ |_c$.

Let $P(X) \in \widehat{K^c}[X]$ be a monic polynomial and let $\alpha \in \Omega$ be a root of $P(X)$. For all $m \geq 1$, pick a $Q_m(X) \in K^c[X]$ as in Proposition 1.63 for $\varepsilon = 1/m$. Pick a root $\beta_m \in K^c$ of $Q_m(X)$ such that $|\alpha - \beta_m|_c < 1/m$. Then α is the limit of the sequence $(\beta_m)_m$, hence $\alpha \in \widehat{K^c}$. □

Notation. Let p be any prime number. Then $\mathbb{C}_p$ denotes the completion of an algebraic closure $\mathbb{Q}_p^c$ of $\mathbb{Q}_p$. Denote again by $|\ |_p$ the unique extension of the p-adic absolute value on $\mathbb{Q}_p$, then $(\mathbb{C}_p, |\ |_p)$ is complete and algebraically closed. We have $|\mathbb{C}_p^*|_p = p^{\mathbb{Q}} \subset \mathbb{R}^*$.

Let us come back to Proposition 1.61 when L/K is a finite extension. How to understand the different extensions of $|\ |_K$ to L ? A topological point of view (meaning relying on the completion $\widehat{K}$) is the following. Consider the tensor product

$$B_L := L \otimes_K \widehat{K}.$$

This is a finite dimensional $\widehat{K}$-algebra. It only has finitely maximal ideals $\mathfrak{m}_1, \dots, \mathfrak{m}_n$, their number n is roughly bounded by $\dim_{\widehat{K}} B_L = [L : K]$. The quotient $\widehat{L}_i$ of B_L by $\mathfrak{m}_i$ is a finite extension of $\widehat{K}$, hence gets a unique extension $|\ |_i$ of $|\ |_K$. We have a canonical K-algebra homomorphism $L \to B_L$, $x \mapsto x \otimes 1$. The composition $\phi_i : L \to B_L \to \widehat{L}_i$ is an embedding, and $|\ |_i$ induces by ϕ_i^{-1} an extension of $|\ |_K$ to L.

Note that B_L has canonically a structure of $\widehat{K}$-Banach space and L is dense in B_L because K is dense in $\widehat{K}$. One can wonder why the canonical K-algebra homomorphism $L \to B_L$ does not extend to $\widehat{L}_i \to B_L$. The reason is the following. Write $v \in L$ in a K-basis of L: $v = \sum_{1 \leq j \leq d} \lambda_j e_j$. Then v is small in B_L means that all coordinates $|\lambda_j|$ are small. However, if we fix an absolute value $|\ |_i$ on L, $|v|_i$ small does not imply that all $|\lambda_j|$ are small. This would be true if we ask $|v|_i$ be small for all extensions $|\ |_i$ on L.

One can check this on a concrete case. For example take $K = \mathbb{Q}$ with the 7-adic topology, take $L = K[\sqrt{2}]$. There are two extensions of $||_7$ to L. The first one is $(3 + \sqrt{2})$-adic and the second one is $(3 - \sqrt{2})$-adic. Write $(3 + \sqrt{2})^n = a_n + b_n\sqrt{2}$. Then $a_n = \sum_{0 \leq k \leq n/2} \binom{n}{2k} 3^{n-2k} 2^k$. As $2 \equiv 3^2 \mod 7$ we have

$$a_n \equiv \sum_{0 \leq k \leq n/2} \binom{n}{2k} 3^{n-2k} 3^{2k} \equiv 3^n 2^{n-1} \mod 7$$

(Expand $(1+1)^n + (1-1)^n$). We see that $(3+\sqrt{2})^n$ does not converge to 0 for the $\mathbb{Q}_7$-topology on $L \otimes_{\mathbb{Q}} \mathbb{Q}_7$.

Proposition 1.65. *The extensions of $|\ |_K$ to L correspond to the maximal ideals of $L \otimes_K \widehat{K}$.*

Proof. (1) *Different maximal ideals give differents extensions of $|\ |_K$.* By the Chinese Remainder Theorem, the canonical morphism

$$B_L \to \prod_{1 \leq i \leq n} \widehat{L}_i = \prod_{1 \leq i \leq n} B_L/\mathfrak{m}_i$$

is surjective. It is continuous because both sides are Banach spaces. Fix $i \neq j$. Let $x' \in B_L$ with image 1 in $\widehat{L}_i$ and 0 in $\widehat{L}_j$. Let $x \in L$ be close enough to x', then $|x|_i = 1$ and $|x|_j < 1$. So $|\ |_i \neq |\ |_j$.

(2) *Any extension of $|\ |_K$ to L is given by a maximal ideal.* Consider an extension $|\ |_L$ of $|\ |_K$ to L and the completion $\widehat{L}$ of L with respect to this absolute value. We have two natural embeddings $\phi : L \to \widehat{L}$ and $\psi : \widehat{K} \to \widehat{L}$ (given by the universal property of the completions). By the universal property of the tensor product, we then have a canonical morphism of K-algebras

$$B_L = L \otimes_K \widehat{K} \to \widehat{L}, \quad x \otimes y \mapsto \phi(x)\psi(y).$$

The image of this map is dense in $\widehat{L}$ (it contains L), finite dimensional over $\widehat{K}$ (because B_L is), hence is closed and equals to $\widehat{L}$. Therefore $\widehat{L}$ is a quotient of B_L, thus it coincides with one of the $\widehat{L}_i$'s. □

Example 1.66 Consider the quadratic extension $L = \mathbb{Q}[\sqrt{2}]$ of $\mathbb{Q}$. The minimal polynomial of $\sqrt{2}$ is $X^2 - 2$. In $\mathbb{Q}_7[X]$, it has two irreducible factors because it is equal to $(X-3)(X+3)$ $\mathbb{F}_7[X]$. Therefore the 7-adic absolute value on $\mathbb{Q}$ has two extensions to $\mathbb{Q}[\sqrt{2}]$.

As $X^2 - 2$ is irreducible in $\mathbb{Q}_2[X]$, the 2-adic absolute value on $\mathbb{Q}$ has a unique extension to $\mathbb{Q}[\sqrt{2}]$.

Exercise 1.67 Let K be as above L/K be a finite extension.

1. Suppose that L/K separable. Let $P(X)$ be the minimal polynomial of primitive element of L. Show that the maximal ideals of $L \otimes_K \widehat{K}$ are induced by the irreducible factors of $P(X)$ in $\widehat{K}[X]$.

2. Suppose that L/K is purely inseparable. Show that $L \otimes_K \widehat{K}$ has only one maximal ideal.

Archimedean case. Let L be a number field with r_1 real embeddings and $2r_2$ imaginary embeddings.

Proposition 1.68. *The usual absolute value $|\ |_\infty$ on $\mathbb{Q}$ admits exactly r_1 extensions to L with completions isomorphic to $\mathbb{R}$ and r_2 extensions to L with complexion isomorphic to $\mathbb{C}$.*

Proof. TD. □

1.6 Topological structure of K

First recall the definition of product topology. Let $\{X_i\}_{i\in I}$ be a (possibly infinite) familly of topological spaces. Let $X = \prod_{i\in I} X_i$. Then the product topology is exactly that one which makes all the projections $p_i : X \to X_i$ continuous. This means that for any finite subset $J \subset I$ and for any family of open subsets $\{U_j\}_{j\in J}$, $U_j \subseteq X_j$, the (finite) intersection $\cap_{j\in J} p_j^{-1}(U_j)$ must be open, and that these kind of subsets form a basis of topology.

If the case $I = \mathbb{N}$ and the X_i's are all discrete (all subsets of X_i are open, or equivalently, all singletons are open) , then a basis of topology for X is given by the subsets of the form $\cap_{0\le k\le n-1} p_k^{-1}(x_j)$, for any $n \in \mathbb{N}$ and for any points $x_j \in X_j$ (the n-th first coordinates are fixed, and no conditions on the other coordinates).

Let $(K, |\ |)$ be a non-trivial complete ultrametric valued field. Fix an element $t \in K$ such that $0 < |t| < 1$. Let $\Sigma \subset \mathcal{O}_K$ be a complete system of representatives of the quotient set $\mathcal{O}_K/t\mathcal{O}_K$. We choose $0 \in K$ as a representative of the class of 0. Endow Σ with the discrete topology and $\Sigma^{\mathbb{N}}$ with the product topology.

Proposition 1.69. *The map*

$$f :\ \Sigma^{\mathbb{N}} \to \mathcal{O}_K,\ (x_n)_{n\ge 0} \mapsto \sum_{n\ge 0} x_n t^n$$

is a homeomorphism.

Proof. First as $|x_n t^n| \le |t|^n$ converges to 0, the infinite sum converges in K and f is well-defined.

Let $\underline{x} \neq \underline{y} \in \Sigma^{\mathbb{N}}$. Let n_0 be the smallest integer such that $x_{n_0} \neq y_{n_0}$. Let us show that

$$|f(\underline{x}) - f(\underline{y})| = |x_{n_0} - y_{n_0}||t|^{n_0} > |t|^{n_0+1}. \tag{2}$$

Indeed, let $z_0 = x_{n_0} - y_{n_0}$. As x_{n_0} and y_{n_0} have distinct images in $\mathcal{O}_K/t\mathcal{O}_K$, $|z_0| > |t|$. We can write

$$f(\underline{x}) - f(\underline{y}) = z_0 t^{n_0}(1 + (z_0^{-1}t) \sum_{n \geq n_0+1} (x_n - y_n)t^{n-n_0-1})$$

with $|x_n - y_n| \leq 1$ for all $n > n_0$ and $|z_0^{-1}t| < 1$. This implies the desired equality and inequality. The injectivity of f follows.

Let us prove the surjectivity of f. We have $f(0) = 0$. Let $x \in \mathcal{O}_K$ non-zero, there exists $n_0 \in \mathbb{N}$ such that $|x| \leq |t|^{n_0}$. Let $a_0 \in \Sigma$ be a representative of the class of $x/t^{n_0} \in \mathcal{O}_K$. Then $|x - a_0 t^{n_0}| \leq |t|^{n_0+1}$. Let $a_1 \in \mathcal{O}_K$ be a representative of $t^{-(n_0+1)}(x - a_0 t^{n_0})$, then

$$|x - a_0 t^{n_0} - a_1 t^{n_0+1}| \leq |t|^{n_0+2}.$$

We construct inductively a sequence $(a_n)_{n \geq 0}$ in Σ such that

$$x = \sum_{n \geq 0} a_n t^{n_0+n}.$$

Therefore f is surjective.

It remains to prove that f is a homeomorphism. Let $\lambda \in \mathcal{O}_K$ and let $m \in \mathbb{N}$. Let us determine the pre-image by f of the closed disc $D(\lambda, |t|^m)$. Let $\lambda = f(\underline{a})$. Let $\underline{x} = (x_n)_n \in \Sigma^{\mathbb{N}}$ and different from $\underline{a}$. Let n_0 be the smallest integer such that $x_{n_0} \neq a_{n_0}$. By Equation (2), the condition is $|x_{n_0} - a_{n_0}||t|^{n_0} \leq |t|^m$. Which is equivalent to $n_0 \geq m$. So

$$f^{-1}(D(\lambda, |t|^m)) = \{(x_n)_n \in \Sigma^{\mathbb{N}} \mid x_n = a_n, \forall n \leq m - 1.\}$$

and it is open in $\Sigma^{\mathbb{N}}$. Therefore f transforms a basis of topology for $\Sigma^{\mathbb{N}}$ to a basis of topology of $\mathcal{O}_K$, it is thus a homeomorphism. □

Corollary 1.70. *If $\mathcal{O}_K/t\mathcal{O}_K$ is a finite set, then $\mathcal{O}_K$ is compact and K is locally compact.*

Proof. Finite discrete spaces are compact and product of any family of compact spaces is compact. Therefore $\mathcal{O}_K$ is compact. For any $\lambda \in K$, $\lambda + \mathcal{O}_K$ is a compact open neighborhood of λ, so K is locally compact. □

Remark 1.71 The only way to get a finite $\mathcal{O}_K/t\mathcal{O}_K$ is that $\mathcal{O}_K$ is given by a discrete valuation on K with finite residue field. Also $\mathcal{O}_K$ is not compact if $\mathcal{O}_K/t\mathcal{O}_K$ is infinite, because $\Sigma^{\mathbb{N}}$ is not compact.

Example 1.72 Let p be a prime number, we can take $\Sigma = \{0, 1, \cdots, p-1\}$. And we find that $\mathbb{Z}_p$ is compact and $\mathbb{Q}_p$ is locally compact.

2 Algebraic theory

In this section, we study ultrametric valued fields from the point of view of valuation rings. We will restrict ourselves to the case of discrete valuations. The rings we consider are commutative with unity.

References for this section are notes of J. Milne, `https://www.jmilne.org/math/CourseNotes/` "Fields and Galois Theory", and "Algebraic Number Theory".

2.1 Integral extensions

Let $A \subseteq B$ be integral domains. An element $b \in B$ is said to be *integral over* A if we have an (integral dependence) equation

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0$$

with $n \geq 1$ and $a_i \in A$. We say that B is *integral over* A if all elements of B are integral over A.

Proposition 2.1. *Let $b \in B$. Then the following properties are equivalent:*

1. *b is integral over A;*
2. *the sub-A-algebra $A[b]$ of B generated by b is finitely generated as A-module.*
3. *There exists a non-zero finitely generated A-module M, contained in B, such that $bM \subseteq M$.*

Corollary 2.2. *Let C be an integral domain, let B be a subring of C and let A be a subring of B.*

1. *The set of the elements of B integral over A is a sub-A-algebra of B.*
2. *(Transitivity) If B is integral over A and C is integral over B, then C is integral over A.*

Definition 2.3 The set of the elements of B integral over A is called the *integral closure of A in B*. When $B = \mathrm{Frac}(A)$, it is just called the *integral closure of A*. When A is equal to its integral closure, then A is said to be *integrally closed*.

Example 2.4 PIDs, and more generally, UFDs (Unique Factorial Domain, or factorial) are integrally closed.

Example 2.5 Let L be a number field (finite extension of $\mathbb{Q}$). The integral elements of L over $\mathbb{Z}$ are called the *integers of L*. The integral closure of $\mathbb{Z}$ in L is often denoted by $\mathcal{O}_L$.

Remark 2.6 Let $A \subseteq B$ be integral domains. If we have a domain B_0 with $A \subseteq B_0 \subseteq B$ and

1. $\mathrm{Frac}(B_0) = \mathrm{Frac}(B)$,
2. B_0 is integral over A,

3. B_0 is integrally closed,

then B_0 is the integral closure of A in B. Indeed, by (2), B_0 is contained in the integral closure. If $b \in B$ is integral over A, then it is integral B_0. As $b \in \mathrm{Frac}(B) = \mathrm{Frac}(B_0)$, (3) implies that $b \in B_0$.

Let A be an integral domain with $K = \mathrm{Frac}(A)$. Let L be a finite extension of K. If $b \in L$, a *conjugate* of b is a root (in some algebraic closure K^c of K) of the minimal polynomial of b over K. For any conjugate $b' \in K^c$ of b, we have a K-isomorphism $\sigma : K[b] \to K[b']$ taking b to b'. In particular, if b is integral over A, then so is b'.

Proposition 2.7. *Suppose A integrally closed. Let L be a finite extension of $K = \mathrm{Frac}(A)$. Let $b \in L$ be integral over A. Let $P(x)$ be the minimal polynomial of $b \in L$ over K. Then $P(x) \in A[x]$. In particular $\mathrm{Tr}_{L/K}(b), N_{L/K}(b) \in A$.*

Proof. The roots of $P(X)$ (in an algebraic closure K^c containing b) are all integral over A, so the coefficients of $P(X)$ are integral over A, but they also belong to K, so they belong to A by the hypothesis on A. □

Theorem 2.8. *Let A be a noetherian integrally closed domain with $K = \mathrm{Frac}(A)$. Let L/K be a finite separable extension. Then the integral closure B of A in L is a noetherian integrally closed domain, finitely generated over A (as A-module).*

Proof. Note first that for any $\lambda \in L$, there exists $a \in A$ non-zero such that $a\lambda \in B$. Indeed, if a is a commun denominator of the minimal polynomial of λ over K, then $a\lambda$ is integral over A.

