VALUED FIELDS

MICHAEL TEMKIN

1. Real valuations and real valued field

1.1. **Some history and plan of the chapter.** Early history of the theory of real valuations is surveyed in detail in the notes [Roq02] of Roquette. Another reference is [Bou72, Chapter VI, §6]. Here we only mark the main points and the interested reader is referred to these references.

In 1908 Hensel published a book ..., where he introduced p-adic numbers via formal series $\sum_{n\geq n_0}^{\infty} a_n p^n$. This puzzled mathematicians and led to the usual philosophical question: "do they really exist"? Real valuations were defined by Joseph Kürschák in a work announced in Cambridge in 1912 and published in 1913 in [Kür13]. His motivation was to provide a rigorous framework for p-adic numbers, and to show that $\mathbb{Q}_p$ can be embedded into an algebraically valued complete real valued field. The main step was to show that real valuation extend through finite extensions, where he extended to this setting a result of Hadamard on radii of convergence of algebraic functions. The other steps are easier: one completes $\overline{\mathbb{Q}_p}$ with respect to the obtained valuation and proves that the obtained field $\mathbb{C}_p$ is algebraically closed. Note also that Kürschák suspected that $\overline{\mathbb{Q}_p}$ is not complete and the latter steps are necessary, but this was proved by Ostrowski later.

In 1918 Ostrowski proved two classification theorems: he classified real valuations on $\mathbb{Q}$ by showing that the only non-trivial completions are $\mathbb{Q}_p$ and $\mathbb{R}$, and showed that $\mathbb{R}$ and $\mathbb{C}$ are the only archimedean complete real valued fields. This allowed to simplify the proof that valuations extend by excluding the archimedean case and using Hensel's lemma, which is only available in the non-archimedean setting. In fact, it was Ostrowski who first proved it in this generality.

1.2. **Definitions and Ostrowski's theorem.**

1.2.1. *Norms and real valuations.* A *seminorm* on a ring A is a map $|\ |\colon A \to \mathbb{R}_{\geq 0}$ such that $|0| = 0$, $|a| = |-a|$, $|a+b| \leq |a| + |b|$ and $|ab| \leq |a| \cdot |b|$. The kernel $\mathrm{Ker}(|\ |) = \{x \in A|\ |x| = 0\}$ is obviously an ideal. A seminorm is a *non-archimedean* if it satisfies the *strong triangle inequality* $|a+b| \leq \max(|a|, |b|)$. A seminorm is *power mulitplicative* if $|a^n| = |a|^n$ for any $a \in A$ and $n \in \mathbb{N}$. A power multiplicative seminorm is called *archimedean* if the axiom of Archimedes is satisfied: for any $x \in A$ there exists $n \in \mathbb{N}$ such that $|n| > |x|$. Clearly, this happens if and only there exists $n \in \mathbb{N}$ with $|n| > 1$.

A seminorm is a *real semivaluation* if it is multiplicative: $|1| = 1$ and $|ab| = |a| \cdot |b|$. In particular, in this case $\mathrm{Ker}(|\ |)$ is a prime ideal.

A seminorm is a *norm* (resp. a real semivaluation is a *real valuation*) if $\mathrm{Ker}(|\ |) = 0$. A pair $(A, |\ |)$ will be called seminormed ring (resp. normed ring, real semivalued ring, or real valued ring).

1.2.2. *Archimedean versus non-archimedean dichotomy.* Recall that we have defined the property of being non-archimedean via the strong triangle inequality, and the property of being archimedean via the archimedes axiom that $|\mathbb{N}|$ is unbounded. The above theorem implies that this is indeed a dichotomy, and there exists no third possibility.

Theorem 1.2.3. *The following conditions for a real semivaluation $|\ |$ on a ring A are equivalent:*

(1) *$|\ |$ is not archimedean, that is, $|\mathbb{Z}| \le 1$,*
(2) *$|\ |$ is non-archimedean,*
(3) *the induced semivaluation $|\ |_{\mathbb{Z}}$ on $\mathbb{Z}$ is non-archimedean.*

Proof. The implications (2)$\Longrightarrow$(3) is obvious. If (3) holds, then $|n+1| \le \max(|n|, 1)$ hence $|\mathbb{N}| \le 1$ by induction on n, and hence also $|\mathbb{Z}| \le 1$. It remains to prove (1)$\Longrightarrow$(2), so assume that $|\mathbb{Z}| \le 1$. Given $x, y \in A$ let $r = \max(|x|, |y|)$. Estimating $|x+y|^n = |(x+y)^n|$ via the binomial expansion yields

$$|x+y|^n \le (n+1)r^n \max_{0\le i\le n} \left| \binom{n}{i} \right| \le (n+1)r^n.$$

Extracting the n-root and passing to the limit we obtain that $|x+y| \le r$, that is, the semivaluation is non-archimedean. □

As an immediate corollary we obtain

Corollary 1.2.4. *A semivaluation $|\ |$ on a ring A is non-archimedean (resp. archimedean) if and only if so is the induced semivaluation $|\ |_{\mathbb{Z}}$ on $\mathbb{Z}$.*

Exercise 1.2.5. An open ball $B_r(a)$ (resp. closed ball $E_r(a)$) of radius r with center at $a \in A$ is defined to be the set of all elements $x \in A$ such that $|x - a| < r$ (resp. $|x - a| \le r$). Show that any element of a non-archimedean ball is its center and a closed unit ball is a union of open ones.

1.2.6. *Extension to fields of fractions.* Valued rings are analogues of domains in the seminormed algebra. In particular, this is indicated by the following result.

Lemma 1.2.7. *Any real valuation $|\ |$ on a domain A extends by multiplicativity to the ring of fractions $K = \mathrm{Frac}(A)$, yielding an isometric embedding of $(A, |\ |)$ into a real valued field.*

Proof. One should only check that $|\frac{a}{b}|_K = \frac{|a|}{|b|}$ defines a subadditive function on K:

$$\frac{|a|}{|b|} + \frac{|c|}{|d|} \ge \frac{|ad+bc|}{bd}.$$

This follows from the subadditivity of $|\ |$. □

Exercise 1.2.8. Any seminorm $|\ |$ factors canonically into a composition of $A \to A' = A/\mathrm{Ker}(|\ |)$ and a norm $|\ |' \colon A' \to \mathbb{R}_{\ge 0}$. In other words, any seminorm is induced from the quotient norm on the factor by its kernel.

Any homomorphism from a ring A to a real valued field K induces a real semivaluation on A. We say that $A \to K_1$ and $A \to K_2$ are equivalent if they factor through $A \to K$ and isometric immersions $K \hookrightarrow K_i$. In particular, each equivalence class contains the minimal element generated (as a field) by the image of A. Conversely, if A is real semivalued, $A/\mathrm{Ker}(|\ |)$ is real valued and its fraction field acquires a natural real valuation by Lemma 1.2.7. This can be summarized as follows:

Lemma 1.2.9. *For a ring A there is a natural bijection between real semivaluations on A and equivalence classes of homomorphism from A to valued fields. The minimal representative of the class corresponding to $|\ |$ is $A \to \mathrm{Frac}(A/\mathrm{Ker}(|\ |))$.*

1.2.10. *First examples.* The *trivial norm* $|\ |_0$ on A is defined by $|a|_0 = 1$ if $a \neq 0$. It is a real valuation if and only if 0 is a prime ideal.

The usual archimedean absolute value $|\ |_\infty$ on $\mathbb{C}$ induces a real valuation on any subring of $\mathbb{C}$. Moreover, $|\ |_\infty^r$ satisfies the triangle inequality for $0 < r \leq 1$ and hence is a real valuation too. The norms in this family are archimedean, and they tend to $|\ |_0$ as r tends to 0.

For any prime p the trivial valuation on $\mathbb{F}_p$ induces a valuation on $\mathbb{Z}$ that we symbolically denote $|\ |_p^\infty$. They satisfy $|p\mathbb{Z}|_p^\infty = 0$ and $|\mathbb{Z} \setminus p\mathbb{Z}|_p^\infty = 1$.

For any $n \in \mathbb{Z}$ choose maximal power of p dividing n, say p^l, and set $|n|_p = p^{-l}$. This is a non-archimedean real valuation on $\mathbb{Z}$ called the *p-adic valuation*. It extends to the whole $\mathbb{Q}$ by multiplicativity, and $|p^l \frac{m}{n}|_p = p^{-l}$ for any $m, n \in \mathbb{Z} \setminus p\mathbb{Z}$. For any $r > 0$ the power $|\ |_p^r$ is also a non-archimedean valuation.