By construction B is an integrally closed domain. Consider the K-bilinear form $L \times L \to K$ defined by the trace: $(x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$. A characterization of L/K being separable is that this bilinear form is nondegenerate. Let $e_1, \ldots, e_n$ be a basis of L with $e_i \in B$. Let $e_1^*, \ldots, e_n^*$ be the dual basis of L w.r.t. the trace form. For any $b \in B$, we have

$$b = \sum_i \lambda_i e_i^*, \quad \lambda_i \in K.$$

We have $\lambda_i = \mathrm{Tr}_{L/K}(be_i) \in A$. So $B \subseteq \sum_i Ae_i^*$. As A is noetherian, B is finitely generated over A and is therefore noetherian as well. □

2.2 Dedekind domains

Definition 2.9 A *Dedekind domain* is an integral domain A such that

1. A is noetherian;
2. A is integrally closed;
3. Non-zero prime ideals of A are maximal.

Example 2.10 Fields and principal ideal domains are Dedekind.

In a PID, any non-zero element is uniquely (up to permutation and multiplication by units) product of powers of prime elements. A fundamental fact on Dedekind domains is that this property holds when replacing elements of the ring by ideals.

Theorem 2.11 (Decomposition of ideals)**.** *Let A be a Dedekind domain. Let I be a non-zero ideal of A. Then there exist pairwise distinct maximal ideals $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ and positive integers $r_1, \dots, r_n$ such that*

$$I = \mathfrak{m}_1^{r_1} ... \mathfrak{m}_n^{r_n}.$$

Moreover, the $\mathfrak{m}_i$'s are exactly the maximal ideals of A containing I, and the set of the $(\mathfrak{m}_i, r_i)$'s is unique.

By convention, if $I = A$, then the product is indexed by the empty set.

Proof. See Milne, ANT, Theorem 3.7. □

Definition 2.12 A *local ring* is a ring with a unique maximal ideal. If $\mathfrak{p}$ is a prime ideal in a ring A, then the localization $A_\mathfrak{p}$ of A with respect to $A \setminus \mathfrak{p}$ is a local ring. Its maximal ideal is $\mathfrak{p}A_\mathfrak{p}$.

Proposition 2.13. *Let A be a Dedekind domain, let $S \subset A$ be a multiplicative subset, then $S^{-1}A$ is also a Dedekind domain.*

Proof. It is straightforward to check that $S^{-1}A$ is noetherian and integrally closed. Let $\mathfrak{q} \subset S^{-1}A$ be a non-zero prime ideal. Then $\mathfrak{p} := \mathfrak{q} \cap A$ is a prime ideal. Let $\beta = a/s \in \mathfrak{p}$ with $a \in A$, $s \in S$, then $a \in \mathfrak{p}$. We see in this way that $\mathfrak{q} = \mathfrak{p}S^{-1}A$.

As $\mathfrak{q}$ is non-zero, $\mathfrak{p}$ is non-zero thus maximal. If $\mathfrak{q} \subset \mathfrak{m}$ for a prime ideal of $S^{-1}A$, then $\mathfrak{m} \cap A = \mathfrak{p}$, so $\mathfrak{m} = \mathfrak{p}S^{-1}A = \mathfrak{q}$.

(As a general fact, the map

$$\{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} \cap S = \emptyset\} \to \operatorname{Spec}(S^{-1}A),\ \mathfrak{p} \mapsto \mathfrak{p}S^{-1}A$$

is a bijection whose inverse map is $\mathfrak{q} \mapsto \mathfrak{q} \cap A$.) □

Corollary 2.14. *Let $\mathfrak{m}$ be a maximal ideal of A, then the local ring $A_\mathfrak{m}$ is a Dedekind domain.*

2.3 Discrete valuation rings

Proposition 2.15. *Any local Dedekind domain $(A, \mathfrak{m})$ is principal.*

Proof. We can suppose that A is not a field. Let I be a non-zero ideal of A. By the decomposition theorem, we have $I = \mathfrak{m}^n$ for some $n \geq 0$. So it is enough to show that $\mathfrak{m}$ is principal. By the uniqueness of in the theorem of decomposition or by Nakayama's lemma, we have $\mathfrak{m} \neq \mathfrak{m}^2$. Take $t \in \mathfrak{m} \smallsetminus \mathfrak{m}^2$. Write $tA = \mathfrak{m}^r$ for some $r \geq 1$. As $t \notin \mathfrak{m}^2$, we have $r \leq 1$. So $r = 1$ and $\mathfrak{m} = tA$ is principal. □

Let $(A, \mathfrak{m})$ be a local Dedekind domain with $\mathfrak{m} \neq 0$. For any $a \in A$ non-zero, there is a unique integer $v(a) \geq 0$ such that $aA = \mathfrak{m}^{v(a)}$ by the decomposition theorem. If we chose a generator t of $\mathfrak{m}$, then this is equivalent to $a = t^{v(a)}u$ with $u \in A^*$ (a unit of A).

This defines a map $v : A \smallsetminus \{0\} \to \mathbb{N}$ such that $v(ab) = v(a) + v(b)$. Therefore it extends to a valuation $v : K^* \to \mathbb{Z}$ (where $K = \mathrm{Frac}(A)$) with $v(K^*) = \mathbb{Z}$.

Conversely, let K be a field endowed with a valuation $v : K^* \to \mathbb{R}$ whose image is a non-zero discrete subgroup (hence equal to some $n_0\mathbb{Z}$). Then $v/n_0 : K^* \to \mathbb{Z}$ is surjective and is called a *normalized* discrete valuation.

Lemma 2.16. *In the above settings, the valuation ring $\mathcal{O}_K$ is a local Dekedind domain which is not a field.*

Proof. First we prove that $\mathcal{O}_K$ is a PID. For any non-zero ideal $I \subseteq \mathfrak{m}_K$ non-zero, we consider $r = \min\{v(a) \mid a \in I,\ a \neq 0\} = v(a_0)$. For any $a \in I$, $v(a/a_0) \geq 0$, so $a \in a_0 A$ and $I = a_0 A$ is principal.

For $a \in K^*$, we have $a \in \mathcal{O}_K^*$ if and only if $v(a) = 0$ so $\mathcal{O}_K^* = \mathcal{O}_K \smallsetminus \mathfrak{m}_K$. This is equivalent to $\mathfrak{m}_K$ being the unique maximal ideal of $\mathcal{O}_K$. □

Definition 2.17 A *discrete valuation ring* is a local Dedekind domain A which is not a field. Equivalently, it is the valuation ring of a non-trivial discrete valuation on $\mathrm{Frac}(A)$.

Example 2.18 For any prime number p, $\mathbb{Z}_p$ and $\mathbb{Z}_{p\mathbb{Z}}$ are discrete valuation rings.

2.4 Extensions of Dedekind domains

Lemma 2.19. *Let $A \to B$ be an integral extension of integral domains.*

1. *A is a field if and only if B is a field.*
2. *Let $\mathfrak{p}$ be a prime ideal of B. Then $\mathfrak{p}$ is maximal if and only if $\mathfrak{p} \cap A$ is a maximal ideal of A.*
3. *If all non-zero prime ideals of A are maximal, then the same property holds for B.*

Proof. See Exercise 2 in TD4. □

Theorem 2.20. *Let A be a Dedekind domain. Let L be a finite separable extension of $K := \mathrm{Frac}(A)$ and let B be the integral closure of A in L.*

1. *The ring B is a Dedekind domain, finite over A (as A-module).*

2. *For any maximal ideal* $\mathfrak{n}$ *of* A*, there are only finitely maximal ideals* $\mathfrak{m}$ *of* B *which contain* $\mathfrak{n}$*.*

Proof. (1) By construction B is integrally closed. It is noetherian and finite over A by Theorem 2.8. By Lemma 2.19, B is a Dedekind domain.

(2) Apply the decomposition theorem 2.11 to the ideal $\mathfrak{n}B$ of B. □

Corollary 2.21. *The ring of integers in a number field* L *(Example 2.5) is a Dedekind domain and is module-finite over* $\mathbb{Z}$*.*

Remark 2.22 By a theorem of Krull-Akizuki, even if L/K is not separable, B is still a Dedekind domain, but not necessary finite over A. We will prove below this result when A is *semi-local*, *i.e.* has only has finitely maximal ideals. In the rest of the this subsection we will prove this theorem is a special case (Corollary 2.26).

Definition 2.23 In an algebraic extension of fields L/K, an element $\alpha \in L$ is *separable over* K if its minimal polynomial over K is a separable polynomial. An algebraic extension is *separable* if all its elements are separable over K.

It is known that the set of elements in L separable over K form a separable extension, called *separable closure of* K *in* L.

An algebraic extension L/K is *purely inseparable* if the separable closure of K in L is K itself. This is equivalent to the fact that $\mathrm{char}(K) = p > 0$ for any element $x \in L$, there exists a positive integer $e > 0$ such that $x^{p^e} \in K$. If moreover L/K is finite, then there exists such an e which works for all $x \in L$.

Lemma 2.24. *Let* $\mathcal{O}_K$ *be a discrete valuation ring with field of fractions* K*. Let* L/K *be a finite purely inseparable extension. Then the integral closure of* $\mathcal{O}_K$ *in* L *is a discrete valuation ring.*

Proof. Let p be the characterisitc of K. Let $e \geq 1$ be such that for all $x \in L$ we have $x^{p^e} \in K$.

(1) Let $x \in L$. Then x is integral over $\mathcal{O}_K$ if and only if $x^{p^e} \in \mathcal{O}_K$. The if part is obvious. Suppose that x is integral over $\mathcal{O}_K$. Then $x^{p^e} \in K$ and is integral over $\mathcal{O}_K$, thus $x^{p^e} \in \mathcal{O}_K$ as the latter is integrally closed.

(2) Let v_K be a valuation on K correspong to $\mathcal{O}_K$. Define for all $x \in L$, $v_L(x) := v_K(x^{p^e})/p^e$. This is a discrete valuation on L. By (1), its valuation ring coincides with the integral closure of $\mathcal{O}_K$ in L. □

Lemma 2.25. *Let* A *be a semi-local noetherian domain, let* B *be an integral domain, integral over* A*. If for any maximal ideal* $\mathfrak{m} \subset A$*,* $A_\mathfrak{m} \otimes_A B$ *is noetherian, then* B *is noetherian.*

Proof. Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ be the maximal ideals of A. Denote by $B_i = A_{\mathfrak{m}_i} \otimes_A B = S_i^{-1}B$ where $S_i = A \setminus \mathfrak{m}_i$ is a multiplicative subset of B.

(1) Let I be an ideal of B. Then the pre-image by $B \to \prod_i B_i$ of $\prod_i (IB_i)$ is equal to I. Indeed, let $x \in B$ be such that $x \in IB_i$ for all $i \leq r$. Consider $J := \{a \in A \mid ax \in I\}$. This is an ideal of A. If $J = A$, then $1 \in J$ and $x \in I$. Suppose $J \neq A$, then it is contained in some $\mathfrak{m}_i$. But $x \in IB_i$ implies that there exists $s_i \in A \setminus \mathfrak{m}_i$ such that $s_i x \in I$. So $s_i \in J \subseteq \mathfrak{m}_i$. Hence $s_i \in \mathfrak{m}_i$, contradiction.

(2) Let I be an ideal of B. Then IB_i is finitely generated for all $i \leq n$. There exists a finite system of generators of IB_i beloning to I (the denominators are invertible in B_i). So there exists a finite subset of I which generates IB_i for each $i \leq n$. Let I' be the ideal of B generated by this subset. We have $IB_i = I'B_i$ for all $i \leq n$. By (1) $I = I'$ and I is finitely generated. □

Corollary 2.26. *Let A be a semi-local Dedekind domain. Let L be a finite extension of $K = \mathrm{Frac}(A)$. Then the integral closure B of A in L is a semi-local Dedekind domain.*

Proof. Denote by F the separable closure of K in L and by B' the integral closure of A in F. By Theorem 2.20, B' is a semi-local Dedekind domain.

To finish the proof we can replace A with B' and suppose that L/K is purely inseparable. For any maximal ideal $\mathfrak{m}$ of A, $A_{\mathfrak{m}} \otimes_A B$ is integral over $A_{\mathfrak{n}}$, and being a localization of B, is integrally closed. Therefore $A_{\mathfrak{m}} \otimes_A B$ is the integral closure of $A_{\mathfrak{m}}$ in L. By Lemma 2.24, it is a discrete valuation ring, hence noetherian. By Lemma 2.25, B is noetherian. It is a Dedekind domain by Lemma 2.19.

Finally we need to check that B is semi-local. Let $p = \mathrm{char}(K) > 0$, let $e \geq 1$ be such that $L^{p^e} \subseteq K$. Then as we saw in the proof of Lemma 2.24, $B^{p^e} \subseteq A$. Let $\mathfrak{m}$ be a maximal of B. Then $\mathfrak{m} \cap A = \mathfrak{m}_0$ is a maximal ideal of A (Lemma 2.19). As $\mathfrak{m}^{p^e} \subset \mathfrak{m} \cap A = \mathfrak{m}_0$, we have $\mathfrak{m} \subseteq \sqrt{\mathfrak{m}_0 B} \subseteq \sqrt{\mathfrak{m}} = \mathfrak{m}$. Thus $\mathfrak{m} = \sqrt{\mathfrak{m}_0 B}$. This means that there is only one maximal ideal of B containing a given maximal ideal of A. But any maximal ideal of B contains a maximal ideal of A (Lemma 2.19), so we have a bijection between the maximal ideals of A and that of B. Therefore B is semi-local as A. □

Example 2.27 Let k be a field of characteristic $p > 0$. Let $k((t)) = \mathrm{Frac}(k[[t]])$ be endowed with the (discrete) t-adic valuation. By a dimension argument (or cardinality argument if we take a finite field k), we know that there exists $s \in k[[t]]$ which is not algebraic over $k(t)$. Let

$$K := k(t, s^p) \subset L := k(t, s) \subset k((t))$$

both endowed with the restriction of the t-adic valuation. By Lemma 2.24, the integral closure of $\mathcal{O}_K$ in L coincides with $\mathcal{O}_L$.

Now let us show that $\mathcal{O}_L$ is not finite over $\mathcal{O}_K$. If it was, then it is free of some finite rank $d \geq 1$ over $\mathcal{O}_K$ because the latter is a PID. Hence $\mathcal{O}_L/(t)$ is free of rank d over $\mathcal{O}_K/(t)$. But both quotients are equal to k, so $d = 1$ and $\mathcal{O}_L = \mathcal{O}_K$. Impossible because $[L : K] = p > 1$.

Now we can give an algebraic interpretation of Proposition 1.61 in the case of discrete valued fields.

Proposition 2.28. *Let $(K, |\ |_K)$ be a valued field given by a discrete valuation v_K on K. Let L/K be a finite extension. Let $\widetilde{\mathcal{O}}_K$ be the integral closure of $\mathcal{O}_K$ in L. There is a bijection between the extensions of $|\ |_K$ to L and the maximal ideals of $\widetilde{\mathcal{O}}_K$.*

Proof. Let $\mathfrak{m}$ be a maximal ideal of $\widetilde{\mathcal{O}}_K$. Then $(\widetilde{\mathcal{O}}_K)_{\mathfrak{m}}$ is a discrete valuation ring. Let $v_{\mathfrak{m}} : L^* \to \mathbb{Z}$ be the corresponding normalized valuation. Let $t \in \mathcal{O}_K$ be a uniformizing element of $\mathcal{O}_K$. Then $v_{\mathfrak{m}}(t)^{-1} v_{\mathfrak{m}} : L^* \to \mathbb{Q}$ is a valuation

extending v_K. The maximal ideal of this valuation ring $\mathfrak{m}(\widetilde{\mathcal{O}}_K)_{\mathfrak{m}}$, so different maximal ideals give different extensions of v_K.

Conversely, let $v_L : L^* \to \mathbb{R}$ be a valuation extending v_K. Let $\mathcal{O}_{v_L}$ be its valuation ring. It contains $\widetilde{\mathcal{O}}_K$: indeed for any $b \in \widetilde{\mathcal{O}}_K$, we have an integral dependence equation

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$$

with $a_i \in A \subseteq \mathcal{O}_{v_L}$, hence $v_L(b) \geq 0$.

Let $\mathfrak{m} = \widetilde{\mathcal{O}}_K \cap \mathfrak{m}_{v_L}$. This is a prime ideal of $\widetilde{\mathcal{O}}_K$ containing $\mathfrak{m}_K$, hence non-zero. So $\mathfrak{m}$ is a maximal ideal. Let us show that $(\widetilde{\mathcal{O}}_K)_{\mathfrak{m}} = \mathcal{O}_{v_L}$. This will imply that $v_L = v_{\mathfrak{m}}$.

Let $s \in \widetilde{\mathcal{O}}_K \smallsetminus \mathfrak{m}$, then $s \in \mathcal{O}_{v_L} \smallsetminus \mathfrak{m}_{v_L}$, hence $v_L(s) = 0$ and $s \in \mathcal{O}_{v_L}^*$. This implies that $(\widetilde{\mathcal{O}}_K)_{\mathfrak{m}} \subseteq \mathcal{O}_{v_L}$. Let $x \in \mathcal{O}_{v_L}$. If $x \notin (\widetilde{\mathcal{O}}_K)_{\mathfrak{m}}$, then $1/x \in \mathfrak{m}(\widetilde{\mathcal{O}}_K)_{\mathfrak{m}} \subset \mathfrak{m}_{v_L}$, and $v_L(x) = -v_L(1/x) < 0$, contradiction. □

Exercise 2.29 Show that any semi-local Dedekind domain is a PID (use the Chinese Remainder Theorem).

3 Ramification

The general setting in this section is the following:

1. $\mathcal{O}_K$ is a non-trivial discrete valuation ring with field of fractions K;
2. the maximal ideal of $\mathcal{O}_K$ is denoted by $\mathfrak{m}_K$; π_K will be a generator of $\mathfrak{m}_K$;
3. the residue field $\mathcal{O}_K/\mathfrak{m}_K$ is denoted by k.

An *extension of discrete valuation rings* is a pair of discrete valuation rings $\mathcal{O}_K$, $\mathcal{O}_L$ such that $\mathcal{O}_K \subseteq \mathcal{O}_L$ and $\mathfrak{m}_K \subseteq \mathfrak{m}_L$. The ramification theory studies such extensions (mostly when the corresponding extension of the fields of fractions L/K is finite).

3.1 Ramification index and residue extension

Definition 3.1 Let $\mathcal{O}_K \to \mathcal{O}_L$ be an extension of dvr's. Write $\mathfrak{m}_K\mathcal{O}_L = \mathfrak{m}_L^e\mathcal{O}_L$. Then e is called the *ramification index of* $\mathcal{O}_L$ *over* $\mathcal{O}_K$. It is denoted by $e_{\mathcal{O}_L/\mathcal{O}_K}$. The extension $k \to \kappa_L = \mathcal{O}_L/\mathfrak{m}_L$ is called the *residue extension*. The degree $[\kappa_L : k]$ is called the *residue degree* and often denoted by $f_{\mathcal{O}_L/\mathcal{O}_K}$.

The ramification index e and the residue extension are also called (slightly abusively) the ramification index and the residue extension of L/K. Then $e_{\mathcal{O}_L/\mathcal{O}_K}$ and $f_{\mathcal{O}_L/\mathcal{O}_K}$ are respectively denoted by $e_{L/K}$ and $f_{L/K}$. There is no ambiguity if $\widetilde{\mathcal{O}}_K$ is local.

Example 3.2 Covers of regular algebraic curves (or Riemann surfaces). Let $K = \mathbb{C}(z)$ and let d be an integer ≥ 2. Let $L = K(z)[t]$ with $t^d = z$. Then $K \to L$ is unramified outside of $z = 0$. Above $z = 0$ (that is K with the z-adic valuation), the ramification index is d. From a geometric point of view, the graph of the "function" $t = z^{1/d}$ has d leaves outside of $z = 0$, they all meet at the point $z = t = 0$.

The map $\mathbb{C}^* \to \mathbb{C}^*$, $z \mapsto z^d$ is a topological cover of degree d.

Example 3.3 Let $K = \mathbb{Q}$ be endowed with the 2-adic valuation, and let $L = \mathbb{Q}[\sqrt{2}]$. The integral closure of $\mathbb{Z}$ in L is $\mathbb{Z}[\sqrt{2}]$ because 2 is not congruent to 1 mod 4. We saw that the 2-adic valuation has a unique extension to L. The ramification index is 2, and the residue extension is trivial.

Lemma 3.4. *Let $\mathcal{O}_K \to \mathcal{O}_L \to \mathcal{O}_F$ be extensions of discrete valuation rings.*

1. *(Transitivity) We have $e_{F/K} = e_{F/L}e_{L/K}$ and $f_{F/K} = f_{F/L}f_{L/K}$.*
2. *The extension $K \to \widehat{K}$ has ramification index 1 and trivial residue extension.*
3. *The ramification index and residue extension of $\widehat{K} \to \widehat{L}$ are the same as that of $K \to L$.*

Proof. Straightforward. □

We are going to prove Theorem 3.9 which relates the above invariants to the degree of L/K. We need some preparations. For any $\mathcal{O}_K$-algebra B, the quotient $B/\mathfrak{m}_K B$ is canonically a k-algebra (hence a k-vector space).

Lemma 3.5. *Let $\mathcal{O}_K \to \mathcal{O}_L$ be an extension of discrete valuation rings with ramification index e. Let κ_L be the residue field $\mathcal{O}_L/\mathfrak{m}_L$ of $\mathcal{O}_L$ and let $f = [\kappa_L : k]$ be the residue degree. Then*

$$\dim_k(\mathcal{O}_L/\mathfrak{m}_K\mathcal{O}_L) = ef \in \mathbb{N} \cup \{+\infty\}.$$

Proof. Fix a uniformizing element π_L of $\mathcal{O}_L$. Then $\mathfrak{m}_K\mathcal{O}_L = \pi_L^e\mathcal{O}_L$.

(1) Let $b_1, \dots, b_n \in \mathcal{O}_L$ be such that their classes in κ_L are k-linearly independent. Then the image of the family $\{\pi_L^i b_j \mid 0 \le i \le e-1,\ 1 \le j \le n\}$ in $\mathcal{O}_L/\mathfrak{m}\mathcal{O}_L$ is linearly independent over k.

Indeed, let $a_{ij} \in \mathcal{O}_K$ be such that

$$\sum_{i,j} a_{ij}(\pi_L^i b_j) \in \mathfrak{m}_K\mathcal{O}_L.$$

with at least one $a_{i_0,j_0} \in \mathcal{O}_K^*$. Choose i_0 to be the smallest possible. Then $a_{i,j}\pi_L^i b_j \in a_{i,j}\mathcal{O}_K \subseteq \mathfrak{m}_K\mathcal{O}_L$ for all $i < i_0$, and $a_{i,j}\pi_L^i b_j \in \pi_L^{i_0+1}\mathcal{O}_L$ if $i > i_0$. Therefore

$$\sum_{j\le n} a_{i_0,j}(\pi_L^{i_0} b_j) \in \mathfrak{m}_L^{i_0+1}$$

and

$$\sum_{j\le n} a_{i_0,j} b_j \in \mathfrak{m}_L.$$

Contradiction. The property (1) implies that $ef \le \dim_k(\mathcal{O}_L/\mathfrak{m}_K\mathcal{O}_L)$ (whenever the latter is finite).

(2) Conversely, suppose that f is finite. Let $b_1, \dots, b_f \in \mathcal{O}_L$ be the lifting of a basis of κ_L over k. Then $\mathcal{O}_L \subseteq \sum_{1\le j\le f} b_j\mathcal{O}_K + \pi_L\mathcal{O}_L$. Multiplying the inclusion by π_L implies that $\pi_L\mathcal{O}_L \subseteq \sum_{1\le j\le f} b_j\pi_L\mathcal{O}_K + \pi_L^2\mathcal{O}_L$, thus

$$\mathcal{O}_L \subseteq \sum_{1\le j\le f} b_j\mathcal{O}_K + \sum_{1\le j\le f} b_j\pi_L\mathcal{O}_K + \pi_L^2\mathcal{O}_L.$$

Repeating this operation we get for any $N > 0$

$$\mathcal{O}_L \subseteq \sum_{1\le j\le f,\ 0\le i\le N} b_j\pi_L^i\mathcal{O}_K + \pi_L^{N+1}\mathcal{O}_L.$$

Consider the $\mathcal{O}_K$-module $M = \sum_{1\le j\le f,\ 0\le i\le e-1} b_j\pi_L^i\mathcal{O}_K$. Taking $N = e-1$ we get

$$\mathcal{O}_L \subseteq M + \pi_K\mathcal{O}_L = M + \mathfrak{m}_K\mathcal{O}_L.$$

Hence $\mathcal{O}_L/\mathfrak{m}_K\mathcal{O}_L$ is generated by the classes of the $b_j\pi_L^i$ for $1 \le j \le f$ and $0 \le i \le e-1$. Hence $\dim_k(\mathcal{O}_L/\mathfrak{m}_K\mathcal{O}_L) \le ef$. Note (for the proof of the next lemma) that

$$\mathcal{O}_L \subseteq M + \pi_K^n\mathcal{O}_L \tag{3}$$

for all $n \ge 1$. □

Lemma 3.6. *We have*

$$\dim_k \widetilde{\mathcal{O}}_K/\mathfrak{m}_K\widetilde{\mathcal{O}}_K \le [L : K].$$

The equality holds if K is complete.

Proof. Let $b_1, \dots, b_n \in \widetilde{\mathcal{O}}_K$ be such that their images in the quotient is free over k. Let us show that they form a K-free family (this then imply the desired inequality). Suppose the contrary. Let $a_1, \dots, a_n \in K$ be such that $\sum_i a_i b_i = 0$ and such that not all a_i are zero. Dividing by a a_{i_0} with the smallest valuation, we can suppose that $a_i \in \mathcal{O}_K$ and that at least one $a_i \in \mathcal{O}_K^*$. Passing to the quotient $\widetilde{\mathcal{O}}_K/\mathfrak{m}_K\widetilde{\mathcal{O}}_K$ we see that the classes of the b_i's is not free. Contradiciton.

Suppose now K is complete. Then $\widetilde{\mathcal{O}}_K = \mathcal{O}_L$ is a discrete valuation ring (Proposition 2.28 and Theorem 1.57) . By Lemma 3.5, it is enough to show that $ef \geq [L : K]$. Let $b_1, \dots, b_f \in \mathcal{O}_L$ be the lifting of a basis of κ_L over k. Let M be as in the proof of the above lemma. Then M is dense in $\mathcal{O}_L$ by the inclusion (3). So $M \otimes_{\mathcal{O}_K} K$ is dense in, hence equal to, L because K is complete and $\dim_K L < +\infty$. This implies that $[L : K] = \dim_K(M \otimes_{\mathcal{O}_K} K) \leq ef$. □

Remark 3.7 In the end of the proof above we proved that $\mathcal{O}_L = M$ is finitely generated over $\mathcal{O}_K$.

Lemma 3.8. *Let A be a ring, let $\mathfrak{m}$ be a maximal ideal of A. Then for any integer $r \geq 1$, the canonical homomorphism $A/\mathfrak{m}^r \to A_\mathfrak{m}/\mathfrak{m}^r A_\mathfrak{m}$ is an isomorphism.*

Proof. Quick proof: as a general fact, localization commutes with quotient, $A_\mathfrak{m}/\mathfrak{m}^r A_\mathfrak{m} = (A/\mathfrak{m}^r)_{\bar{\mathfrak{m}}} = A/\mathfrak{m}^r$ because in $A/\mathfrak{m}^r$ the complement of $\bar{\mathfrak{m}}$ consists in invertible elements.

Proof for newbies: Let us suppose A is integral for simplicity, so we can consider $A_\mathfrak{m}$ as a subdomain of $\mathrm{Frac}(A)$. Note that for any $s \in A \smallsetminus \mathfrak{m}$, we have

$$A = sA + \mathfrak{m}^r.$$

Let $a = x_r/s \in \mathfrak{m}^r A_\mathfrak{m} \cap A$ with $x_r \in \mathfrak{m}^r$ and $s \in A \smallsetminus \mathfrak{m}$. Write $1 = sa_0 + y_r$ with $a_0 \in A$ and $y_r \in \mathfrak{m}^r$. Then $a = x_r a_0 + a y_r \in \mathfrak{m}^r$. So $A/\mathfrak{m}^r \to A_\mathfrak{m}/\mathfrak{m}^r A_\mathfrak{m}$ is injective.

Let $a/s \in A_\mathfrak{m}$. Use again $1 = sa_0 + y_r$ to get $a/s = aa_0 + ay_r/s \in A + \mathfrak{m}^r A_\mathfrak{m}$. This implies the surjectivity. □

Let L/K be a finite extension. Consider the decomposition of $\mathfrak{m}_K\widetilde{\mathcal{O}}_K$

$$\mathfrak{m}_K\widetilde{\mathcal{O}}_K = \prod_{1 \leq i \leq n} \mathfrak{m}_i^{e_i}$$

in $\widetilde{\mathcal{O}}_K$ (Theorem 2.11). Note that the $\mathfrak{m}_i$'s are exactly the maximal ideals of $\widetilde{\mathcal{O}}$ (Lemma 2.19(2)). Denote by $\kappa_i = \widetilde{\mathcal{O}}_K/\mathfrak{m}_i$.

Theorem 3.9. *We have the inequality*

$$\sum_{1 \leq i \leq n} e_i[\kappa_i : k] \leq [L : K]. \tag{4}$$

Moreover, the following properties are equivalent:

(i) *The equality in* (4) *holds;*

(ii) *$\widetilde{\mathcal{O}}_K$ is (module-)finite over $\mathcal{O}_K$;*

(iii) *The ring $L \otimes_K \widehat{K}$ is reduced.*

Proof. By the Chinese Remainder Theorem and Lemma 3.8, we have canonical isomorphisms

$$\widetilde{\mathcal{O}}_K/\mathfrak{m}_K\widetilde{\mathcal{O}}_K \simeq \prod_{1\le i\le n} \widetilde{\mathcal{O}}_K/\mathfrak{m}_i^{e_i} \simeq \prod_{1\le i\le n} (\widetilde{\mathcal{O}}_K)_{\mathfrak{m}_i}/\mathfrak{m}_i^{e_i}(\widetilde{\mathcal{O}}_K)_{\mathfrak{m}_i}. \tag{5}$$

By Lemmas 3.5 and 3.6,

$$[L:K] \ge \dim_k \widetilde{\mathcal{O}}_K/\mathfrak{m}_K\widetilde{\mathcal{O}}_K = \sum_{1\le i\le n} e_i[\kappa_i : k].$$

The equality in (4) holds if and only if

$$\dim_k \widetilde{\mathcal{O}}_K/\mathfrak{m}_K\widetilde{\mathcal{O}}_K = [L:K]. \tag{6}$$

(ii) $\Longrightarrow$ (i). If $\widetilde{\mathcal{O}}_K$ is finite over $\mathcal{O}_K$ then it is free of rank $[L:K]$ and Equality (6) holds.