In the same venue, if k is a field then any element $h \neq 0$ of $k(t)$ can be represented as $t^n \frac{f(t)}{g(t)}$ with $f, g \in k[t] \setminus tk[t]$. Fixing any $s \in (0,1)$ and setting $|h|_t = s^{-n}$ one obtains a non-archimedean *t-adic* valuation. This time there is no natural normalization, so the choice $s \in (0,1)$ is arbitrary.

Finally, one possible way to generalize the last two examples is as follows. Assume that A is a unique factorization domain with $K = \mathrm{Frac}(A)$, and $\pi \in A$ is a prime. Then any element $x \in K^\times$ can be represented as $\pi^l \frac{a}{b}$ with $a, b \in A \setminus \pi A$, and setting $|x|_\pi = s^{-l}$ defines a π-adic valuation on A and K.

Exercise 1.2.11. Verify the above examples.

1.2.12. *Gauss valuations.* Let k be a non-archimedean real valued field. Given $r \geq 0$ consider the real valued function $|\ |_r = |\ |_{t,r}$ on $k[t]$ given by $|\sum a_i t^i|_{t,r} = \max_i r^i |a_i|$. Since k is non-archimedean it is easy to see that $|\ |_r$ is a semivaluation. One calls $|\ |_1$ *Gauss valuation* because the fact that it is a valuation is essentially the classical Gauss lemma. For $r > 0$ it is called a *generalize Gauss valuation* or *t-monomial* valuation. The latter notion indicates that the valuation is defined by its values on the monomials.

Exercise 1.2.13. Check that $|\ |_r$ is indeed a valuation. Describe $|\ |_r$ when k is trivially valued: if $r < 1$ then it is t-adic, if $r = 1$ then it is trivial, and if $r > 1$ then $|f(t)|_r = r^{\deg(f)}$ and the continuation to $k(t)$ is t^{-1}-adic.

1.2.14. *Ostrowski's theorem.* Any ring A admits a unique homomorphism $\mathbb{Z} \to A$, hence any real semivaluation $|\ |$ (or seminorm) on A induces a real semivaluation on $\mathbb{Z}$. The latter is a simplest invariant of $|\ |$, so it is natural to start studying real semivaluations (or valuations) with classifying them on $\mathbb{Z}$. In fact, we have already seen all possibilities as the following famous theorem states:

Theorem 1.2.15 (Ostrowski)**.** *The full list of real semivaluations on $\mathbb{Z}$ is as follows:*

(0) *The trivial valuation $|\ |_0$.*
(1) *The archimedean valuations $|\ |_\infty^r$ with $r \in (0,1]$.*

(2) *The p-adic valuations $|\ |_p^r$ with $r \in (0, \infty)$.*
(3) *The semivaluations $|\ |_p^\infty$ with non-trivial kernels.*

and the full list of real semivaluations on $\mathbb{Q}$ is obtained by removing case (3).

Proof. We have checked earlier that everything in the list is a semivaluation on $\mathbb{Z}$ (resp. $\mathbb{Q}$). Let us check that a real semivaluation on $\mathbb{Z}$ belongs to the list. Assume first that $|\ |$ is not a valuation. Then the kernel is a non-trivial prime ideal, say $p\mathbb{Z}$. It follows that $|a + pb| = |a|$, and hence $|\ |$ is induced from a semivaluation on $\mathbb{F}_p$. For any $x \in \mathbb{F}_p^\times$ we have that $|x|^{p-1} = |x^{p-1}| = |1| = 1$. Hence $|x| = 1$ and we obtain that the semivaluation on $\mathbb{F}_p$ is trivial, and $|\ | = |\ |_p^\infty$.

In the sequel we assume that $|\ |$ is a valuation. Assume first that the valuation is archimedean, in particular, there exists $a \in \mathbb{N}$ with $|a| > 1$. Fix a natural $m > 1$ and set $C = \max(1, |2|, \dots, |m-1|)$. For any natural $n > 1$ consider the base m-decomposition $n = \sum_{i=0}^d a_i m^i$, where $d = [\log_m(n)]$, and note that $|n| \le C \sum_{i=0}^d |m|^d$. For $|m| < 1$ this would imply that $|n| < \frac{C}{1-|m|}$ contradicting that $|\mathbb{N}|$ is unbounded. For $|m| = 1$ this would imply that $|n| \le C(d+1)$ and hence growthes at most linearly in $\log(n)$. This contradicts that $|a^l| = |a|^l$ growthes exponentially in l.

Thus, $|m| > 1$ and $|n| \le C'|m|^d$, for the constant $C' = \frac{C|m|}{|m|-1}$. Substituting n^l instead of n and applying $\log_{|m|}$ yields $l \log_{|m|}(|n|) \le \log_{|m|}(C') + [l \log_m(n)]$. Dividing by l and tending it to infinity we obtain that $\log_{|m|}(|n|) \le \log_m(n)$. The same argument with switched m and n yields the opposite inequality $\log_{|m|}(|n|)^{-1} \le \log_m(n)^{-1}$. Hence the equality holds and we obtain that $|n| = |m|^{\log_m(n)}$ for any $n > 1$. This implies that $|n| = n^r$, where $r = \log_m(|m|) > 0$. Since $|2| \le |1|+|1| = 2$, we have that $r \le 1$. Finally, since $|-n| = |-1| \cdot |n| = |n|$ we obtain that $|\ | = |\ |_\infty^r$.

In the sequel we also assume that the valuation is non-archimedean, and so $|\mathbb{Z}| \le 1$. Let I be the set of integers such that $|n| < 1$. It follows from the strong triangle inequality that I is an ideal, and using the multiplicativity of $|\ |$ we even obtain that I is prime. If $I = 0$, then $|\ | = |\ |_0$, so it remains to consider the case when $I = (p)$. By our assumptions $0 < |p| < 1$, hence there exists $r \in (0, \infty)$ with $|p| = p^{-r}$. We claim that $|\ | = |\ |_p^r$. Indeed, if $n = p^l a$ with $a \in \mathbb{Z} \setminus I$, then $|a| = 1$ by the definition of I, and hence $|n| = |p^l| = p^{-rl}$, as required.

We have shown that in any case $|\ |$ belongs to the list. Finally, any semivaluation $|\ |_\mathbb{Q}$ on $\mathbb{Q}$ is a valuation because $\mathbb{Q}$ has no non-zero ideals. Hence the restriction $|\ |$ of $|\ |_\mathbb{Q}$ onto $\mathbb{Z}$ is of the form (0)–(2), and $|\ |_\mathbb{Q}$ is determined by $|\ |$ by the multiplicativity. $\square$

1.3. **Completions.**

1.3.1. *Metric completion.* Any seminorm on a ring A defines a translation invariant semimetric $d(x, y) = |x - y|$ on A. The *completion* $\widehat{A}$ of A with respect to d, also called sometimes *separated completion*, is the set of equivalence classes of Cauchy sequences $(x_n)_{n \in \mathbb{N}}$. Recall that (x_n) is Cauchy if $\lim_{m,n\to\infty} d(x_m, x_n) = 0$ and sequences $(x_n), (y_n)$ are equivalent if $\lim_{n\to\infty} d(x_n, y_n) = 0$. Sending $a \i A$ to the constant sequence defines a completion map $A \to \widehat{A}$. Setting $d((x_n), (y_n)) = \lim_n d(x_n, y_n)$ makes $\widehat{A}$ a complete metric space, that is, the one for which the completion is a bijection.

Exercise 1.3.2. (i) Check that indeed $\widehat{A} = \widehat{\widehat{A}}$.

(ii) Show that the completion map factors as $A \to A/\mathrm{Ker}(|\ |) \hookrightarrow \widehat{A}$, where the embedding $A/\mathrm{Ker}(|\ |) \hookrightarrow \widehat{A}$ is the completion map of the ring $A/\mathrm{Ker}((\ |))$ with the quotient norm. In particular, the completion is injective if and only $|\ |$ is a norm.

1.3.3. *Operations.* One can also extend the arithmetic operations to $\widehat{A}$ either by continuity or just by setting $(x_n) + (y_n) = (x_n + y_n)$ and $(x_n) + (y_n) = (x_n + y_n)$ and checking that this definition is independent of the choice of the representatives (x_n), (y_n) of elements $x, y \in \widehat{A}$. In addition, if F is a normed field, then $\widehat{F}$ is a field because for any $a \neq 0$ in $\widehat{F}$ only finitely many elements of it representatives are not zero, and removing them we find a representative (a_n) with $a_n \in F^\times$. Then $(a_n^{-1}) = (a_n)^{-1}$ in $\widehat{F}$.