(i) $\Longrightarrow$ (ii). Suppose that the equality (6) holds. Let $b_1, \dots, b_m \in \widetilde{\mathcal{O}}_K$ be a lifting of a basis of $\widetilde{\mathcal{O}}_K/\mathfrak{m}_K\widetilde{\mathcal{O}}_K$ over k. Then this family is free over $\mathcal{O}_K$. As $m = [L:K]$, it is also a basis of L over K. Let $b \in \widetilde{\mathcal{O}}_K$. There exist $\lambda_1, \dots, \lambda_m \in K$ such that $b = \sum_{1\le i\le m} \lambda_i b_i$. Let $r = \min_i\{v_K(\lambda_i)\}$. Then $b = \pi_K^r \sum_i (\pi_K^{-r}\lambda_i) b_i$. As the b_i's are free over k, this implies that $r \ge 0$. So $\lambda_i \in \mathcal{O}_K$ and the b_i's is a basis of $\widetilde{\mathcal{O}}_K$ over $\mathcal{O}_K$.

(iii) and (i). (Not presented during the lecture) Fix an absolute value $|\ |_K$ corresponding to the valuation on K. For each $i \le n$, denote by $|\ |_i$ the extension of $|\ |_K$ to L corresponding to the maximal ideal $\mathfrak{m}_i$ (so $\mathcal{O}_{(L,|\ |_i)} = (\widetilde{\mathcal{O}}_K)_{\mathfrak{m}_i}$). Denote by $\widehat{L}_i$ the completion of $(L, |\ |_i)$. Then $e_{\widehat{L}_i/\widehat{K}} = e_i$ and $\kappa_{\widehat{L}_i} = \kappa_i$ (Lemma 3.4). By Lemmas 3.5, 3.6, $e_i[\kappa_i : k] = \sum_{1\le i\le n} [\widehat{L}_i : \widehat{K}]$. Thus

$$\sum_{1\le i\le n} e_i[\kappa_i : k] = \sum_{1\le i\le n} [\widehat{L}_i : \widehat{K}] = \dim_{\widehat{K}} \big(\prod_{1\le i\le n} \widehat{L}_i \big).$$

We have a surjective $\widehat{K}$-linear map

$$L \otimes_K \widehat{K} \to \prod_{1\le i\le n} \widehat{L}_i$$

whose kernel is nilpotentl. As $\dim_{\widehat{K}}(L \otimes_K \widehat{K}) = [L:K]$, we see that Equality (6) holds if and only if $L \otimes_K \widehat{K}$ is reduced. □

Corollary 3.10. *Let L/K be a finite extension. If L/K is separable or if K is complete, then*

$$[L:K] = \sum_{1\le i\le n} e_i[\kappa_i : k].$$

From now on, we only consider finite extensions L/K such that

$$\widetilde{\mathcal{O}}_K \quad \textbf{is finite over} \quad \mathcal{O}_K. \tag{7}$$

Below we give a method to compute the ramification data when $\widetilde{\mathcal{O}}_K$ has a simple form.

Proposition 3.11. *Let L/K be a finite extension. Suppose that $\widetilde{\mathcal{O}}_K = \mathcal{O}_K[\alpha]$ for some α. Let $P(X) \in \mathcal{O}_K[X]$ be the minimal polynomial of α over K. Let*

$$\bar{P}(X) = \prod_{1 \leq i \leq n} p_i(X)^{r_i} \in k[X].$$

be the factorization of $\bar{P}(X)$ in $k[X]$. Then

1. *there are exactly n maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ in $\widetilde{\mathcal{O}}_K$, with $\mathfrak{m}_i = (\mathfrak{m}_K, P_i(\alpha))$ for any lifting $P_i(X) \in \mathcal{O}_K[X]$ of $p_i(X)$;*
2. *$\widetilde{\mathcal{O}}_K/\mathfrak{m}_i \simeq k[X]/(p_i(X))$, and $f_i := f_{(\widetilde{\mathcal{O}}_K)_{\mathfrak{m}_i}/\mathcal{O}_K} = \deg p_i(X)$.*
3. *$e_i := e_{(\widetilde{\mathcal{O}}_K)_{\mathfrak{m}_i}/\mathcal{O}_K} = r_i$.*

Proof. (1)-(2) We have an isomorphism $\mathcal{O}_K[X]/(P(X)) \to \widetilde{\mathcal{O}}_K$ taking the class of X to α. The maximal ideals of $\widetilde{\mathcal{O}}_K/(\mathfrak{m}_K) \simeq k[X]/(\bar{P}(X))$ are those generated by the class of the $p_i(X)$'s in $k[X]/(\bar{P}(X))$.

Let $\mathfrak{m}$ be a maximal ideal of $\widetilde{\mathcal{O}}_K$. Then its image modulo $\mathfrak{m}_K$ is equal to some of the above maximal ideals, therefore $\mathfrak{m}$ contains $(\mathfrak{m}_K, P_i(\alpha))$ for some $i \leq n$. As the latter is maximal, there is equality. Different i's give different maximal ideals in $\widetilde{\mathcal{O}}_K/(\mathfrak{m}_K)$, hence different maximal ideals in $\widetilde{\mathcal{O}}_K$.

(3) We have $P(X) = \prod_{1 \leq i \leq n} P_i(X)^{r_i} + \varepsilon(X)$ with $\varepsilon(X)$ having coefficients in $\mathfrak{m}_K$. So

$$\prod_{1 \leq i \leq n} \mathfrak{m}_i^{r_i} = \prod_{1 \leq i \leq n} (\mathfrak{m}_K, P_i(\alpha))^{r_i} \subseteq \mathfrak{m}_k \widetilde{\mathcal{O}}_K = \prod_{1 \leq i \leq n} \mathfrak{m}_i^{e_i}.$$

Therefore $r_i \geq e_i$ for all $i \leq n$. As

$$\sum_i r_i f_i = \deg \bar{P}(X) = \deg P(X) = [L : K] = \sum_i e_i f_i,$$

we get $r_i = e_i$ for all $i \leq n$. □

Definition 3.12 Let L be a finite extension of K. Let $\mathfrak{m}$ be a maximal ideal of $\widetilde{\mathcal{O}}_K$. We say that L/K is *unramified at* $\mathfrak{m}$ if $e_{(\widetilde{\mathcal{O}}_K)_{\mathfrak{m}}/\mathcal{O}_K} = 1$ and if $\widetilde{\mathcal{O}}_K/\mathfrak{m}$ of k is separable.

We say that L/K is *unramfied* if it unramified at all maximal ideals of $\widetilde{\mathcal{O}}_K$.

Example 3.13 Let $d \geq 2$, $K = \mathbb{C}(z)$, $L = K[t]$ with $t^d = z$. For any $c \in \mathbb{C}$, denote by $\mathfrak{m}_c = (z-c)\mathbb{C}[z]$, and endow K with the $\mathfrak{m}$-adic valuation. The valuation ring $\mathcal{O}_{K,c}$ is $\mathbb{C}[z]_{\mathfrak{m}_c}$. Its integral closure in L is $\mathcal{O}_{K,c}[t] \simeq \mathcal{O}_{K,c}[X]/(X^d - z)$.

The maximal ideals of $\mathcal{O}_{K,c}[t]$ are those generated by the $(t - \alpha_i)$'s where $\alpha_1, \ldots, \alpha_d \in \mathbb{C}$ are the d-th roots of c. If $c \neq 0$, then there are d distinct such maximal ideals. Theorem 3.9 implies that all ramification indexes are equal to 1 (the residue extensions are always trivial). In this case L is unramified over K (when the latter is endowed with the $\mathfrak{m}_c$-adic valuation).

If $c = 0$, as $t^d = z$, we have $e \geq d$, hence $e = d$.

Corollary 3.14. *Let $L = K[\alpha]$ and let $P(X) \in \mathcal{O}_K[X]$ be the minimal polynomial of α over K (so α is integral over $\mathcal{O}_K$). Suppose that $\bar{P}(X) \in k[X]$ is separable. Then L is unramfied over K, and the number of maximal ideals of $\widetilde{\mathcal{O}}_K$ is equal to the number of irreducible factors of $\bar{P}(X)$.*

Proof. The ring $\mathcal{O}_K[\alpha] \simeq \mathcal{O}_K[X]/(P(X))$ integrally closed (use Exercise 1 in TD4) and integral over $\mathcal{O}_K$, so it is equal to $\widetilde{\mathcal{O}}_K$. Then apply Proposition 3.11. □

Example 3.15 Let p be a prime number. For all $n \geq 1$, $\xi_n \in \mathbb{C}_p$ denotes a primitive p-root of unity.

1. Let $n \geq 1$ be prime to p, then $\mathbb{Q}_p \to L := \mathbb{Q}_p(\xi_n)$, is unramified. Indeed, let $F_n(X) \in \mathbb{Z}_p[X]$ be the minimal polynomial of ξ_n over $\mathbb{Q}_p$. It divides the cyclotomic polyomial $\Phi_n(X)$ which divides $X^n - 1$ in $\mathbb{Z}[X]$. So over $\mathbb{F}_p$, $\bar{F}_n(X)$ divides $X^n - 1$, hence is separable. Then apply Corollary 3.14.

2. Consider $L = \mathbb{Q}_p(\xi_p)$. Then $\xi_p \equiv 1 \mod \mathfrak{m}_L$ because $(\xi_p - 1)^p \equiv 0 \mod p$. Let $\lambda_p = \xi_p - 1$. Then the relation $(1 + \lambda_p)^p = 1$ gives

$$\lambda_p^{p-1} + p\lambda_p^{p-2} + ... + (p(p-1)/2)\lambda_p + p = 0$$

(all the intermediate coefficients are divisible by p). So

$$p(-1 + \lambda_p a) = \lambda_p^{p-1}$$

for some $a \in \mathcal{O}_L$. This implies that $e \geq p - 1$. As $p - 1 \geq [\mathbb{Q}_p(\xi_p) : \mathbb{Q}_p] = ef$, we get $[\mathbb{Q}_p(\xi_p) : \mathbb{Q}_p] = p - 1 = e$ and $f = 1$.

3.2 Monogeneity

Definition 3.16 A *monogeneous* algebra over a ring A is an A-algebra B of the form $A[b]$ for some $b \in B$. It is known that finite separable extensions of a field k are monogeneous (Primitive element theorem).

Exercise 3.17 Let $K = k[X]/(F(X))$ be a separable extension of k. Then for any $r \geq 1$, $k[X]/(F(X)^r)$ is isomorphic to $K[Y]/(Y^r)$.

Lemma 3.18. *Let k be a field.*

1. *Any finite product of finite monogeneous k-algebras is monogeneous if k is infinite.*
2. *If E is a finite product of finite monogeneous k-algebras, then E is monogeneous if and only if E_{red} is monogeneous.*
3. *Suppose k is finite. Let E be the product of $n \geq 2$ finite extensions of k, then E is monogeneous if* $\mathrm{Card}(k) \geq \max(n, 3)$.

Proof. (1) It is enough to prove that any finite product of finite local monogeneous k-algebras is monogeneous. Let $E = \prod_{1 \leq i \leq n} E_i$ with E_i local monogeneous k-algebras. So we have isomorphisms $k[X]/(f_i(X)^{r_i}) \simeq E_i$ for all $i \leq n$ with monic irreducible polynomials $f_i(X) \in k[X]$ and $r_i > 0$. As k is infinite, the set of monic irreducible polynomials $\{f_i(X + c) \mid c \in k\}$ is infinite. Therefore, replacing each $f_i(X)$ with a suitable $f_i(X + c_i)$ (and we still have $E_i \simeq k[X]/(f_i(X + c)^{r_i})$), we can suppose that the $f_i(X)$ are pairwise distinct, thus pairwise coprime. By the Chinese Remainder Theorem

$$\prod_i E_i \simeq k[X]/(\prod_i (f_i(X)^{r_i})$$

is monogeneous.

(2) Use Exercice 3.17.

(3) Write $E = \prod_{1 \leq i \leq n} k[X]/(f_i(X))$ with monic irreducible polynomials $f_i(X) \in k[X]$. If for each $d \geq 1$, the number of $f_i(X)$'s of degree d does not exceed the total number of monic irreducible polynomials of degree d over k, then we can replace them by pairwise distinct monic irreducible polynomials of degree d. Use again CRT as above to conclude. For the proof of the concrete lower bound, refer to Pascal's lecture. (To be completed here). □

Remark 3.19 Let $k = \mathbb{F}_q$. The product k^{q+1} is not monogeneous.

Definition 3.20 Let k be a field. A *finite separable k-algebra* is a finite product of finite separable extensions of k. (The true definition is a finite k-algebra B such that $B \otimes_k k'$ is reduced for any field extension k'/k).

Proposition 3.21 (Monogeneity)**.** *Let L/K be a finite extension such that $\widetilde{\mathcal{O}}_K$ is finite over $\mathcal{O}_K$. Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ be the maximal ideals of $\widetilde{\mathcal{O}}_K$. Suppose that $\kappa_i := \widetilde{\mathcal{O}}_K/\mathfrak{m}_i$ is separable over k for all i and that $\prod_{1 \leq i \leq n} \kappa_i$ is monogeneous over k. Then $\widetilde{\mathcal{O}}_K$ is monogeneous over $\mathcal{O}_K$.*

Proof. (1) Fix a maximal ideal $\mathfrak{m}$ of $\widetilde{\mathcal{O}}_K$ and let $\mathcal{O}_L = (\widetilde{\mathcal{O}}_K)_{\mathfrak{m}}$. We first show that the k-algebra $\mathcal{O}_L/\mathfrak{m}_K\mathcal{O}_L$ is monogeneous.

Denote by κ_L the residue field of $\mathcal{O}_L$. It is monogeneous over k. Lift a generator $\bar{\alpha}$ of κ_L/k to $\alpha \in \mathcal{O}_L$. Lift the minimal polynomial $\bar{P}(X)$ of $\bar{\alpha}$ over k to a monic $P(X) \in \mathcal{O}_K[X]$. Let us show that modifying α if necessary, $P(\alpha)$ is a uniformizing element of $\mathcal{O}_L$.

Chose an arbitrary uniformizing element $\pi_L \in \mathcal{O}_L$. We claim that $P(\alpha)$ or $P(\alpha + \pi_L)$ is a uniformizing element of $\mathcal{O}_L$. Indeed, using Taylor expansion of $P(X)$ at α (that is $P(X+\alpha) - P(\alpha) = (P'(\alpha) + XQ(X))X$ for some $Q(X) \in \mathcal{O}_L[X]$) we have

$$P(\alpha + \pi_L) - P(\alpha) = (P'(\alpha) + \pi_L\beta)\pi_L, \quad \beta \in \mathcal{O}_L.$$

As $\bar{P}(X)$ is separable, $\bar{P}'(\bar{\alpha}) \neq 0$, thus $P'(\alpha) \in \mathcal{O}_L^*$ and the rhs is a generator of $\pi_L\mathcal{O}_L$. As $P(\alpha+\pi_L), P(\alpha) \in \pi_L\mathcal{O}_L$, one of them generates $\pi_L\mathcal{O}_L$.

Now fix $\pi_L = P(\alpha)$ as a uniformizing element of $\mathcal{O}_L$. Let $e = e_{\mathcal{O}_L/\mathcal{O}_K}$. As in the proof of Lemma 3.5, we have

$$\mathcal{O}_L = \sum_{0 \leq i \leq e-1} \mathcal{O}_K[\alpha]\pi_L^i + \mathfrak{m}_K\mathcal{O}_L \subseteq \mathcal{O}_K[\alpha] + \mathfrak{m}_K\mathcal{O}_L.$$

Thus $\mathcal{O}_L/\mathfrak{m}_K\mathcal{O}_L$ is generated by the image of α.

(2) By the previous lemma, $\widetilde{\mathcal{O}}_K/\mathfrak{m}_K\widetilde{\mathcal{O}}_K$ is monogeneous over k. Let $\theta \in \widetilde{\mathcal{O}}_K$ be a lifting of a generator of $\widetilde{\mathcal{O}}_K/\mathfrak{m}_K\widetilde{\mathcal{O}}_K$ as k-algebra. Let $A = \mathcal{O}_K[\theta] \subseteq \widetilde{\mathcal{O}}_K$. As $\widetilde{\mathcal{O}}_K \subseteq A + \mathfrak{m}_K\widetilde{\mathcal{O}}_K$, we have $\widetilde{\mathcal{O}}_K = A$ by Nakayama's lemma (here we use the finite generation hypothesis on $\widetilde{\mathcal{O}}_K$). □

Definition 3.22 Let $\mathcal{O}_K \to \mathcal{O}_L$ be an extension of dvr's satisfying the condition of (7). We say that the extension is *tamely ramified* if the ramification index $e_{\mathcal{O}_L/\mathcal{O}_K}$ is prime to $\mathrm{char}(k)$ (no condition if the latter is zero) and if the residue extension κ_L/k is separable. Otherwise the ramification is said to be *wild*.

We say that L/K is *tamely ramified* if for all maximal ideals $\mathfrak{m}$ of $\widetilde{\mathcal{O}}_K$, the extension $\mathcal{O}_K \to (\widetilde{\mathcal{O}}_K)_{\mathfrak{m}}$ is tamely ramified.

Corollary 3.23. *If L/K is tamely ramified and if $\widetilde{\mathcal{O}}_K$ is local (e.g. if K is complete) or if k is infinite, then $\widetilde{\mathcal{O}}_K$ is monogeneous over $\mathcal{O}_K$.*

Definition 3.24 Let L be a finite extension of K. We say that L/K is *totally ramified* if $\widetilde{\mathcal{O}}_K = \mathcal{O}_L$ is a discrete valuation ring and if $e_{\mathcal{O}_L/\mathcal{O}_K} = [L:K]$ (thus the residue extension is trivial).

By the above proposition, totally ramified extensions are monogeneous. We can be more precise about its structure.

Proposition 3.25. *Let $\mathcal{O}_K$ be a discrete valuation ring. Let $d \geq 1$.*

1. *Let*
$$P(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_1X + a_0 \in \mathcal{O}_K[X]$$
be an Eisenstein polynomial (i.e., $a_i \in \mathfrak{m}_K$ for all $0 \leq i \leq d-1$ and $a_0 \notin \mathfrak{m}_K^2$). Let $L = K[X]/(P(X))$. Then L/K is totally ramified, and the class α of X in L is a uniformizing element of $\mathcal{O}_L$.

2. *Let L/K be a totally ramified extension of degree d. Let π_L be a uniformizing element of $\mathcal{O}_L$. Then π_L is the zero of an Eisenstein polynomial $\in \mathcal{O}_K[X]$ of degree d, and $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$.*

Proof. (1) As $a_0 \in \mathfrak{m}_K \smallsetminus \mathfrak{m}_K^2$, it is a uniformizing element of $\mathcal{O}_K$. Let $B = \mathcal{O}_K[X]/(P(X))$. As B is finite over $\mathcal{O}_K$, any maximal ideal $\mathfrak{m}$ of B contains the maximal ideal of $\mathcal{O}_K$, hence a_0. As

$$a_0(1 + \sum_{1 \leq i \leq d-1} (a_i a_0^{-1})\alpha^i) = -\alpha^d,$$

we have $\alpha \in \mathfrak{m}$ and $a_0 \in \alpha B$. Now $B/(a_0, \alpha) \simeq k[X]/(X) = k$, so $\mathfrak{m}_B := (a_0, \alpha) = \alpha B$ is maximal and contained in $\mathfrak{m}$. Therefore $\mathfrak{m} = \mathfrak{m}_B$ and B is local and principal. As it is finite over $\mathcal{O}_K$, it is equal to the integral closure $\widetilde{\mathcal{O}}_K$ of $\mathcal{O}_K$ in L, and $\widetilde{\mathcal{O}}_K = \mathcal{O}_L$ is a discrete valuation ring. The above relation shows that $\mathfrak{m}_K B \subseteq \mathfrak{m}_B^d$. Therefore the ramification index $e \geq d$. Theorem 3.9 implies that $e = d$ and α is a uniformizing element. Thus the extension is totally ramified.

(2) By definition $\widetilde{\mathcal{O}}_K = \mathcal{O}_L$ is a dvr. Let π_L be a uniformizing element of $\mathcal{O}_L$. Let $P(X) = X^n + \sum_{0 \leq i \leq n-1} a_i X^i$ be the minimal polynomial of π_L over K, with $n \leq d$. Then $P(X) \in \widetilde{\mathcal{O}}_K[X]$ (Proposition 2.7). We have $a_0 \in \pi_L \mathcal{O}_L \cap \mathcal{O}_K = \mathfrak{m}_K$. Let us show that $a_i \in \mathfrak{m}_K$ for all $i \leq n-1$. If not, let i_0 be the smallest index such that $a_{i_0} \in \mathcal{O}_K^*$. Then, as $P(\pi_L) = 0$,

$$(\pi_L^{n-i_0} + a_{n-1}\pi_L^{n-1-i_0} + \cdots + a_{i_0})\pi_L^{i_0} \in \mathfrak{m}_K \mathcal{O}_L = \pi_L^d \mathcal{O}_L,$$

and $i_0 \leq n-1 < d$, absurd! So $a_i \in \mathfrak{m}_K$ for all $i \leq n-1$. Therefore

$$a_0 \in -\pi_L^n + \mathfrak{m}_K \pi_L \mathcal{O}_L \subset \pi_L^n(-1 + \pi_L \mathcal{O}_L).$$

This implies that $n \geq d = e_{L/K}$, hence $n = d$, $a_0 \notin \mathfrak{m}_K^2$ and $L = K[\pi_L]$. By (1), π_L being the root of an Eisenstein polynomial of degree d, generates $\mathcal{O}_L$ over $\mathcal{O}_K$. □

3.3 Decomposition of extensions of complete dvr's

In this subsection we assume K is *complete* (Henselian is enough). See also § 3.4

Lemma 3.26. *Let $\mathcal{O}_K$ be a complete dvr. Let L/K be a tamely totally ramified extension of degree e. Then there exists a uniformizing element π_L of $\mathcal{O}_L$ such that $\pi_L^e \in \mathcal{O}_K$ (hence π_L^e is a uniformizing element of $\mathcal{O}_K$). Thus $\mathcal{O}_L \simeq \mathcal{O}_K[X]/(X^e - \pi_K)$ for some uniformizing element π_K of $\mathcal{O}_K$.*

Proof. Let π_K and π_L be respectively uniformizing elements of $\mathcal{O}_K$ and $\mathcal{O}_L$. Then $\pi_K = \pi_L^e u$ for some unit $u \in \mathcal{O}_L$. As the residue extension of L/K is trivial, $u = v(1+\epsilon)$ for some $v \in \mathcal{O}_K^*$ and $\epsilon \in \mathfrak{m}_L$. The polynomial $X^e - (1+\epsilon) \in \mathcal{O}_L[X]$ has a simple root 1 in $k[X]$. As L is complete, this polynomial has a root $w \in 1 + \mathfrak{m}_L \subset \mathcal{O}_L^*$. Replacing π_L with $w\pi_L$ and π_K with π_K/v, we get $\pi_L^e = \pi_K$. □

Lemma 3.27. *Let $\mathcal{O}_K$ be a complete dvr of residue characteristic (the characteristic of the residue field) $p > 0$. Let L/K be a finite extension such that the residue extension κ_L/k is purely inseparable. Let e' be a prime to p divisor of $e_{L/K}$. Then there exists a unique totally ramified subextension of L/K of ramification index e'.*

Proof. (1) *Existence.* Let π_K, π_L be respective uniformizing elements of $\mathcal{O}_K, \mathcal{O}_L$. There exists $u \in \mathcal{O}_L^*$ such that $\pi_K = u\pi_L^e$. Let $r \geq 0$ be such that $\bar{u}^{p^r} = \bar{\lambda} \in \kappa_L$ with $\lambda \in \mathcal{O}_K^*$. Let $a, b \in \mathbb{Z}$ be such that $ap^r + be' = 1$. Then $\bar{\lambda}^a \bar{u}^{be'} = \bar{u}$ and we have

$$u = (\lambda^a)(u^b)^{e'}(1+\epsilon), \quad \epsilon \in \mathfrak{m}_L.$$

Let $1 + \epsilon = (1+\delta)^{e'}$ for some $\delta \in \mathfrak{m}_L$. Then

$$(u^b(1+\delta)\pi_L^{e/e'})^{e'} = \lambda^{-a}\pi_K$$

and the subextension of L generated by $u^b(1+\delta)\pi_L^{e/e'}$ is totally and tamely ramified of degree e' over K.

(2) *Uniqueness.* Let L_1, L_2 be two subextensions of L with the required properties. By Lemma 3.26 they are generated respectively by uniformizing elements π_{L_1}, π_{L_2} such that $\pi_{L_i}^{e'} = \pi_{K,i}$ is a uniformizing element of $\mathcal{O}_K$. This implies that $\lambda := \pi_{K,1}\pi_{K,2}^{-1} \in \mathcal{O}_K^*$ satisfies $\bar{\lambda} = \bar{u}^{e'}$ where $u = \pi_{L_1}\pi_{L_2}^{-1} \in \mathcal{O}_L^*$. As κ_L is purely inseparable over k, this implies that $\bar{u} \in k$ and $\lambda = \lambda_1^{e'}$ with $\lambda_1 \in \mathcal{O}_K^*$ (because elements of $1 + \mathfrak{m}_K$ are e'-powers). Therefore $\pi_{L_1} = \lambda_1\pi_{L_2} \in L_2$ (uniqueness of e'-th root in L) and $L_1 = L_2$. $\square$

Theorem 3.28. *Let $\mathcal{O}_K$ be a complete dvr. Let L/K be a finite extension.*

1. *For any separable sub-extension $\kappa \subseteq \kappa_L$, there exists a unique unramified subextension $F \subseteq L$ with residue field equal to κ.*
2. *There exists a biggest unramified subextension K^{ur} of L.*
3. *There exists a biggest tamely ramified subextension K^{tam} of L.*

Proof. (1) Let $\kappa = k[\theta]$ for some $\theta \in \kappa$. Let $P(X) \in \mathcal{O}_K[X]$ be a monic lifting of the minimal polynomial of θ over k. We know that $P(X)$ is irreducible in $K[X]$ (TD 6). By Hensel's lemma, θ lifts to a zero $\alpha \in L$ of $P(X)$. Let $F = K[\alpha] \subseteq L$. By Corollary 3.14, F is unramified over K. In the proof of the same corollary it is shown that $\mathcal{O}_F = \mathcal{O}_K[\alpha]$. By Proposition 3.11, the residue field of F is κ.

Let F' be another unramified subextension of L with residue field equal to κ. Then $[F' : K] = [\kappa : k]$. By Hensel's lemma, θ lifts to a zero $\alpha' \in F'$ of $P(X)$. By the uniqueness in L we have $\alpha = \alpha' \in F'$, hence $F \subseteq F'$. But they have the same degree over K, so they are equal.

(2) Let k^s be the separable closure of k in κ_L, let K^{ur} be the unramified subextension of L with residue field k^s. If F is any unramified subextension of L, its residue field κ_F is contained in k^s. Applying (1) to the extension K^{ur}/K, there exists an unramified subextension $F' \subseteq K^{ur}$ with residue field equal to κ_F. Applying again (1) to L we get $F = F' \subseteq K^{ur}$.

(3) If $\mathrm{char}(k) = 0$, L/K is tamely ramified. Suppose $\mathrm{char}(k) = p > 0$. Let e' be the biggest prime to p divisor of $e_{L/K}$. By Lemma 3.27, there exists a totally ramified subextension K^{tam}/K^{ur} of L/K^{ur} of degree e'. Then K^{tam} is tamely ramified over K. It remains to show that it is the biggest one.

Let F be a tamely ramified subextension of L/K. Define F^{ur} as the biggest unramified subextension of L/F. It is enough to show that $F^{ur} \subseteq K^{tam}$. By construction its residue field is the separable closure of κ_F in κ_L. As κ_F is separable over k, this separable closure is k^s. Replacing F with F^{ur} we can suppose that the residue field of F is k^s. The biggest unramified subextension of F/K is an unramfieid subextension of L/K with residue field k^s. So it is equal to K^{ur} by (1). Thus $K^{ur} \subseteq F$. The ramification index $e_{F/K^{ur}}$ is a prime to p divisor of $e_{L/K^{ur}}$. By Lemma 3.27, $F \subseteq K^{tam}$. □

Corollary 3.29. *Let K be complete and let L/K be a finite extension. Then we have a unique decomposition*

$$K \xrightarrow{\text{unramified}} K^{ur} \xrightarrow{\text{tamely totally ramified}} K^{tam} \xrightarrow{\text{wildely ramified}} L$$

such that the extension L/K^{tam} has purely inseparable residue extension and the ramification index is a power of $p = \mathrm{char}(k)$ (equal to 1 if $\mathrm{char}(k) = 0$).

Remark 3.30 The ramification theory for L/K^{tam} is much more complicated.

Example 3.31 Let $K = \mathbb{Q}_p$ and $L = \mathbb{Q}_p(\zeta_{p^r})$ with $r \geq 1$. Then $K^{ur} = K$, $K^{tam} = \mathbb{Q}_p(\zeta_p)$ and L/K^{tam} is totally ramified with ramification index p^{r-1}. The proof is similar to Exercise 3 of the midterm exam).

Exercise 3.32 Suppose that K is complete with algebraically closed residue field k. If $\mathrm{char}(k) = 0$, show that any finite extension of K is cyclic. If $\mathrm{char}(k) = p > 0$, show the same result for extensions of degree prime to p.

Below is a "non-embedded" version of Theorem 3.28(1). It was not presented during the lecture.

Proposition 3.33. *Suppose K is complete.*

1. *Let κ be a finite separable extension of k. There there exists a finite unramfied extension L/K with residue field κ. Moreover L is unique up to (non-unique) isomorphism of K-extension.*

2. *Let k^s be a separable closure of k. Then there exists an algebraic extension K^{ur}/K with residue field k^s and such that $\mathcal{O}_K \to \mathcal{O}_{K^{ur}}$ has ramification index 1. Moreover K^{ur} is unique up to (non-unique) isomorphism of K-extensions.*

Proof. (1) Let $\kappa = k[\theta]$ for some $\theta \in \kappa$. Let $P(X) \in \mathcal{O}_K[X]$ be a monic lifting of the minimal polynomial of θ over k and let $L = K[X]/(P(X))$. The rest of the proof is exactly the same as for Theorem 3.28(1).

(2) Fix an algebraic closure K^c of K. Consider the set of (possibly infinite) subextensions L/K such that $\mathcal{O}_L/\mathcal{O}_K$ has ramification index 1 and separable residue extension. Then apply Zorn's lemma and (1). □

Exercise 3.34 Let K be complete. Let κ/k be a Galois extension. Then there exists an unramified Galois extension L/K with residue field κ and such that $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(\kappa/k)$.

3.4 Galois theory

Recall that a finite extension L/K is a *Galois extension* if it is separable and if for all $\alpha \in L$, all conjuguates of α belong to L. This is equivalent to $|\mathrm{Aut}_K(L)| = [L : K]$. Denote $\mathrm{Aut}_K(L) = \mathrm{Gal}(L/K)$. It is called the Galois group of L/K.

For any subgroup H of G, denote by $L^H := \{\alpha \in L \mid \sigma(x) = x,\ \forall \sigma \in H\}$. The fundamental theorem of Galois theory (Galois correspondance) says that $H \mapsto L^H$ is a decreasing one-to-one map. The inverse map is given by $F \mapsto \{\sigma \in G \mid \sigma|_F = \mathrm{Id}_F\}$. The extension L/L^H is Galois with Galois group H. The extension L^H/K is Galois if and only H is a normal subgroup of G. Then its Galois group is G/H. Let F be a subextension of L/K. Then F/K is Galois if and only if F is stable by the action of $\mathrm{Gal}(L/K)$, we then have a canonical exact sequence

$$1 \to \mathrm{Gal}(L/F) \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K) \to 1. \tag{8}$$

Note that a Galois extension of a Galois extension is not Galois in general.