1.3.4. *Examples.* The trivial case: the trivial norm $|\ |_0$ defines trivial trivial completion $A = \widehat{A}$ and the induced topology is discrete. In the same fashion, $\mathbb{F}_p$ is the completion of $\mathbb{Z}$ with respect to $|\ |_p^\infty$.

The archimedean case: $(\mathbb{R}, |\ |_\infty^r)$ is the completion $(\mathbb{Q}, |\ |_\infty^r)$, hence also of any subfield provided with the induced norm. Similarly, $(\mathbb{C}, |\ |_\infty^r)$ is the completion of any its non-real subfield. The topologies are the usual one and do not depend on r.

The p-adic case: the completion of $\mathbb{Q}$ with respect to $|\ |_p^r$ is called the field of *p-adic numbers* and is denoted $\mathbb{Q}_p$. Again, the topology and the field are independent of r. The subring $\mathbb{Z}_p$ of *integral p-adic numbers* is defined as the completion of $(\mathbb{Z}, |\ |_p^r)$.

The power series case: the completion of $k(t)$ with respect to the t-adic valuation is the field $k((t))$ of *Lauernet series* over k. Again, the completion of $k[t]$ defines the subring of integers $k[[t]]$, which is the ring of formal power series over k.

Exercise 1.3.5. (i) Prove that $\mathbb{Z}_p$ and $k[[t]]$ are the closed unit balls with center at 0.

(ii) Prove that any p-adic number possesses a unique base-p presentation $a = \sum_{n=n_0}^\infty a_n p^n$ with $n_0 \in \mathbb{Z}$ and $a_n \in \{0, 1, \dots, p-1\}$. What is the presentation of -1 in $\mathbb{Q}_2$?

(iii) Prove that a p-adic number is in $\mathbb{Q}$ if and only if its coefficients a_n are periodic for large enough n.

1.3.6. *Analytic fields.* By an *analytic field*[1] we mean a complete real valued field. These are fields suited for developing analysis via convergent power series. In particular, one might study classical series in different fields and compare their radii of convergence. Often this carries a valuable information about algebraic or algebra-differential properties of the fields.

Remark 1.3.7. On the computational side, the non-archimedean analysis is usually simpler. For example, a series $\sum a_n$ converges if and only if $|a_n|$ tend to 0. In particular, there is no distinction between absolute and conditional convergence.

Exercise 1.3.8. (i) For a series $f(x) = \sum_{n=0}^\infty a_n x^n$ define the radius of convergence $r_{\mathrm{conv}}(f) = (\liminf_n |a_n|^{1/n})^{-1}$. Show that the series converges whenever $|x| < r_{\mathrm{conv}}(f)$ and does not converge whenever $|x| > r_{\mathrm{conv}}(f)$.

(ii) Show that the binomial series $(1+x)^{1/p} = \sum_{n=0}^\infty \binom{1/p}{n} x^n$ with a prime p has radius of convergence 1 in $\mathbb{Q}_l$ with $l \neq p$ and radius of convergence $|p|^{\frac{p}{p-1}}$ in $\mathbb{Q}_p$.

[1] This notion is not common in the literature.

(As we will later see, this is related to wild ramification phenomena.) Check that in these cases the series does not converge when $|x| = r_{\rm conv}$.

(iii) Compute the radii of convergence of $\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$ and $\log(1+x) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}x^n}{n}$ in $\mathbb{Q}_p$.

1.3.9. *Completed residue field.* Lemma 1.2.9 easily implies the following analytic version:

Lemma 1.3.10. *For a ring A there is a natural bijection between real semivaluations on A and equivalence classes of homomorphism from A to analytic fields. The minimal representative of the class corresponding to $|\ |$ is the homomorphism from A to the completion of* $\mathrm{Frac}(A/\mathrm{Ker}(|\ |))$.

1.4. **Analytic spectrum and geometry of valuations.**

1.4.1. *The spectrum.* By *spectrum* or *analytic spectrum* $X = \mathcal{M}(\mathcal{A})$ of a seminormed ring $\mathcal{A} = (A, |\ |)$ we mean the set of all bounded real semivaluations on $\mathcal{A}$. We prefer to think about elements of the spectrum geometrically, so we call them *points* of X and denote by letters x, y, etc. The seminorms will be also denoted $|\ |_x, |\ |_y$, etc. In addition, X possesses a natural topology whose bases is formed by the sets $\{x \in X |\ r_1 < |f|_x < r_2\}$ with $f \in A$ and $r_i \in \mathbb{R}$. This is the weakest topology in which all functions $|f| \colon X \to \mathbb{R}$ are continuous.

Remark 1.4.2. (i) Analytic spectrum of Berkovich spectrum was introduced by Vladimir Berkovich in [Ber90, Chapter 1], and it serves as a building block of analytic geometry (also referred to as Berkovich geometry), which can be studied both over both archimedean and non-archimedean real valued fields, and even over $\mathbb{Z}$. In the book one considers Banach $\mathcal{A}$ (that is normed and complete), but this does not really restricts the generality as $\mathcal{M}(\mathcal{A}) = \mathcal{M}(\widehat{\mathcal{A}})$. In particular, Berkovich proves that $\mathcal{M}(\widehat{\mathcal{A}})$ is compact.

(ii) A far predecessor of this definition is the famous theorem of Gel'fand-Naymark that spectrum of C^* algebras defines an anti-equivalence between the categories of C^* algebras and compact topological spaces. To some extent this theorem motivated later definition of spectrum of rings in algebraic geometry.

1.4.3. *Completed residue fields.* For any point $|\ |_x$ of X we define the *completed residue field* $\mathcal{H}(x)$ as the completion of the real valued field $\mathrm{Frac}(\mathcal{A}/\mathrm{Ker}(|\ |))$, and denote the corresponding bounded homomorphism by $\chi_x \colon \mathcal{A} \to \mathcal{H}(x)$. BY Lemma 1.3.10 we obtain

Lemma 1.4.4. *For any seminormed ring $\mathcal{A}$ the spectrum $\mathcal{M}(\mathcal{A})$ is naturally bijective to the set of equivalence classes of bounded homomorphisms of A to analytic fields, and χ_x is the minimal representative of the class corresponding to $|\ |_x$.*

1.4.5. *First examples.* In fact, Ostrowski's theorem gives a precise description of the set $\mathcal{M}(\mathbb{Z}, |\ |_\infty)$. The domination of valuations turns it into an ordered tree with the root $|\ |_\infty$ and leaves $|\ |_p^\infty$. The completed residue field is as follows: (0) $\mathbb{Q}$ at $|\ |_0$, (1) $\mathbb{R}$ at $|\ |_\infty^r$, (2) $\mathbb{Q}_p$ at $|\ |_p$ and its finite powers, (3) $\mathbb{F}_p$ at $|\ |_p^\infty$.

Exercise 1.4.6. (i) Describe the topology on $\mathcal{M}(\mathbb{Z}, |\ |_\infty)$. For example, describe the set $0.5 < |57| < 3$.

(ii) Obtain a similar description for $E_k(r) = \mathcal{M}(k[t], |\ |_{t,r})$, where k is an algebraically closed field, $r > 1$ and $|f(t)|_{t,r} = r^{\deg(f)}$.

Remark 1.4.7. In fact, $E_k(r)$ is a Berkovich analytic closed disc of radius r over the trivially valued field k. Already here we observe the non-archimedean phenomenon that closed discs over the analytic field k contain "non-classical" points not corresponding to elements of k. This happens because, unlike the archimedean case, the valuation can be extended (and in many ways) to $k(t)$.

1.4.8. *Non-archimedean affine line.* More generally, we define closed Berkovich disc of radius r over an analytic field k as $E_k(r) = \mathcal{M}(k[t]_r)$, where $k[t]_r$ is the polynomial ring provided with the generalized Gauss norm $|\ |_r$. If $s \le r$ then $|\ |_s \le |\ |_r$ and we obtain a natural embedding $E_k(s) \subseteq E_k(r)$. The union $\mathbb{A}^1_k = \cup_r E_k(r)$ is called *Berkovich affine line* over k.

Exercise 1.4.9. (i) Show that $\mathbb{A}^1_k$ is the set of all real semivaluations on $k[t]$ extending the valuation of k and $E_k(r)$ is the set of all real semivaluations $|\ |$ such that $|t| \le r$.

(ii) Show that $E_k(r)$ only depends on the completion $\widehat{k}$. Moreover, it is actually the spectrum of the completion $\widehat{k}\{t\}_r$ of $k[t]_r$. Show that $\widehat{k}\{t\}_r$ consists of all series $\sum_{i=0}^{\infty} a_i t^i$ such that $\lim_i r^i|a_i| = 0$.