If we drop the separability condition in the definition of Galois extensions, we get the *normal extensions*. Any purely inseparable is normal. It is easy to show that a finite extension L/K is normal if and only if the separable closure K^s of K in L is Galois. Then $\mathrm{Aut}_K(L) = \mathrm{Gal}(K^s/K)$.

Any finite extension L/K is contained in a smallest normal extension $\widetilde{L}/K$ (Galois if L/K is separable). This allows sometime to reduce a problem on finite extensions to normal (resp. Galois) extensions.

A fundamental problem is number theory is to understand the Galois groups of Galois extensions of $\mathbb{Q}$. The ramification theory provides some insights on these groups.

Recall the following useful result in commutative algebra.

Lemma 3.35 (Avoidance lemma)**.** *Let A be a commutative ring, let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be prime ideals of A such that $\mathfrak{p}_1 \not\subset \mathfrak{p}_i$ for all $i \geq 2$. Then*

$$\mathfrak{p}_1 \not\subset \cup_{2 \leq i \leq n} \mathfrak{p}_i.$$

Proof. By induction on n. In the case where all the prime ideals are maximal (as in the next proposition), one can also use the Chinese Remainder Theorem. □

Let K be a discrete valuation field and let L/K be a finite Galois extension. As L/K is seprable, the integral closure $\widetilde{\mathcal{O}}_K$ of $\mathcal{O}_K$ is L is finite over $\mathcal{O}_K$ (Theorem 2.8). The Galois group $G = \mathrm{Gal}(L/K)$ acts naturally on the set of maximal ideals of $\widetilde{\mathcal{O}}_K$.

Proposition 3.36. *The Galois group G acts transitively on the maximal ideals of $\widetilde{\mathcal{O}}_K$.*

Proof. Let $\mathfrak{m}, \mathfrak{m}'$ be a two maximal ideals of $\widetilde{\mathcal{O}}_K$. Suppose that $\mathfrak{m} \neq \sigma(\mathfrak{m}')$ for all $\sigma \in G$. So $\mathfrak{m} \not\subset \sigma(\mathfrak{m}')$ for all $\sigma \in G$. Pick $x \in \mathfrak{m} \setminus \cup_{\sigma \in G} \sigma(\mathfrak{m}')$. Then $\prod_{\sigma \in G} \sigma(x) = N_{L/K}(x) \in \mathcal{O}_K \cap \mathfrak{m} = \mathfrak{m}_K \subseteq \mathfrak{m}'$. So $\sigma(x) \in \mathfrak{m}'$ for some $\sigma \in G$, thus $x \in \sigma^{-1}(\mathfrak{m}')$. Contradiction. □

Corollary 3.37. *The ramification index (respectively the residue degree) is the same for all maximal ideals of $\widetilde{\mathcal{O}}_K$.*

Definition 3.38 Let $\mathfrak{m}$ be a maximal ideal of $\widetilde{\mathcal{O}}_K$. Then the stabilizer

$$D_{\mathfrak{m}} := \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathfrak{m}) = \mathfrak{m}\}$$

is called the *decomposition group at* $\mathfrak{m}$. Any $\sigma \in D_{\mathfrak{m}}$ acts naturally on $\kappa_{\mathfrak{m}} = \widetilde{\mathcal{O}}_K/\mathfrak{m}$. The subgroup

$$I_{\mathfrak{m}} := \{\sigma \in D_{\mathfrak{m}} \mid \sigma|_{\kappa_m} = 1\}$$

is called the *inertia group at* $\mathfrak{m}$. By construction this is a normal subgroup of $D_{\mathfrak{m}}$. If $\mathfrak{m}'$ is another maximal ideal of $\widetilde{\mathcal{O}}_K$, then $\mathfrak{m}' = \sigma(\mathfrak{m})$ for some $\sigma \in G$. We have $D_{\mathfrak{m}'} = \sigma^{-1} D_{\mathfrak{m}} \sigma$ and $I_{\mathfrak{m}'} = \sigma^{-1} I_{\mathfrak{m}} \sigma$.

Corollary 3.39. *There is a (non canonical) bijection between the set of maximal ideals of $\widetilde{\mathcal{O}}_K$ and the quotient $G/D_{\mathfrak{m}}$. In particular $G = D_{\mathfrak{m}}$ if and only if $\widetilde{\mathcal{O}}_K$ is local, if and only if $|\ |_K$ has a unique extension to L.*

Proof. The first part is an immediate consequence of Proposition 3.36. The second equivalence is Proposition 2.28. □

Proposition 3.40. *The extension $\kappa_{\mathfrak{m}}/k$ is normal and the canonical sequence of groups*

$$1 \to I_{\mathfrak{m}} \to D_{\mathfrak{m}} \to \mathrm{Aut}_k(\kappa_{\mathfrak{m}}) \to 1$$

is exact.

Proof. Let $\theta \in \kappa_{\mathfrak{m}}$, let $p(X)$ be its minimal polynomial over k. We first show that $p(X)$ is split in $\kappa_{\mathfrak{m}}$. This means that all conjugates of θ belong to $\kappa_{\mathfrak{m}}$ and thus $\kappa_{\mathfrak{m}}/k$ is a normal extension.

Let $\alpha \in \widetilde{\mathcal{O}}_K$ be a lifting of θ. Consider $P(X) := \prod_{\sigma \in G}(X - \sigma(\alpha))$. Then $P(X) \in \mathcal{O}_K[X]$ and $\bar{P}(X) \in k[X]$ vanishes at θ. Therefore $p(X) \mid \bar{P}(X)$. As $\bar{P}(X) = \prod_{\sigma}(X - \overline{\sigma(\alpha)})$ is split in $\kappa_{\mathfrak{m}}$, the same holds for $p(X)$ and we are done with the first part.

For the exactness of the sequence we only have to prove that the natural morphism

$$r : D_{\mathfrak{m}} \to \mathrm{Aut}_k(\kappa_{\mathfrak{m}}) = \mathrm{Gal}(\kappa_{\mathfrak{m}}^s/k)$$

is surjective. We can suppose that $\kappa_{\mathfrak{m}}^s \neq k$ (otherwise $\mathrm{Aut}_k(\kappa_{\mathfrak{m}}) = \{1\}$). Fix a generator θ of the extension $\kappa_{\mathfrak{m}}^s/k$. Let $\tau \in \mathrm{Gal}(\kappa_{\mathfrak{m}}^s/k)$. It is enough to show that there exists $\sigma \in D_{\mathfrak{m}}$ such that $r(\sigma)(\theta) = \tau(\theta)$ (this implies that $\tau = r(\sigma)$ as θ generates $\kappa_{\mathfrak{m}}^s$). This equality means that $\tau(\theta) = \overline{\sigma(\alpha)}$ for an arbitrary lifting $\alpha \in \widetilde{\mathcal{O}}_K$ of θ.

With the above notation we have $p(X) \mid \bar{P}(X)$, hence $\tau(\theta)$ is equal to $\overline{\sigma(\alpha)}$ for some $\sigma \in G$. We are not yet done, because we don't know whether $\sigma \in D_{\mathfrak{m}}$. By the Chinese Remainder Theorem, there exists a lifting $\alpha \in \widetilde{\mathcal{O}}_K$ of θ such that $\alpha \in \mathfrak{m}'$ for all $\mathfrak{m}' \neq \mathfrak{m}$. Let us then prove that $\sigma \in D_{\mathfrak{m}}$. If not, then $\sigma^{-1} \notin D_{\mathfrak{m}}$, hence $\mathfrak{m}' := \sigma^{-1}(\mathfrak{m}) \neq \mathfrak{m}$. By construction, $\alpha \in \mathfrak{m}'$, thus $\sigma(\alpha) \in \mathfrak{m}$. Hence $\tau(\theta) = 0$ and $\kappa_{\mathfrak{m}}^s = k$, contradiction. □

Exercise 3.41 Let L/K be a Galois extension (without absolute values). Let Ω/K be an extension such that $L \otimes_K \Omega$ is a field.

1. The extension $\Omega \to L_\Omega := L \otimes_K \Omega$ is Galois, and the canonical group homomorphism $\mathrm{Gal}(L/K) \to \mathrm{Gal}(L_\Omega/\Omega)$ is an isomorphism.

2. The association $F \rightsquigarrow F_\Omega := F \otimes_K \Omega$ is an one-to-one correspondence between the subextentions of L/K and that of L_Ω/Ω. The canonical map $\mathrm{Gal}(L/F) \to \mathrm{Gal}(L_\Omega/F_\Omega)$ is an isomorphism.

Exercise 3.42 Let L/K be a finite extension of discrete valued fields. Show that $\widehat{K} \to \widehat{L}$ is an isomorphism if and only if $e_{L/K} = f_{L/K} = 1$. Such an extension is called an *immediate extension*.

Recall our settings: $(K, |\ |_K)$ is a discrete valued field, L/K is a finite Galois extension. Fix an extension of $|\ |_K$ to L and denote by $\mathfrak{m}$ the corresponding maximal ideal of $\widetilde{\mathcal{O}}_K$ and $|\ |_{\mathfrak{m}}$ the absolute value. Denote for simplicity $D = D_{\mathfrak{m}}$ and $I = I_{\mathfrak{m}}$ the decomposition and inertia groups at $\mathfrak{m}$.

Theorem 3.43. *Denote by $|\ |_D$ and $|\ |_I$ the restrictions of $|\ |_{\mathfrak{m}}$ to L^D and L^I respectively, and by k_D and k_I the corresponding residue fields.*

$$(K, |\ |_K) \longrightarrow (L^D, |\ |_D) \longrightarrow (L^I, |\ |_I) \longrightarrow (L, |\ |_{\mathfrak{m}})$$

$$k \longrightarrow k_D \longrightarrow k_I \longrightarrow \kappa_{\mathfrak{m}}.$$

Let κ_m^s be the separable closure of k in κ_m.

1. *The absolute value $|\ |_{\mathfrak{m}}$ is the unique one extending $|\ |_D$ to L. In particular the completion of L with respect to $|\ |_{\mathfrak{m}}$ satisfies*

$$\widehat{L} \simeq L \otimes_{L^D} \widehat{L^D}.$$

   The extension $\widehat{L}/\widehat{L^D}$ is Galois with Galois group isomorphic to D.

2. *The extension $(K, |\ |_K) \to (L^D, |\ |_D)$ is unramified with trivial residue extension (hence $\widehat{K} = \widehat{L^D}$, see Exercise 3.42).*

3. *The Galois extension $L^D \to L^I$ is unramified with Galois residue extension $k \to \kappa_{\mathfrak{m}}^s$.*

4. *The Galois extension $L^I \to L$ has ramification index $e = e_{L/K}$ and residue extension $\kappa_{\mathfrak{m}}^s \to \kappa_{\mathfrak{m}}$ which is purely inseparable.*

Proof. (1) The Galois group of the Galois extension L/L^D is D and by definition it fixes $\mathfrak{m}$. The first sentence of (1) follows from Corollary 3.39. As L is separable over L^D, $L \otimes_{L^D} \widehat{L^D}$ is reduced and finite over the field $\widehat{L^D}$, it has only one maximal ideal by Proposition 1.65. So $L \otimes_{L^D} \widehat{L^D}$ is a field. The canonical homomorphism (of K-algebras) $L \otimes_{L^D} \widehat{L^D} \to \widehat{(L, |\ |_{\mathfrak{m}})}$ is then an isomorphism (see Step 2 of the proof of Proposition 1.65). Apply Exercise 3.41 to conclude.

(2) We have $|G| = [L : K] = (|G|/|D|)e_{L/K}f_{L/K}$ by Theorem 3.9. So $|D| = e_{L/K}f_{L/K}$. Applying the same theorem to the Galois extension L/L^D and by (1) we get $|D| = e_{L/L^D}f_{L/L^D}$. But e_{L/L^D} and f_{L/L^D} divide respectively $e_{L/K}$ and $f_{L/K}$, so $e_{L/L^D} = e_{L/K}$ and $f_{L/L^D} = f_{L/K}$. Therefore $e_{L^D/K} = f_{L^D/K} = 1$.

(3)-(4) The Galois extension L/L^I has decomposition and inertia at $\mathfrak{m}$ both equal to I. By Proposition 3.40, the residue extension of L/L^I is purely inseparable.

By Proposition 3.40, $|D/I| = [\kappa_{\mathfrak{m}}^s : k]$. As $\kappa_{\mathfrak{m}}^s \subseteq \kappa_I$ by the above assertion, and because $k_D = k$, we have

$$[\kappa_{\mathfrak{m}}^s : k] \leq [k_I : k] = [k_I : k_D] \leq |D/I|.$$

Therefore $\kappa_I = \kappa_{\mathfrak{m}}^s$ and $e_{L^I/L^D} = [L^I : L^D]/[k_I : k_D] = 1$. This proves (3). Finally $e_{L/L^I} = e_{L/K}/(e_{L^I/L^D}e_{L^D/K}) = e_{L/K}$. □

Remark 3.44 The extension $(L^D, |\ |_D) \to L^I$ is *inert*, that is, unramified and $|\ |_D$ has unique extension to L^I. So the extension $K \to L^I$ is very nice, all bad things are concentrated in L/L^I.

Remark 3.45 The ramification of L/K at $\mathfrak{m}$ is the same as that of L/L^D at $\mathfrak{m}$, which is the same as that of $\widehat{L}/\widehat{K}$. By Exercise 3.41 for the study of ramification we can restrict ourselves to Galois extensions of complete discrete valuation fields.

Remark 3.46 If D is a normal subgroup of G, then all maximal ideals have the same decomposition group. The extension $K \to L^D$ is then totally split and L^I is the biggest unramified subextension of L.

It remains to study the extension $(L^I, |\ |_I) \to (L, |\ |_{\mathfrak{m}})$.

Corollary 3.47. *Suppose* $\mathrm{char}(k) = p > 0$. *The extension L/K is tamely ramified at $\mathfrak{m}$ (therefore at all maximal ideals) if and only if I has order prime to p. In this case the extension $(L^I, |\ |_I \to (L, |\ |_{\mathfrak{m}})$ is totally ramified.*

Proof. By Theorem 3.43, $e_{L/K} = e_{L/L^I}$ and the residue extension of L/L^I is purely inseparable. □

Theorem 3.48. *Keep the general Galois settings. Let $I \subseteq G$ be the inertia subgroup at some $\mathfrak{m}$.*

1. *If* $\mathrm{char}(k) = 0$, *then I is cyclic.*
2. *Suppose* $\mathrm{char}(k) = p > 0$. *Then we have an exact sequence*

$$1 \to P \to I \to T \to 1$$

where T is a cyclic group, of order prime to p, and P is a p-group. In particular P is the unique p-Sylow subgroup of G.

Proof. Endow L^I with the restriction of $|\ |_{\mathfrak{m}}$ as before. As I is the Galois group of L/L^I and is also the inertia subgroup at $\mathfrak{m}$. So we can replace K with L^I and suppose that $G = I$. By Remark 3.45 we can suppose K is complete.

First suppose L/K is tamely ramified. Then it is totally ramified by the previous corollary. By Lemma 3.26, $L = K[\pi_L]$ with $\pi_L^e = \pi_K$, where $e = e_{L/K} = [L : K]$. For any $\sigma \in \mathrm{Gal}(L/K)$, $\zeta := \sigma(\pi_L)/\pi_L$ is an e-th root of unity. Its image in $k_{\mathfrak{m}} = k$ is root of $X^e - 1 \in k[X]$. By Hensel's lemma, $\zeta \in K$. So we have a map $\mathrm{Gal}(L/K) \to \mu_e(K)$ (the group of ζ's in K^* such that $\zeta^e = 1$), defined by $\sigma \mapsto \sigma(\pi_L)/\pi_L$. It is immediate to check that this is an injective group homomorphism. It is an isomorphism by comparing the cardinalities of both groups. Hence $\mathrm{Gal}(L/K)$ is cyclic in this case. This implies (1).

Suppose now $\mathrm{char}(k) = p > 0$. Consider the biggest tamely ramified subextension K^{tam} of L/K (Theorem 3.28). By the uniqueness of this subextion, it is fixed by G. Hence it is Galois over K. By what precedes, $T := \mathrm{Gal}(K^{tam}/K)$ is cyclic of order e' prime to p. By the same theorem, the extension L/K^{tam} has ramification index a power of p and the residue extension is purely inseparable, so $P := \mathrm{Gal}(L/K^{tam})$ has order a power of p. The exact sequence (8) in our case is the desired exact sequence.

Finally, the p-Sylow subgroups of G are subgroups which are p-groups and maximal for the inclusion. They are all conjugate to each other. As $|G/P|$ has order prime to p, P is maximal. It is a normal subgroup, hence equal to all its conjugates. □

Example 3.49 The Galois group of any tamely ramified Galois extension of $\mathbb{Q}_p$ is extension of a cyclic group by a cyclic group.

Remark 3.50 Keep the hypothesis and notation of Theorem 3.43. We then have a decomposition

$$K \to L^D \to L^I \to L^P \to L$$

The extension $K \to L^I$ is unramified, $L^I \to L^P$ is totally and tamely ramified, and $L^P \to L$ has ramification index (at $\mathfrak{m}$) a power of p, and purely inseparable residue extension. This is the analogue of Corollary 3.29. It can be shown that $(L^I, |\,|_L)$ is the biggest unramified subextension of $(L, |\,|_\mathfrak{m})$ and $(L^P, |\,|_P)$, where $|\,|_P$ is the restriction of $|\,|_\mathfrak{m}$ to L^P, is the biggest tamely ramified subextension.

The extension $(K, |\,|_K) \to (L^D, |\,|_D)$ is an immediate extension, but $|\,|_K$ can be extended to absolute values on L^D, different from $|\,|_D$, for we which we do not have information on the ramification.

Exercise 3.51 Keep the hypothesis of Theorem 3.48.

1. Show that there exists an element of order $|T|$ in G.
2. Show that there exists a subextension F of L/K such that L is tamely ramified over F and $[F : K]$ is a power of p.

Exercise 3.52 (Functoriality) Let L/K be a Galois extension. Let F be a subextension of L/K. Fix a maximal ideal $\mathfrak{m}$ the integral closure of $\mathcal{O}_K$ in L and let $\mathfrak{n}$ be the intersection of $\mathfrak{m}$ with the integral closure of $\mathcal{O}_K$ in F. Endow F with the absolute value corresponding to $\mathfrak{n}$. Show that

1. Show that $D_\mathfrak{m}(L/F) := D_\mathfrak{m} \cap \mathrm{Gal}(L/F)$ is the decomposition of $F \to L$ at $\mathfrak{m}$. Same for the inertia group $I_\mathfrak{m}(L/F)$.
2. Suppose moreover that F/K is Galois. Show that we have the exact sequences
$$1 \to I_\mathfrak{m}(L/F) \to I_\mathfrak{m} \to I_\mathfrak{n}(F/K) \to 1$$
$$1 \to D_\mathfrak{m}(L/F) \to D_\mathfrak{m} \to D_\mathfrak{n}(F/K) \to 1$$

We pursue the study of the inertia group by introducing a filtration on it. Let K be a discrete valuation field. Let L/K be a Galois extension. Let I, D be respectively the inertia and decomposition group at some $\mathfrak{m}_L$. Denote the corresponding normalized valuation on L by v_L, and the valuation ring by $\mathcal{O}_L$. To study I we can replace K with L^D, endowed with the restriction of $v_\mathfrak{m}$, and suppose $G = D$. So we are in the situation where the integral closure $\widetilde{\mathcal{O}}_K$ of $\mathcal{O}_K$ in L is local (equivalently, there is only one absolute value on L extending that of K).

Furthermore we suppose from now on that the *residue field k of K is perfect*. The definition of the ramification groups is slightly different otherwise. Then by Proposition 3.21,

$$\mathcal{O}_L = \mathcal{O}_K[\alpha]$$

for some $\alpha \in \mathcal{O}_L$.

We introduce a *filtration* (*i.e.* a decreasing sequence of subgroups) on G. We put $G_{-1} = G$. For all $i \geq 0$, G acts naturally on $\mathcal{O}_L/\mathfrak{m}_L^{i+1}$. Put

$$G_i := \ker(G \to \mathrm{Aut}(\mathcal{O}_L/\mathfrak{m}_L^{i+1})).$$

So G_0 is just the inertia group I. Clearly the G_i's form a decreasing sequence of normal subgroups of G. The G_i's are called the *lower ramification subgroups*. There is a filtration by upper ramification subgroups, but we will not talk about it.

Lemma 3.53. *Let $i \geq 0$. Let $\sigma \in G$. Then $\sigma \in G_i$ if and only if any of the following conditions is satisfied:*

(i) $v_L(\sigma(x) - x) \geq i + 1$ *for all* $x \in \mathcal{O}_L$*;*

(ii) $v_L(\sigma(\alpha) - \alpha) \geq i + 1$.

Proof. If $\sigma \in G_i$, then (i), hence (ii), are satisfied by definition. Suppose (ii) holds. Let $x \in \mathcal{O}_L$. Write $x = \sum_{j \geq 0} a_j \alpha^j$ with $a_j \in \mathcal{O}_K$. For all $j \geq 0$, we have $\sigma(\alpha^j) - \alpha^j \in (\sigma(\alpha) - \alpha)\mathcal{O}_L \in \mathfrak{m}_L^{i+1}$. Therefore

$$\sigma(x) - x = \sum_{j \geq 0} a_j(\sigma(\alpha)^j - \alpha^j) \in \mathfrak{m}_L^{i+1},$$

so $\sigma \in G_i$. □

For each $\sigma \in G \setminus \{1\}$, define

$$i_G(\sigma) = v_L(\sigma(\alpha) - \alpha) \in \mathbb{N}.$$

This also the biggest integer i such that $\sigma \in G_{i-1}$ and $\sigma \notin G_i$. By convention $i_G(1) = +\infty$.

Proposition 3.54. *We have $G_i = \{1\}$ for i big enough.*

Proof. The equality holds when $i \geq \max_{\sigma \in G, \sigma \neq 1}\{i_G(\sigma)\}$. □

Now we study the structure of the quotient groups G_i/G_{i+1}. As $G_{-1}/G_0 = D/I$ is isomorphic to the Galois group of the residue extension of L/K, we concentrate ourselves to $i \geq 0$. Denote by $U^{(0)} = \mathcal{O}_L^*$ and for all $i \geq 1$, $U^{(i)} = 1 + \mathfrak{m}_L^i$. We saw in the midterm exam that we haev an isomorphism of groups $U^{(i)}/U^{(i+1)} \simeq k$ for all $i \geq 0$.

Proposition 3.55. *Fix a uniformizing element π_L of $\mathcal{O}_L$. Let $i \geq 0$.*

1. *Let $\sigma \in G_0$. Then $\sigma \in G_i$ if and only if $\sigma(\pi_L)/\pi_L \in U^{(i)}$.*

2. *The map $\sigma \mapsto \sigma(\pi_L)/\pi_L$ induces an injective group homomorphism*

$$G_i/G_{i+1} \to U^{(i)}/U^{(i+1)}.$$

Proof. We work with G_0, hence with the extension L/L^{G_0} which is totally ramified. We can suppose $K = L^{G_0}$. Therefore $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$. Now $\sigma \in G_i$ if and only if $\sigma(\pi_L) - \pi_L \in \pi_L^{i+1}$, which is equivalent to $\sigma(\pi_L)/\pi_L \in U^{(i)}$. This proves (1).

Let us prove that the map $\phi_i : G_i \to U^{(i)}/U^{(i+1)}$ induced by $\sigma \mapsto \sigma(\pi_L)/\pi_L$ is a group homomorphism. Let $\sigma_1, \sigma_2 \in G_i$. Write $\sigma_2(\pi_L) = \pi_L u$ with $u \in U^{(i)}$. Then

$$\frac{(\sigma_1\sigma_2)(\pi_L)}{\pi_L} = \frac{\sigma_1(\pi_L)}{\pi_L}\sigma_1(u) = \frac{\sigma_1(\pi_L)}{\pi_L}\frac{\sigma_2(\pi_L)}{\pi_L}\frac{\sigma_1(u)}{u}.$$

As $\sigma_1 \in G_i$, $\sigma_1(u) - u \in \mathfrak{m}_L^{i+1}$, hence $\sigma_1(u)/u \in U^{(i+1)}$. This implies that

$$\frac{(\sigma_1\sigma_2)(\pi_L)}{\pi_L} \equiv \frac{\sigma_1(\pi_L)}{\pi_L}\frac{\sigma_2(\pi_L)}{\pi_L} \mod U^{(i+1)}.$$

Finally, the kernel of ϕ_i is G_{i+1} by (1). So ϕ_i induces an injective group homomorphism as desired. □

Corollary 3.56. *Suppose* $\mathrm{char}(k) = p > 0$.

1. *The quotient G_0/G_1 is isomorphic to a subgroup of k^* and is cyclic of order prime to p.*
2. *For all $i \geq 1$, G_i/G_{i+1} is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{r_i}$ for some $r_i \geq 0$.*

Proof. (1) It is well-knwon that any finite subgroup of k^* is cyclic. Here the order is prime to p because there is no non-trivial element of order p in k^*.

(2) This is because k is a $\mathbb{F}_p$-vector space. □

We see that G_1 is nothing but the p-Sylow P of $I = G_0$ (Theorem 3.48).

Exercise 3.57 Let F be a subextension of L/K, let $H = \mathrm{Gal}(L/F)$. Then the filtration of H is given by $H_i = G_i \cap H$, and we have $i_H = i_G|_H$.

Example 3.58 Let p be a prime number, $K = \mathbb{Q}_p$ and $L = \mathbb{Q}_p(\zeta_{p^r})$ $(r \geq 1)$. We saw in Example 3.31 that L/K is totally ramified of degree $(p-1)p^{r-1}$. In particular $[L : K] = [\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}]$. The canonical homomorphism

$$\mathbb{Q}_p \otimes_{\mathbb{Q}} \mathbb{Q}[\zeta_{p^r}] \to L$$

is surjective, and both sides have the same (finite) dimension over $\mathbb{Q}_p$, so it is an isomorphism and L/K is Galois with Galois group $\mathrm{Gal}(\mathbb{Q}[\zeta_{p^r}]/\mathbb{Q})$. The map

$$(\mathbb{Z}/p^r\mathbb{Z})^* \to G = \mathrm{Gal}(L/K), \quad \bar{m} \mapsto \sigma_m : \zeta_{p^r} \mapsto \zeta_{p^r}^m$$

is an isomorphism of groups. A uniformizer of L is $\lambda_{p^r} := 1 - \zeta_{p^r}$, so $\mathcal{O}_L = \mathbb{Z}_p[\lambda_{p^r}]$.

Let us determine the lower ramification groups. For all $q \leq r$, denote by $\zeta_{p^q} = \zeta_{p^r}^{p^{r-q}}$ a primitive p^q-th root of unity. Let $\bar{m} \in (\mathbb{Z}/p^r\mathbb{Z})^*$ be different from 1. We have

$$\sigma_m(\lambda_{p^r}) - \lambda_{p^r} = \zeta_{p^r}(1 - \zeta_{p^r}^{m-1}).$$

Let $s = v_p(m-1)$. Write $m - 1 = p^s m'$ with m' prime to p. Then

$$1 - \zeta_{p^r}^{m-1} = 1 - \zeta_{p^{r-s}}^{m'}$$

is a uniformizer of $L_{r-s} := \mathbb{Q}_p(\zeta_{p^{r-s}})$. Therefore

$$v_L(1-\zeta_{p^r}^{m-1}) = e_{L/L_{r-s}} = \frac{e_{L/\mathbb{Q}_p}}{e_{L_{r-s}/\mathbb{Q}_p}} = \frac{[L:\mathbb{Q}_p]}{[L_{r-s}:\mathbb{Q}_p]} = p^s$$

and $i_G(\sigma_m) = p^s$. In otherwords, $\sigma_m \in G_{p^s-1} \setminus G_{p^s}$.

To summarize, for all $i \geq 0$, we have

$$G_i = \begin{cases} \ker((\mathbb{Z}/p^r\mathbb{Z})^* \to (\mathbb{Z}/p^s\mathbb{Z})^*) & \text{if } \ p^{s-1} \leq i \leq p^s - 1 \\ \{1\} & \text{if } \ i \geq p^{r-1}. \end{cases}$$

In another words,

$$G_{-1} = G_0 \supset G_1 = G_2 = ... = G_{p-1} \supset G_p = G_{p+1} = ... = G_{p^2-1} \supset G_{p^2} ...$$

with $G_{p^s} = \ker((\mathbb{Z}/p^r\mathbb{Z})^* \to (\mathbb{Z}/p^{s+1}\mathbb{Z})^*)$ for all $0 \leq s \leq r-1$.

4 Some applications in algebraic geometry

4.1 Height on projective spaces over $\bar{\mathbb{Q}}$

It is a classical fact that for any $r \in \mathbb{Q}^*$, we have

$$|r| \prod_p |r|_p = 1.$$

We want to generalize this to some other fields.

Let K be a field, let M_K be a set of (non equivalent) absolute values on K and for each $v \in M_K$ we are given a real number $\lambda_v > 0$. We say that $(M_K, \{\lambda_v\}_{v \in M_K})$ satisfies the *product formula* if the following conditions are satisfied:

1. All but finitely many v's are ultrametric (and discrete);
2. for all $x \in K^*$ we have $|x|_v = 1$ except for finitely many v's;
3. for all $x \in K^*$
$$\prod_{v \in M_K} \|x\|_v = 1$$
where $\|x\|_v = |x|_v^{\lambda_v}$.

Example 4.1 For $K = \mathbb{Q}$, the set of the p-adic absolute values and the usual absolute value together with $\lambda_v = 1$ for all v, satisfies the product formula.

Example 4.2 Let $K = k(X)$ be the field of fractions over a field k. Fix a positive real number $c > 0$. For any maximal ideal $\mathfrak{m}$ of $k[X]$, we consider the normalized $\mathfrak{m}$-adic valuation $K^* \to \mathbb{Z}$ and put $|x|_{\mathfrak{m}} = c^{-v_{\mathfrak{m}}(x)}$. Define $|\ |_\infty$ as the absolute value defined as above for the maximal ideal $(1/X)k[1/X]$ of $k[1/X]$. For each of these absolute value put $\lambda_v = 1$. Then we have the product formula property.

Now let M_K be as above with product formula. Let L be a finite separable extension of K. We are going to construct a family of absolute values on L satisfying the product formula.

For each $v \in M_K$, consider the completion K_v of K with respect to v. We know that v extends to finitely many absolute values $w_1, \ldots, w_n$ on L and that

$$L \otimes_K K_v \simeq \prod_i L_{w_i}.$$

We let M_L be the set of all such extensions w's. When $w \in M_L$ is an extension of some $v \in M_K$ we say that w *divides* v and we write $w \mid v$. Put

$$\|x\|_w := \|N_{L_w/K_v}(x)\|_v^{1/d}.$$

Note that $|x|_w = |N_{L_w/K_v}(x)|^{1/[L_w:K_v]}$ (Theorem 1.57), so

$$\|x\|_w = |x|_w^{[L_w:K_v]/d}$$

is an absolute value on L.