1.4.10. *Monomial points of* $\mathbb{A}^1_k$. A point $x \in \mathbb{A}^1_k$ and the corresponding real semivaluation $|\ |_x$ are called *monomial* if $|\ |_x$ is the generalized Gauss valuation for an appropriate coordinate $t-a$. Geometrically x is obtained from a generalized Gauss point by translating by $a \in k$. We will use the notation $|\sum_i a_i(t-a)^i|_{a,r} = \max_i r^i|a_i|$. It follows from the strong triangle inequality that $|\ |_{a,r} = |\ |_{b,s}$ if and only if $|a-b| \le r = s$. Thus, the structure of the set M of monomial points is as follows: M is covered by rays $R_a = \{|\ |_{a,r}\}$ with $r \ge 0$ and two rays R_a and R_b collide for $r \ge |a-b|$.

1.4.11. *Classification of points on* $\mathbb{A}^1_k$. Monomial points are divided to 3 types as follows: (1) $r = 0$, (2) $r \in |k^\times|$, (3) $r \notin |k|$. Geometrically, $\mathbb{A}^1_k$ is a huge tree and points of type 1 are leaves, points of type 2 are vertices, and points of type 3 lie inside the edges. Moreover, one can safely identify points of type 1 with the elements of k. They are often called classical or rigid points. We will see that there is just one more (nasty) type of points, which are also leaves. We will call them points of type 4.

Theorem 1.4.12. *Assume that k is an algebraically closed real valued field and $x \in \mathbb{A}^1_k$ is a point with the corresponding real semivaluation $|\ |$ on $k[t]$. Let $r = \inf_{a\in k} |t-a|$, then*

(i) The point x is monomial if and only if the infimum is achieved. Furthermore, if $r = |t-a|$ for some $a \in k$, then $|\ | = |\ |_{a,r}$.

(ii) The point x is of type 4 if and only if the infimum is not achieved. Furthermore, if in this case a_i are such that the sequence $r_i = |t-a_i|$ monotonically decreases and tends to r, then $E_k(a_i, r_i)$ is a nested sequence of discs and $\{x\} = \cap_i E_k(a_i, r_i)$. In particular, this intersection contains no elements of k in the intersection.

In addition, $\mathbb{A}^1_k$ contains a point of type 4 if and only if there exists a family of nested discs $\mathcal{E} = \{E_k(a_i, r_i)\}_i$ whose intersection contains no elements of k.

Proof. Any polynomial splits to linear factors, hence $|\ |$ is determined by the values of $|t-a|$. If the infimum is achieved, say $r = |t-a|$, then $|t-b| \le \max(r, |a-b|)$

hence $|t-b| = r$ whenever $|a-b| \le r$. If $|a-b| > r$, the strong triangle inequality implies that $|t-b| = |a-b|$. This proves that $|\ |$ and $|\ |_{a,r}$ coincide on linear factors, and hence they are equal.

If the infimum is not achieved then the valuation is obviously non-monomial. Furthermore, there is no element $a \in k$ in the intersection because otherwise $|a-t| \le r_i$ for any i and hence $|a-t| \le r$. Furthermore, $|\ |$ is dominated by the real valued function $|\ |_{\mathcal{E}} = \inf_i(|\ |_{a_i,r_i})$, which is clearly multiplicative. This implies that necessarily $|\ | = |\ |_{\mathcal{E}}$. Finally, any nested family of discs $\mathcal{E}$ induces a semivaluation $|\ |_{\mathcal{E}}$ as above, and it is easy to see that this semivaluation is not monomial if and only if the intersection does not contain classical points. $\square$

Remark 1.4.13. If k is not algebraically closed, then the most natural approach is to factor elements of $k[t]$ in $\overline{k}[t]$. This leads to a description of $\mathbb{A}^1_k$ in terms of $\mathbb{A}^1_{\overline{k}}$, but one has to develop the theory of extension of valuations first. Once this will have been done, we will show that $\mathbb{A}^1_k = \mathbb{A}^1_{\widehat{k}}/\mathrm{Gal}(k^s/k)$ for an analytic k.

1.4.14. *Existence of points of type 4.* We say that $r = \inf_{a\in k}|t-a|_x$ is the radius of x with respect to the coordinate t on $\mathbb{A}^1_k$. Points of type 4 and radius 0 correspond to intersections of discs of radii tending to 0. Clearly, such points exist if and only if k is not complete. Furthermore, k is called *spherically complete* if there exists no points of type 4 over k.

Remark 1.4.15. (i) We will later see that an algebraically closed k is not spherically complete in all "reasonably small" non-trivially valued cases. This might look surprising, but unless k is locally compact, there is no "good reason" why nested families of discs should have a common element in k.

(ii) We will see that any valued field can be embedded into a spherically complete one, but this uses Zorn's lemma, and there is no natural construction in general.

(iii) We will later show that Berkovich affine line is locally compact. Intuitively, adding points of type 4 to the set of monomial semivaluations is the most natural way to achieve this property.

1.4.16. *The archimedean case.* One can develop a similar archimedean theory using norms (but not valuations) $|\sum_i a_i t^i|_r = \sum_i r^i|a_i|$. However, as we will show below in this case one does not obtain anything new because there exist only classical points and hence $\mathbb{A}^1_{\mathbb{C}} = \mathbb{C}$. Similarly, $\mathbb{A}^1_{\mathbb{R}}$ is the quotient of $\mathbb{C}$ by the complex conjugation.

1.5. **Classification of archimedean valuations.** After some preparations we will show that any archimedean semivaluation is induced from a homomorphism to $\mathbb{C}$. Naturally, this reduces to showing that one cannot extend the archimedean valuation to $\mathbb{R}(x)$, and for this it suffices to show that any semivaluation on $\mathbb{R}[x]$ has a non-trivial kernel.

1.5.1. *Semivaluations on* $\mathbb{C}[t]$. We start with studying the situation on $\mathbb{C}[t]$. The basic idea is the same as in the non-archimedean case: find the center of a semivaluation, that is, find a which minimizes $|t-a|$.

Lemma 1.5.2. *Any archimedean semivaluation $|\ |$ on $\mathbb{C}[t]$ has a non-trivial kernel.*

Proof. By Ostrowski's theorem there exists $r \in (0,1]$ such that $|a| = |a|_\infty^r$ for any $a \in \mathbb{C}$. Define a real-valued function on $\mathbb{C}$ by $f(a) = |t-a|$. Then $|f(a) - f(b)| \le$

$|a-b| \le |a-b|_\infty$ and hence f is continuous in the usual topology (even Lipschitz). Since $f(0) = |t|$ and $f(a) \ge |a| - |t|$, the function f attains a global maximum for some a_0 inside the disc given by $|a| \le 2|t|$. Replacing t by $t - a_0$ we can assume that $|t| \le |t-a|$ for any $a \in \mathbb{C}$. We claim that $|t| = 0$, and so $\mathrm{Ker}(|\ |) = (t)$.

If $|t| > 0$, then replacing t by ct with $c = |t|^{-1}$ we can assume that $|t| = 1$. Any monic polynomial $f(t)$ is a product of linear monic factors, hence $|f| \ge 1$. In addition, if $a \in \mathbb{C}$ is a root of f, then $f = (t-a)g$ and $|f| \ge |t-a| \cdot |g| \ge |t-a|$. In particular, $|t-a| \le |t^n - a^n| \le 1 + |a|^n$ for any $a \in \mathbb{C}$ and $n \in \mathbb{N}$. If $|a| < 1$ then tending n to infinity we obtain that $|t-a| = 1$. Since we can replace t by $t-a$, we have actually proved that if $|t-a| = 1$ then $|t-b| = 1$ for any $b \in \mathbb{C}$ such that $|a-b| < 1$. Therefore, $|t-a| = 1$ for any $a \in \mathbb{C}$, while the triangle inequality implies that $|t-a|$ tends to infinity as $|a|$ tends to infinity. The contradiction concludes the proof. □

1.5.3. *Semivaluations on* $\mathbb{R}[t]$. Probably, the most natural way to extend this result to $\mathbb{R}[t]$ is by extending the semivaluation, but the following more technical approach is faster. The idea is to just extend the above argument to irreducible quadratic polynomials.

Lemma 1.5.4. *Any archimedean semivaluation* $|\ |$ *on* $\mathbb{R}[t]$ *has a non-trivial kernel.*

Proof. As in the proof of Lemma 1.5.2, $|t-a|$ attains its minimum C on $\mathbb{R}$, and we can assume that $C > 0$. Setting $|t| = r$ we have that $|t^2 + at + b| \ge |at + b| - |t^2| \ge C|a| - r^2$ and $|t^2 + at + b| \ge |b| - r^2 - r|a|$. It follows that $|t^2 + at + b|$ tends to infinity when $|a| + |b|$ tends to infinity, and hence attains its minimum C_2 on a polynomial $t^2 + a_0 t + b_0$. Setting $c = \max(C^{-1}, C_2^{-1/2})$ and replacing t by ct we achieve that $|f| \ge 1$ for monic polynomials of degree 1 and 2, and there exists such an f_0 with $|f_0| = 1$. Since any monic polynomial g is a product of linear and quadratic ones, this also implies that $|g| \ge 1$.

Now, if f_0 is linear, then the same argument as in Lemma 1.5.2 concludes the proof. So, assume that $|t-a| > 1$ for any $a \in \mathbb{R}$. In particular, $|f| > 1$ for quadratic reducible polynomials, and hence f_0 is quadratic irreducible. By a linear change of coordinate we can assume that $f_0 = t^2 + b^2$. We claim that in this case $|t^2 + (b+c)^2| = 1$ for any $c \in \mathbb{R}$ with $|c| < 1$. Proving this will conclude the proof because using this iteratively one obtains that $|t| = 1$, yielding a contradiction. Note that $(b+c)i$ is a root of the complex polynomial $h(t) = (t - bi)^n - (ci)^n$, hence the real monic polynomial $h\overline{h}$ is divisible by $t^2 + (b+c)^2$ and we obtain that $|h\overline{h}| \ge |t^2 + (b+c)^2|$. Expanding the expression for $h\overline{h}$ one obtains that $h\overline{h} = (t^2+b^2)^n + 2c^n\phi(t) + c^{2n}$ for a monic polynomial $\phi(t)$. In particular, $|h\overline{h}| \le 1 + |2c^n| + |c^{2n}|$ and tending n to infinity we obtain that $|t^2 + (b+c)^2| \le 1$, as required. □

We preferred the above argument because we do not know a too simple proof that valuations can be extended. In these notes, the archimedean case will just follow from the classification, and in the non-archimedean one we will use valuation rings and an algebraic technique.

Exercise 1.5.5. Trying to find a simple proof of the fact that any semivaluation $|\ |$ on $\mathbb{R}[x]$ extends to a semivaluation $|\ |_\mathbb{C}$ on $\mathbb{C}[x]$ we came up with the following wrong argument. Find the mistake: the function $|\ |_\mathbb{C} := |f\overline{f}|^{1/2}$, where $\overline{f}$ is the complex conjugate, is multiplicative. So, we should only prove that $|f+g|_\mathbb{C} \le |f|_\mathbb{C} + |g|_\mathbb{C}$, that is, $|N(f)+N(g)+f\overline{g}+\overline{f}g|^{1/2}\le |N(f)|^{1/2}+|N(g)|^{1/2}$. Taking squares we obtain that this is equivalent to

$$|N(f)+N(g)+f\overline{g}+\overline{f}g|\le |N(f)|+|N(g)|+2|N(f)N(g)|^{1/2},$$

and the latter follows from the observation that

$$|f\overline{g}+\overline{f}g|\le |g\overline{f}|+|\overline{f}g|=2|N(f)N(g)|^{1/2}.$$

Remark 1.5.6. In fact, the same argument would imply that the complex valuation on $k=\mathbb{Q}[\sqrt{-2}]$ extends to $K=\mathbb{Q}[\sqrt{-2},i]$ by the same formula. The latter is wrong because although a^2+b^2 has no non-trivial zeros in k, it can be arbitrarily small with respect to $\min(|a|,|b|)$. This is also related to the facts that K embeds into $\widehat{k}$ and there are two extensions of the valuation to K corresponding to the conjugate embeddings of K into $\widehat{k}$. We will later see the same phenomenons in the non-archimedean situation.

1.5.7. *Second Ostrowski's theorem.* Now we can finally classify all archimedean valuations.

Theorem 1.5.8. *(i) $\mathbb{R}$ and $\mathbb{C}$ are the only complete archimedean real valued fields, and the valuation is of the form $|\ |_\infty^r$.*

(ii) Any archimedean semivaluation $|\ |$ on a ring A is induced from $|\ |_\infty^r$ via a homomorphism $i\colon A\to\mathbb{C}$, and $|\ |$ is a valuation if and only if i is an embedding.

Proof. Part (ii) follows from (i) via Lemma 1.4.4. To prove (i) assume that K is a complete archimedean field. By Ostrowski's theorem, K contains $\mathbb{R}$ and the valuation on $\mathbb{R}$ is $|\ |_\infty^r$. By Lemma 1.5.4, K does not contain transcendental extensions of $\mathbb{R}$, hence either $K=\mathbb{R}$ or $K=\mathbb{C}$. In the second case, we should also check that if a valuation $|\ |$ on $\mathbb{C}$ extends $|\ |_\infty^r$ on $\mathbb{R}$, then $|\ |=|\ |_\infty^r$. It suffices to prove that $|a|=|\overline{a}|$ for any $a\in\mathbb{C}$, since then $|a|=|a\overline{a}|_\infty^{r/2}=|a|_\infty^r$. Moreover, it suffices to deal with the case when $|a|=1$. By compactness of the unit circle $S=e^{2\pi i\mathbb{R}}$, the function $f(a)=|x/\overline{x}|$ attains its maximum at some $a\in S$. If $f(a)>1$, then $f(a^2)=f(a)^2>f(a)$, which is impossible. So $f(a)\le 1$, and in the same way $f(a)\ge 1$. □

Remark 1.5.9. A stronger and somewhat more famous theorem of Gel'fand-Mazur states that any normed $\mathbb{C}$-algebra which is a field coincides with $\mathbb{C}$. In fact, Stanisław Mazur even proved that $\mathbb{R}$, $\mathbb{C}$ and the quaternions $\mathbb{H}$ are the only normed (not necessarily commutative) division $\mathbb{R}$-algebras. One proof can be found in [Bou72, VI.6.4]: unlike the case of valued fields we have studied, analysis of complete normed fields easily reduces to normed fields over $\mathbb{C}$. As in our argument, this case is done by studying $\min_a|t-a|$, but the argument requires more care. We will later deduce classification of normed fields from the second Ostrowski's theorem and Berkovich's theorem on analytic spectra.

1.5.10. *Archimedean affine lines.* As a corollary we now obtain the expected description of archimedean affine lines.

Corollary 1.5.11. *One has that $\mathbb{A}^1_{\mathbb{C}}=\mathbb{C}$ and $\mathbb{A}^1_{\mathbb{R}}=\mathbb{C}/\sigma$, where σ is the complex conjugation.*

Proof. These are precisely the isomorphism classes of homomorphisms $\mathbb{C}[x]\to\mathbb{C}$ and $\mathbb{R}[x]\to\mathbb{C}$. □

1.6. **Hensel's lemma.**

1.6.1. *Reduction of seminormed rings.* If A is a non-archimedean seminormed ring, then the closed unit ball $A^\circ := \{a \in A|\ |a| \le 1\}$ is a subring and the open unit ball $A^{\circ\circ} := \{a \in A|\ |a| < 1\}$ is an ideal in A°. The quotient $\widetilde{A} := A^\circ/A^{\circ\circ}$ is called the *reduction* of A. If k is a field then $\widetilde{k}$ is a field, called the *residue field* of k. The image of $a \in A^\circ$ in $\widetilde{A}$ is called the *reduction* of a and denoted $\widetilde{a}$.

Exercise 1.6.2. (i) Check that, indeed, if k is a field, then $\widetilde{k}$ is a field.

(ii) Show that the seminorm on A is multiplicative (resp. power-multiplicative) if and only if $\widetilde{A}$ is a domain (resp. a reduced ring).

1.6.3. *Residue field and group of values.* For any real-valued field k the *group of values* $|k^\times| \subseteq \mathbf{R}^\times_{>0}$ and the residue field $\widetilde{k}$ are the two most important invariants of k. The ring k° is often called the *ring of integers* of k. One says that k is of *equal characteristic* if $\mathrm{char}(k) = \mathrm{char}(\widetilde{k})$, for example, this is the case with $k((t))$. Otherwise, $\mathrm{char}(k) = 0$, $\mathrm{char}(\widetilde{k}) = p > 0$ and one says that k is of *mixed characteristic*. Characteristics divide non-archimedean fields into three classes. We will later see that the Galois theory in the equal characteristic zero case is relatively simple, while it is very complicated and of comparable difficulty in the two cases of residual characteristic zero.