Lemma 4.3. *Keep the above notation.*

1. *Fix $v \in M_K$. For all $x \in L$ we have*
$$\prod_{w|v} \|x\|_w = \|N_{L/K}(x)\|_v^{1/d}.$$

2. *For all $x \in L$,*
$$\prod_{w \in M_L} \|x\|_w = 1.$$

3. *If $x \in K$, then*
$$\prod_{w|v} \|x\|_w = \|x\|_v.$$

Proof. (1) For any finite algebra E over a field F one can define the norm $N_{E/F}(x) \in F$ of an element $x \in E$ as the determinant of the multiplication-by-x (F-linear) endomorphism of E. Then it is clear that $N_{E/F}$ commutes with field extensions on F.

In our case we get $N_{L/K}(x) = N_{L\otimes_K K_v/K_v}(x \otimes 1)$. As $L \otimes_K K_v$ is the direct sum of the L_w's, we have $N_{L/K}(x) = \prod_w N_{L_w/K_v}(x)$, where we identify x with its image in L_v. This implies (1).

(2) This is a consequence of (1) and of the product formula on K. And (3) is true because $N_{L/K}(x) = x^{[L:K]}$ when $x \in K$. □

Definition 4.4 Let $n \geq 1$. Let $P = [x_0, \ldots, x_n] \in \mathbb{P}^n(K)$. Put
$$H_K(P) := \prod_{v \in M_K} \sup_{0 \leq i \leq n} \|x_i\|_v.$$

The product formula insures that the above number does not depend on the choice of the homogeneous coordinates. We have $H_K(P) \geq 1$.

Lemma 4.5. *Let L/K be a finite separable extension.*

1. *Let $P \in \mathbb{P}^n(K) \subset \mathbb{P}^n(L)$. Then $H_K(P) = H_L(P)$. We will drop K from the subscript of H. The latter is then defined over $\mathbb{P}^n(K^s)$ for a separable closure K^s of K.*

2. *Let $P \in \mathbb{P}^n(L)$ and let $\sigma : L \to K^c$ be an embedding of L in an algebraic closure of K. Then $H(\sigma(P)) = H(P)$.*

Proof. (1) For any $v \in M_K$ and any $w \mid v$, we have $\|x_i\|_w = \|x_i\|_v^{[L_w:K_v]/d}$. So
$$\sup_{0 \leq i \leq n} \|x_i\|_w = \sup_{0 \leq i \leq n} \|x_i\|_v^{[L_w:K_v]/d} = (\sup_{0 \leq i \leq n} \|x_i\|_v)^{[L_w:K_v]/d}$$
and $\prod_{w|v} \sup_{0 \leq i \leq n} \|x_i\|_w = \sup_{0 \leq i \leq n} \|x_i\|_v$. This implies that $H_K(P) = H_L(P)$.

(2) We can enlarge L and suppose L/K is finite and Galois. Then the equality comes from the fact that $\mathrm{Gal}(L/K)$ acts on the $w \in L$ by $|x|_{\sigma(w)} := |\sigma(x)|_w$ for all $\sigma \in \mathrm{Gal}(L/K)$ and for all $x \in L$. □

Lemma 4.6. *Let B be a constant. Then the set*

$$\{P \in \mathbb{P}^n(\mathbb{Q}) \mid H(P) \leq B\}$$

is finite.

Proof. Any point $P \in \mathbb{P}^n(\mathbb{Q})$ can be written with integral coordinates $[a_0, \ldots, a_n]$ such that $\gcd(a_0, \ldots, a_n) = 1$. For all prime numbers p, we then have

$$\sup_{0 \leq i \leq n} |a_i|_p = 1.$$

Thus $H(P) = \sup_{0 \leq i \leq n} |a_i|$. This implies clearly the finiteness results. □

Next we want to generalize this result to $\mathbb{P}^n(\bar{\mathbb{Q}})$. Let $P = [x_0, \ldots, x_n] \in \mathbb{P}^n(\bar{\mathbb{Q}})$. We define the *degree of* P as the degree of the extension $K(P) := K(x_i/x_{i_0})$ of K for any index i_0 such that $x_{i_0} \neq 0$. The extension $K(P)$ does not independ on the choice of i_0. We define the height function H on $\mathbb{P}^n(\bar{\mathbb{Q}})$ as above starting from $K = \mathbb{Q}$ with the usual choice of M_K.

Theorem 4.7 (Northcott)**.** *Fix a constant $B \geq 1$. Then the set*

$$\{P \in \mathbb{P}^n(\bar{\mathbb{Q}}) \mid H(P) \leq B,\ \deg P \leq B\}$$

is finite.

Proof. We first reduce the theorem to the case $n = 1$. Let $P = [x_0, x_1, \ldots, x_n] \in \mathbb{P}^n(\bar{\mathbb{Q}})$. We can suppose that at least one of the homogeneous coordinates is equal to 1. Then for any $0 \leq j \leq n$, we have

$$\sup_i \|x_i\|_v \geq \sup\{1, \|x_j\|_v\}$$

and $H(P) \geq H(P_j)$, where $P_j = [1, x_j] \in \mathbb{P}^1(\bar{\mathbb{Q}})$. Moreover $\deg P_j \leq \deg P$. As the P_j's determine P, it is enough to show the theorem for $\mathbb{P}^1(\bar{\mathbb{Q}})$.

So let $P = [1, \alpha] \in \mathbb{P}^1(\bar{\mathbb{Q}})$ with $H(P), \deg P \leq B$. Let $f(X) = X^d + a_1 X^{d-1} + \cdots + a_d$ be the minimal polynomial of α over $\mathbb{Q}$. Let $\alpha_1, \ldots, \alpha_d \in \bar{\mathbb{Q}}$ be the roots of $f(X)$. For any $0 \leq r \leq d-1$, we have

$$a_r = (-1)^r \sum_{1 \leq j_1 < j_2 < \ldots < j_r \leq d} \alpha_{j_1} \ldots \alpha_{j_r}.$$

Let L be the Galois closure of $K(P)/\mathbb{Q}$. For any $w \in M_L$, we have

$$\|a_r\|_w \leq c(w,d)(\sup_{1 \leq j \leq d} \|\alpha_j\|_w)^r \leq c(w,d)(\prod_{1 \leq j \leq d} \sup\{1, \|\alpha_j\|_w\})^r$$

where $c(w,d) = 1$ if w is ultrametric, and $c(w,d) = \binom{d}{r} \leq 2^d$ otherwise. Note that we take the product on the $j \leq d$ to make the right-side independent on j, as the product (on w's) of sup's (on $j \leq d$ is not bounded by the sup (on the $j \leq d$ of the products (on w's). Thus

$$\sup\{1, \|a_r\|_w\} \leq c(w,d) \prod_{1 \leq j \leq d} (\sup\{1, \|\alpha_j\|_w\})^r$$

and

$$H([1,a_r]) \leq \prod_{w\in M_L} c(w,d) \prod_{1\leq j\leq d} (\sup\{1,\|\alpha_j\|_w\})^r = \prod_w c(w,d) \prod_{1\leq j\leq d} H([1,\alpha_j])^r.$$

By Lemma 4.5, $H([1,\alpha_j]) = H([1,\alpha]) \leq B$. The number q of archimedean absolute values in M_L is bounded by $[L:\mathbb{Q}] \leq d!$. So $H([1,a_r]) \leq 2^{dq}B^{dr}$. By Lemma 4.6, there are only finitely such $a_r \in \mathbb{Q}$. So there are only finitely many $f(X)$'s, hence finitely many α's. □

Remark 4.8 The definition of the height on $\mathbb{P}^n(\bar{\mathbb{Q}})$ depends closely on the choice of a system of homogeneous coordinates. More precisely, if $\sigma \in \mathrm{PGL}_n(\mathbb{Q})$, then $H(\sigma(P)) \neq H(P)$ in general. This can be checked when $n = 1$, and $\sigma([x,y]) = [2x,y]$. However there exist constants $\alpha_\sigma, \beta_\sigma \in \mathbb{R}$ such that

$$\alpha_\sigma + \ln H(P) \leq \ln H(P) \leq \beta_\sigma + \ln H(P)$$

for all $P \in \mathbb{P}^n(\bar{\mathbb{Q}})$. We say that the logarithmetic height $h(P) := \ln H(P)$ is well defined (independent on the choice of a system of coordinates) up to bounded functions on $\mathbb{P}^n(\bar{\mathbb{Q}})$.

4.2 Duality for finite morphisms

Serre duality. Let X be a connected smooth projective variety of dimension d over a field k (algebraically closed if you want). Serre's duality theory states that, for any locally free and finite rank sheaf $\mathcal{F}$ on X, and for any $0 \leq i \leq d$, there is a canonical isomorphism of k-vector spaces

$$H^i(X,\mathcal{F}) \simeq H^{d-i}(X,\mathcal{F}^\vee \otimes \Omega^d_{X/k})^\vee$$

where $\mathcal{F}^\vee = \mathcal{H}om_{\mathcal{O}_X}(\mathcal{F},\mathcal{O}_X)$ and $H^{d-i}(*)^\vee$ stands for the dual as k-vector space. This isomorphism is given by a nondegenerate bilinear form

$$H^i(X,\mathcal{F}) \times H^{d-i}(X,\mathcal{F}^\vee \otimes \Omega^d_{X/k}) \to H^d(X,\Omega^d_{X/k}) \simeq k.$$

Now if $f : X \to Y$ is a finite surjective morphism of connected smooth projective varieties over k, by general facts on differential forms there exists a sheaf ω_f on X such that

$$\Omega^d_{X/k} \simeq f^*(\Omega^d_{Y/k}) \otimes_{\mathcal{O}_X} \omega_f.$$

The sheaf $\Omega^d_{X/k}$ is the *dualizing sheaf* for X and ω_f is the *relative dualizing sheaf* for $X \to Y$. They are both invertible sheaves on X.

When f is generically separable (*i.e.* the finite extension $k(Y) \to k(X)$ induced by f is separable), the sheaf ω_f can be described locally as follows. If $B := \mathcal{O}_X(f^{-1}(V))$ is monogeneous over $A := \mathcal{O}_Y(V)$, so $B = A[\alpha]$, we denote by $P(X) \in A[X]$ the minimal polynomial of α over $\mathrm{Frac}(A)$. Again by general fact from differential forms, one can show that

$$\omega_f(f^{-1}(V)) = P'(\alpha)^{-1}\mathcal{O}_X(f^{-1}(V)).$$

This means that there exists a closed subvariety $V(\mathcal{I}_f) \subset X$ with $\mathcal{I}_f$ locally principal such that

$$f^*\Omega^d_{Y/k} = \mathcal{I}_f \Omega^d_{X/k}.$$

The monogeneity hypothesis is satisfied if $\dim X = 1$ and k is infinite (Lemma 3.18 and Proposition 3.21) and we then can view $V(\mathcal{I}_f)$ as a divisor on X:

$$V(\mathcal{I}_f) = \sum_x \dim_k(\mathcal{O}_{X,x}/\mathcal{I}_{f,x})[x].$$

If v_x denotes the normalized discrete valuation on $k(X)$ corresponding to the dvr $\mathcal{O}_{X,x}$, and if t_x is a generator of $\mathcal{I}_{f,x}$, then

$$\dim_k(\mathcal{O}_{X,x}/\mathcal{I}_{f,x}) = v_x(t_x).$$

Theorem 4.9 (Riemann-Hurwitz)**.** *Let $f : X \to Y$ be a finite generically separable morphism of connected smooth projective curves over an algebraically closed field k. Let $d = [k(X) : K(Y)]$. Then*

$$2(g(X) - 1) = 2d(g(Y) - 1) + \deg V(\mathcal{I}_f).$$

Let us compute $\deg V(\mathcal{I}_f)$. We want to relate it to the ramification data of f. Let $K = k(Y)$, $L = k(X)$ and $\mathcal{O}_K = \mathcal{O}_{Y,y}$ where $y = f(x)$. Suppose for simplicity that $f^{-1}(y) = \{x\}$, so that $\mathcal{O}_K \to \mathcal{O}_{X,x}$ is totally ramified. Then $\mathcal{O}_{X,x} = \mathcal{O}_K[\alpha]$ with α a uniformizing element of $\mathcal{O}_{X,x}$, root of an Eisenstein polynomial

$$P(T) = T^e + a_{e-1}T^{e-1} + \cdots + a_0 \in \mathcal{O}_K[T]$$

with $e = e_{\mathcal{O}_{X,x}/\mathcal{O}_{Y,y}}$. As $v_x(a_i) \geq e$, we see that $v_x(P'(\alpha)) = e - 1$ if e is invertible in k, and $v_x(P'(\alpha)) \geq e$ otherwise.

Corollary 4.10. *Keep the above hypothesis.*

1. *If $f : X \to Y$ is unramified, then $g(X) - 1 = d(g(Y) - 1)$.*
2. *We have*

$$2(g(X) - 1) = d(2g(Y) - 1) + \sum_x (e_{x/f(x)} - 1).$$

if and only if f is tamely ramified (i.e., for all $x \in X$, $\mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$ is tamely ramified).

How to compute $\deg V(\mathcal{I}_f)$ when f has possibly wild ramifications ? We suppose that $f : X \to Y$ is Galois. Fix $x \in X$ and denote by $D = \{\sigma \in G \mid \sigma(x) = x\}$ the decomposition group at x. Let $D_{-1} = D \supseteq D_0 \supseteq D_1 \supseteq ...$ be the ramification subgroups.

Proposition 4.11. *We have*

$$\dim_k(\mathcal{O}_{X,x}/\mathcal{I}_{f,x}) = \sum_{\sigma \in D, \sigma \neq 1} i_D(\sigma) = \sum_{i \geq 0} (|D_i| - 1).$$

where the D_i's are the lower ramification groups of D.

Proof. We have $\dim_k(\mathcal{O}_{X,x}/\mathcal{I}_{f,x}) = v_x(P'(\alpha))$. Again suppose $G = D$ for simplicity. We have $P(X) = \prod_\sigma (X - \sigma(\alpha))$, so $P'(\alpha) = \prod_{\sigma \neq 1}(\alpha - \sigma(\alpha)$ and

$$v_x(P'(\alpha) = \sum_{\sigma \neq 1} v_x(\alpha - \sigma(\alpha)) = \sum_{\sigma \neq 1} i_G(\sigma).$$

$$\sum_{\sigma\neq 1} i_G(\sigma) = \sum_{i\geq 0}\sum_{i_G(\sigma)=i} i_G(\sigma) = \sum_{i\geq 0} i|G_{i-1}\setminus G_i| = \sum_i (|G_i|-1).$$

□

Example 4.12 Let k be an algebraically closed field of $\mathrm{char}(k) = 2$. Consider the extension of $k(T)$ defined by $z^2 + T^n z = TQ(T)$ with $Q(0) \neq 0$ and $2n \geq 1 + \deg Q(T)$. This extension defines a morphism $f : X \to \mathbb{P}^1_k$ from a smooth connected curve X to $\mathbb{P}^1_k$. Over the affine open subset $V = \{T \neq \infty\}$ of $\mathbb{P}^1_k$, the equation of X is

$$z^2 + T^n z = TQ(T)$$

because by Jacobian criterion the above affine plane curve U is smooth. The cover $U \to V$ is ramified only at $q := (T = Z = 0)$ with ramification index 2 because $T(Q(T) - T^{n-1}z) = z^2$ and $Q(T) - T^{n-1}z \in \mathcal{O}^*_{U,q}$. We have $\mathcal{O}_X(U) = \mathcal{O}(V)[z]$. The Galois group of $k(X)/k(T)$ is generated by the involution

$$\sigma : z \mapsto z + T^n.$$

So $v_q(\sigma(z) - z) = v_q(T^n) = nv_q(T) = 2n$. Above ∞, the equation of X is

$$(z/T^n)^2 + (z/T^n) = TQ(T)/T^{2n}$$

with $TQ(T)/T^{2n} \in k[1/T]$. It is unramified over ∞. So Riemann-Hurwitz formula says that $2g(X) - 2 = -4 + 2n$ and

$$g(X) = n - 1.$$

References

[1] *F. Lorenz:* Algebra II, Universitext (2008), Springer (§23-24).

[2] *J.P. Serre:* Local fields, GTM 67 (1979), Springer (Chapters I, II and IV).