1.6.4. *Hensel's lemma.* In the following result we provide $K[t]$ with the Gauss valuation. In particular, $(K[t])^\circ = K^\circ[t]$ and the reduction of a polynomial $\sum_i a_i t^i \in K^\circ[t]$ is simply $\sum \widetilde{a}_i \widetilde{t}^i$. Here is an extremely important and famous result going back to Hensel (in the p-adic case), Kürschák and Ostrowski. We start with a general version and then deduce corollaries, including those that are often also referred to as Hensel's lemma.

Theorem 1.6.5. *Let K be an analytic non-archimedean field and let $f(t) \in K^\circ[t]$ be a polynomial over K whose coefficients are integral. Then any factorization $\widetilde{f} = \overline{g}\overline{h}$ of the reduction $\widetilde{f} \in \widetilde{K}[\widetilde{t}]$ with $(\overline{g}, \overline{h}) = 1$ lifts to a factorization $f = gh$ in $K^\circ[t]$ such that $\widetilde{g} = \overline{g}$ and $\deg(g) = \deg(\widetilde{g})$. In addition, if $\overline{g}$ is monic, then one can take g to be monic.*

Proof. Let $n = \deg(f)$, $m = \deg(\overline{g})$ and $l = \deg(\overline{h})$, in particular, $n \ge l + m$. The additional claim is obvious: if $f = gh$ are as in the formulation and $\overline{g}$ is monic, then $g = at^m + \dots$ with $\widetilde{a} = 1$ and the decomposition $f = (a^{-1}g)(ah)$ is as required. Let us prove the main claim. It is common in the theory of complete fields to solve problems by successive approximations. In "ramified" problems one has to start with a good enough approximation, but in the simplest cases like ours, any initial approximation works well. So choose any lifts $g_0, h_0 \in K^\circ[t]$ of $\overline{g}$ and $\overline{h}$ of degrees m and l, respectively.

First, we claim that there exist $r < 1$ such that for any polynomial $\phi(t) \in K[t]$ with $\deg(\phi) \le n$ there exist $u, v \in K[t]$ with $|u| \le |\phi|$, $|v| \le |\phi|$, $\deg(v) < m$, $\deg(u) \le n - m$ and such that the inequality $|\phi - ug_0 - vh_0| \le r|\phi|$ holds. Indeed, since $(\overline{g}, \overline{h}) = 1$, for any natural i there exists a decomposition $\widetilde{t}^i = \overline{u}_i\overline{g} + \overline{v}_i\overline{h}$ in $\widetilde{K}[\widetilde{t}]$ such that $\deg(\overline{v}_i) < m$, and hence for $i \le n$ one also has that

$$\deg(\overline{u}_i) \le \max(i, l + m - 1) - m \le n - m.$$

Taking lifts $u_i, v_i \in K^\circ[t]$ with $\deg(u_i) = \deg(\overline{u}_i)$, $\deg(v_i) = \deg(\overline{v}_i)$ we obtain that $r_i := |t^i - u_i g_0 - v_i h_0| < 1$ and then $r = \max_{i \le n}(r_i)$ is as required, since for $\phi(t) = \sum_{i=0}^n a_i t^i$ one can take $u = \sum_{i=0}^n a_i u_i$ and $v = \sum_{i=0}^n a_i v_i$. Furthermore, the same claim holds for any $g', h' \in K[t]$ such that $|g' - g_0| \le r$ and $|h' - h_0| \le r$ because one can choose the same u, v as for g_0, h_0.

Now, let us deduce the theorem from the claim. The polynomial $\phi_0 = f - g_0 h_0$ satisfies $|\phi_0| < 1$, hence enlarging r we can assume that $|\phi_0| < r < 1$. Using the above claim we inductively choose $u_d, v_d \in K[t]$ such that $|\phi_d - u_d g_d - v_d h_d| \le r|\phi_d|$, and set $g_{d+1} = g_d + v_d$, $h_{d+1} = h_d + u_d$ and $\phi_{d+1} = f - g_{d+1}h_{d+1}$. Then

$$|\phi_{d+1}| = |(\phi_d - u_d g_d - v_d h_d) - u_d v_d \phi_d^2|$$

and by induction on d we obtain that $|u_d| < r^d$, $|v_d| < r^d$ (in particular, $|g_d - g_0| < r$ and $|h_d - h_0| < r$, and the claim applies to g_d, h_d) and $|\phi_{d+1}| < r^{d+1}$. Moreover, since $\deg(v_d) < m$ and $\deg(u_d) \le n - m$, the series $g_0 + v_0 + v_1 + \dots$ and $h_0 + u_0 + u_1 + \dots$ converge to polynomials g and h of degrees at most m and $n - m$, and we have that $f - gh = \lim \phi_d = 0$. It remains to note that $|g - g_0| < r$ and $|h - h_0| < r$, hence the reductions $\widetilde{g} = \widetilde{g}_0 = \overline{g}$ and $\widetilde{h} = \widetilde{h}_0 = \overline{h}$ are as required. □

Remark 1.6.6. The case when the valuation is discrete, is slightly easier because one should only worry for iterative approximations modulo (π^n), where $K^{\circ\circ} = (\pi)$. We will illustrate this in Exercise 1.6.14 below. In our proof, we had to care that the approximation will be improved by a fixed factor $r < 1$, and the choice of this r required some care.

1.6.7. *Corollaries.* Now, let us work out corollaries and particular case of general Hensel's lemma. Taking $\overline{g} = \widetilde{f}$ and $\overline{h} = 1$ we obtain

Corollary 1.6.8. *If K is an analytic non-archimedean field, then any polynomial $f \in K^\circ[t]$ splits in $K^\circ[t]$ as $f = gh$, where $|h - 1| < 1$ and $\deg(g) = \deg(\widetilde{g})$.*

Remark 1.6.9. (i) Based on this corollary we will easily show in the sequel that the valuation of K extends to the algebraic closure K^a. This allows the following geometric interpretation of this result. If $|a| \le 1$ then $|h(a)| = 1$, in particular, all roots of h satisfy $|a| > 1$. On the other side, $g(t) = a_n t^n + \dots$ with $|a_n| = 1$, and it follows easily that all roots of g satisfy $|a| \le 1$. So this factorization simply separates roots of f in the unit disc $E_k(1)$ from the roots in its complement (which can also be viewed as an open disc around infinity). This also indicates that h should be invertible on $E_k(1)$, and indeed $h^{-1} = \sum_i (1-h)^i$ in $\widehat{K[T]}$. Finally, it is worth to note that this splitting is actually an instance of the Weierstrass division theorem for functions on the unit disc.

(ii) Even more generally, the geometric meaning of Hensel's lemma is that the separation of roots of $f \in K^\circ[t]$ by irreducible factors (or by conjugation over K) is finer than the separation to open discs of radius one. Indeed, assume for simplicity that $\widetilde{f} = \prod_i \overline{g}_i$ with $\overline{g}_i = (\widetilde{t} - \widetilde{a}_i)^{n_i}$ and distinct $\widetilde{a}_i$, for example, this happens when $\widetilde{K}$ is algebraically closed. By Hensel's lemma the factorization lifts to $f = h \prod_i g_i$ with monic g_i of degrees n_i, and it is easy to see that all roots of g_i are contained in the open disc around a_i of radius 1.

Another immediate corollary is obtained by restricting to the case of monic polynomials, because in this case the degree is preserved under reduction.

Corollary 1.6.10. *If K is an analytic non-archimedean field and $f(t) \in K^\circ[t]$ is monic, then any factorization $\widetilde{f} = \overline{g}\overline{h}$ in $\widetilde{K}[\widetilde{t}]$ with monic and co-prime $\overline{g}$ and $\overline{h}$ lifts to a factorization $f = gh$ in $K^\circ[t]$ with monic g, h.*

Remark 1.6.11. This monic version of Hensel's lemma is more usual. Our more general variant is equivalent to the combination of the monic version and the Weierstrass division. This formulation of the non-monic version (with a different proof) can be found, for example, in [BGR84, Proposition 3.3.4/3].

Perhaps here is the most classical (and basic) version of Hensel's lemma, which claims that simple roots of the reduction polynomial lift to K uniquely.

Corollary 1.6.12. *If K is an analytic non-archimedean field, $f(t) \in K^\circ[t]$ is a polynomial with integral coefficients and $\overline{a}$ is a simple root of the reduction $\widetilde{f}(\widetilde{t})$, then there exists precisely one root a of f such that $|a| \leq 1$ and $\widetilde{a} = \overline{a}$.*

Proof. By our assumption $\widetilde{f} = (x - \overline{a})\overline{h}$, and $\overline{a}$ is not a root of $\overline{h}$. By Theorem 1.6.5, we obtain a factorization $f = (x-a)h$, with $\widetilde{a} = \overline{a}$, that is, a is a root of f which lifts $\widetilde{a}$. If there exists another lifting α, then $h(\alpha) = 0$ and hence $0 = \widetilde{h}(\widetilde{\alpha}) = \widetilde{h}(\overline{a})$, yielding a contradiction. □

Remark 1.6.13. The fact that there is a unique lifting explains why in our (and any other) proof of Hensel's lemma one can start with an arbitrary initial lifting a' of $\widetilde{a}$. If two liftings would exist (as happens in "ramified problems"), then one should have started with a good enough approximation which distinguishes one solution from the others.

Exercise 1.6.14. [2] For the sake of comparison and illustration let us work out a (technically) simpler proof in the case when K is discrete valued with uniformizer π and $\overline{a}$ is a simple root of $\widetilde{f}$. Complete details in the following argument: taking a lift $a_1 \in K^\circ$ of $\overline{a}$ we achieve that $|f(a_1)| < 1$. By induction, we assume that $|f(a_n)| \leq |\pi^n|$ and we should find $a_{n+1} = a_n - u_n$ such that $|u_n| \leq |\pi^n|$ and $|f(a_{n+1})| \leq |\pi^{n+1}|$. Using the Taylor expansion $f(a_n - u_n) = f(a_n) - f'(a_n)u_n + \dots$ it suffices to find $u_n \in \pi^n K^\circ$ such that $f(a_n) - f'(a_n)u_n \in \pi^{n+1}K^\circ$. Since $\widetilde{f}'(\overline{a}) \neq 0$ and $\widetilde{a}_n = \overline{a}$ by induction, we have that $|f'(a_n)| = 1$. So, we can simply take $u_n = \frac{f(a_n)}{f'(a_n)}$.

Remark 1.6.15. (i) Clearly, the above method is just the non-archimedean version of the classical Newton-Raphson method. In particular, its convergence is faster than what we showed – the mistake behaves as $|u_n^2|$, so one can essentially double n on each step.

(ii) Another interesting observation is that finding successive approximation allows to linearize problem – one just has to solve linear equations modulo π^n.

Finally, we will need the following very important corollary.

Corollary 1.6.16. *If K is an analytic non-archimedean field and $f(t) = t^d + a_1 t^{d-1} + \dots + a_d$ is an irreducible monic polynomial such that $a_d \in K^\circ$, then $f(t) \in K^\circ[t]$.*

---

[2] Should put this before the proof of Hensel's lemma and motivate the proof given where.

Proof. The corollary holds if and only if $r = \max_i |a_i| \le 1$. Assume that this is not the case, and take the minimal i such that $|a_i| = r$. Then the polynomial $g(t) = a_i^{-1} f(t)$ lies in $K^\circ[t]$ and its reduction is a monic polynomial of degree $i > 0$. By Corollary 1.6.8, $f(t) = u(t)h(t)$ with $\deg(h) = i$, which contradicts the irreducibility of f. $\square$

Remark 1.6.17. (i) The non-monic Hensel's lemma was essentially used in the proof.

(ii) This result was used already by Kürschák in 1913 to extend non-archimedean valuations to algebraic extensions, and we will use the same argument. In fact, Kürschák did not prove this claim, but remarked that it is proved as the analogous result in Hensel's book about p-adic numbers.

1.7. **Extensions of valuations for complete fields.**

1.7.1. *Normed vector spaces.* A *normed vector space* over a valued field k is a k-vector space V provided with a norm $\| \ \|$ such that $\|av\| = |a|\|v\|$ for any $a \in k$ and $v \in V$. Seminormed vector spacs are defined similarly. If k is non-archimedean, then we automatically consider only non-archimedean k-norms on V. Note that $\widehat{V}$ is a normed vector space over $\widehat{k}$.

A typical example is the L_∞-norm defined by the condition that there exists a basis $\{v_i\}$ such that $\|\sum_i a_i v_i\| = \max_i |a_i|\|v_i\|$ for any $a_i \in k$. Since we are mainly interested in the non-archimedean case, we will say that such a norm *Cartesian* and the basis $\{v_i\}$ is *orthogonal*. More generally, a basis is r-*orthogonal* for $r \in (0,1]$ if $\|\sum_i a_i v_i\| \ge r \max_i |a_i|\|v_i\|$.

Lemma 1.7.2. *If V is a finite dimensional vector space over a valued field k, then any k-norm on V is bounded by a Cartesian norm and any two Cartesian norms on V are equivalent. In addition, if $V = \mathrm{Span}_k(v_1, \dots, v_n)$, then $\widehat{V} = \mathrm{Span}_{\widehat{k}}(v_1, \dots, v_n)$.*

Proof. The boundedness is obvious since $\|\sum_{i=1}^n a_i v_i\| \le n \max_i |a_i|\|v_i\|$ for any choice of the basis. If $\| \ \|$ and $\| \ \|'$ are Cartesian norms corresponding to two bases and $A \in \mathrm{GL}_n(k)$ is the transition matrix between the bases, then it is easy to see that $\| \ \| \le C\| \ \|'$ for $C = \sum_{i,j=1}^n |a_{ij}|$. $\square$

In the finite-dimensional case, the dimension can only drop under completion.

Lemma 1.7.3. *If a finite dimensional normed vector space over a valued field k is spanned by a set $v_1, \dots, v_d$, then $\widehat{V}$ is spanned over $\widehat{k}$ by the same set. In particular, $\dim_k(V) \ge \dim_{\widehat{k}}(\widehat{V})$.*

Proof. Set $v = v_1$ and $U = \mathrm{Span}_k(v_2, \dots, v_d)$. We can assume by induction on $\dim(V)$ that $v_2, \dots, v_d$ span $\widehat{U}$, and it remains to prove that $\widehat{U} + \widehat{k}v = \widehat{V}$. If $v \in \widehat{U}$ this is obvious, hence we can assume that there exists $r > 0$ such that $\|v - u\| > r$ for any $u \in U$. It follows that $\|av + u\| \ge r|a|$ for any $a \in k$ and $u \in U$. Given an element $\widehat{v} \in \widehat{V}$ find a sequence w_i of elements of V converging to $\widehat{v}$. Writing $w_i = a_i v + u_i$ with $a_i \in k$, $u_i \in U$ we obtain from this inequality that (a_i) is a Cauchy sequence in k, and hence (u_i) is a Cauchy sequence in U. Taking the limits $\widehat{a} \in \widehat{k}$ and $\widehat{u} \in \widehat{U}$ we obtain that $\widehat{v} = \widehat{a}v + \widehat{u}$, as required. $\square$

A typical example of a norm non-equivalent to a Cartesian one is obtained as follows. Assume that k is not complete and choose $a \in \widehat{k} \setminus k$. Then $V = k \oplus ak$ embeds into $\widehat{k}$ and the induced norm is easily seen to be non-Cartesian. In addition, in this case the dimension drops under completion since $\widehat{V} = \widehat{k}$. The following important result provides useful criteria for a norm to be Cartesian and shows that the above is essentially the only mechanism for constructing norms non-equivalent to Cartesian ones.

Theorem 1.7.4. *Let V be a finite dimensional normed vector space over a valued field k. Then the following conditions are equivalent:*

(i) $\| \ \|$ is equivalent to a Cartesian norm.

(ii) V possesses an r-orthogonal basis for some $r \in (0, 1]$.

(iii) Any basis of V is r-orthogonal for some $r \in (0, 1]$.

(iv) The inequality $\dim_k(V) \geq \dim_{\widehat{k}}(\widehat{V})$ is an equality.

Proof. Let $b = \{v_i\}$ be a basis and let $\| \ \|_b$ be the Cartesian norm defined by b. Then automatically $\| \ \| \leq \| \ \|_b$, and an inequality $r\| \ \|_b \leq \| \ \|$ holds if and only if b is r-orthogonal with respect to $\| \ \|$. This proves that (i)$\Longleftrightarrow$(ii), and by Lemma 1.7.2, we also obtain that (i)$\Longleftrightarrow$(iii). It now suffices to prove that (iii)$\Longleftrightarrow$(iv).

Using induction on $d = \dim(V)$ we can assume that $d > 0$ and the theorem holds for smaller values of d. Set $v = v_1$ and $U = \mathrm{Span}_k(v_2, \dots, v_d)$. By induction, $\dim_{\widehat{k}}(\widehat{U}) < d - 1$ if and only if the basis $v_2, \dots, v_d$ of U is not r-orthogonal for any $r > 0$. Clearly, in this case $\dim_{\widehat{k}}(\widehat{V}) < d$ and b is not r-orthogonal for any $r > 0$. So, the equivalence holds in this case, and we can assume in the sequel that $\dim_{\widehat{k}}(\widehat{U}) = d - 1$, and hence also $v_2, \dots, v_d$ is r-orthogonal for some $r > 0$. In this case $\dim_{\widehat{k}}(\widehat{V}) < d$ if and only if $v \in \widehat{U}$. In the latter case, for any $s > 0$ there exist $a_2, \dots, a_d$ such that $\|v + a_2v_2 + \dots + a_dv_d\| < s$, and hence b is not s-orthogonal. Conversely, assume that b is not s-orthogonal for any $s \in (0, r)$. Choose a vector $x = a_1v_1 + \dots a_dv_d$ such that $\|x\| < s \max_i \|a_iv_i\|$. Since $v_2, \dots, v_d$ is r-orthogonal, this implies that $a_1 \neq 0$ and dividing by a_1 we can assume that $x = v + a_2v_2 + \dots$. Tending s to 0 we obtain a sequence $u_s \in U$ such that $\|v - u_s\| < s$. It follows that u_s is a Cauchy sequence in U and hence $v \in \widehat{U}$. □

As a corollary, we obtain the following important result, which is classical in the archimedean setting. Usually one proves the latter using local compactness, which is a stronger condition than completeness of k.

Corollary 1.7.5. *If V is a finite dimensional normed vector space over an analytic field k, then $V = \widehat{V}$ and the norm is equivalent to a Cartesian one.*

Proof. Since $V \to \widehat{V}$ is injective we obtain that $V = \widehat{V}$ by Lemma 1.7.3, and then the norm is equivalent to a Cartesian one by Theorem 1.7.4. □

1.7.6. *Extension of valuations.* Now we are going to use Hensel's lemma and uniqueness of norms to prove the following foundational result. As usually, by the norm $\mathcal{N}r(\alpha)$ of an element α algebraic over K we mean the product of all its conjugates with correct multiplicity in case of inseparable extensions.

Theorem 1.7.7. *Assume that K is an analytic valued field and L/K is an algebraic field extension. Then there exists a unique way to extend the valuation $| \ |$ of K to a valuation $| \ |_L$ on L. In fact, for an element $\alpha \in L$ of degree d it is given by the formula $|\alpha|_L = |\mathcal{N}r(\alpha)|^{1/d}$.*

Proof. The archimedean case is covered by the second Ostrowski's theorem, so we assume that K is non-archimedean. To prove existence we should check that $|\ |_L$ defined by the above formula is a valuation. Clearly it is multiplicative and coincides with $|\ |$ on K, so we should only check that $|x+y|_L \le |x|_L + |y|_L$. Dividing by x or y we reduce this claim to the following particular case: if $\alpha \in L$ satisfies $|\alpha|_L \le 1$, then $|1+\alpha|_L \le 1$. Let $f(t) = t^d + a_1 t^{d-1} + \dots + a_d$ be the minimal polynomial of α. By our assumption $a_d = (-1)^d \mathcal{N}r(\alpha)$ satisfies $|a_d| \le 1$, and hence $|a_i| \le 1$ for any i by Corollary 1.6.16. Since $(-1)^d \mathcal{N}r(\alpha+1)$ is the free coefficient of $f(t-1)$, we have that $|\mathcal{N}r(\alpha+1)| = |1 - a_1 + a_2 - \dots| \le 1$ and thus $|\mathcal{N}r(\alpha+1)| \le 1$, as required.

To prove uniqueness assume, to the contrary, that $|\ |'_L$ is another valuation on L extending $|\ |$. In particular, there exists $\alpha \in L$ such that $|\alpha|_L \ne |\alpha|_{L'}$. Since both $|\ |_L$ and $|\ |_{L'}$ are K-norms on L, their restrictions onto $K(\alpha)$ are equivalent by Corollary 1.7.5. Thus, there exists $C > 0$ such that $C^{-1}|a|_L \le |a|'_L \le C|a|_L$ for any $a \in K(\alpha)$. This contradicts the obvious fact that $|\alpha^d|_L / |\alpha^d|'_L = (|\alpha|_L / |\alpha|'_L)^d$ tends to either zero or infinity. □

By the theorem the valuation of an analytic field K extends to the algebraic closure K^a uniquely. In the sequel, writing $\widehat{K^a}$ we always mean completing K with respect to this valuation. Similarly to K^a, the completed algebraic closure $\widehat{K^a}$ is unique up to an automorphism. One can also phrase this as follows.

Corollary 1.7.8. *If K is an analytic field, then $\widehat{K^a}$ is the minimal analytic extension of K containing the algebraic closure of K. Namely, any embedding of analytic fields $K \hookrightarrow L$ such that L contains K^a factors into a composition of embeddings of valued field $K \hookrightarrow \widehat{K^a} \hookrightarrow L$.*

We record another immediate corollary, which could also be proved in a simple straightforward way.

Corollary 1.7.9. *If l/k is an algebraic extension of real valued fields and K is trivially valued, then l is trivially valued.*

1.7.10. *Preservation of completeness.* The next natural question is whether an extension of a complete field must be complete.

Lemma 1.7.11. *Assume that K is an analytic field and L/K a finite extension. Then L is complete with respect to the valuation extending that of K.*

Proof. Since the valuation on L is a K-norm, this follows from Corollary 1.7.5. □

The case of infinite extensions is outlined in the exercise.

Exercise 1.7.12. Assume that K is an analytic field with a non-trivial valuation and L/K is an infinite algebraic extension.

(i) Assume that the degree of elements of L over K is unbounded (for example, this is the case when L/K is separable). Show that L is not complete.

(ii) Give examples when the degree of elements is bounded and L is complete or incomplete. (Hint: if $[K : K^p] = \infty$ then $L = K^{1/p}$ is an infinite extension and L is complete and L/K contains incomplete subextensions.)

1.7.13. *Bounding the roots.* Our next goal is to show that $\widehat{K^a}$ is, in fact, algebraically closed. For this we will show that roots of polynomials depend continuously on the coefficients, and the first task is to bound them is terms of the coefficients. As usually, we provide $K[t]$ with the Gauss norm.

Lemma 1.7.14. *Assume that f is a monic polynomial over a non-archimedean valued field k and $a \in k$ is a root of f. Then $|a| \le |f|$.*

Proof. Assume, to the contrary, that $|a| > |f|$ and note that $|f| \ge 1$. Writing $f = t^n + \sum_{i=1}^n a_i t^{n-i}$ we obtain that $|a^n| > |a_i a^{n-1}| \ge |a_i a^{n-i}|$ for any i, and hence $|f(a)| = |a^n|$. Since $|a| \ge 1$ we obtain that a is not a root of f. □

Corollary 1.7.15. *Assume that f, g are monic polynomials of degree n over a non-archimedean valued field k and $a \in k$ is a root of f. Then $|g(a)| \le |f - g| \cdot |f|^{n-1}$.*

Proof. Assume that $f = t^n + \sum_{i=1}^n a_i t^{n-i}$ and $g = t^n + \sum_{i=1}^n b_i t^{n-i}$, then

$$|g(a)| = |g(a) - f(a)| \le \max_{1 \le i \le n} |a_i - b_i| \cdot |a|^{n-i} \le \max_{1 \le i \le n} |f - g| \cdot |f|^{n-i} = |f - g| \cdot |f|^{n-1}.$$

□

1.7.16. *Continuity of roots.* Now we can prove that roots of $f(t)$ vary continuously with it.

Theorem 1.7.17. *Assume that $f \in K[t]$ is a monic polynomial of degree n over a non-archimedean analytic field K and $\varepsilon > 0$ a positive number. If $g \in K[t]$ is monic of degree n and such that $|f - g| < \min(1, \varepsilon^n |f|^{1-n})$, then for any root $b \in K^a$ of g there exists a root $a \in K^a$ of f such that $|a - b| < \varepsilon$.*

Proof. Note that $|f| = |g|$ since $|f - g| < 1 \le |f|$. If $a_1, \dots, a_n \in K^a$ are the roots of f, then by Corollary 1.7.15

$$\prod_{i=1}^n |a_i - b| = |f(b)| \le |f - g| \cdot |g|^{n-1} = |f - g| \cdot |f|^{n-1} < \varepsilon^n.$$

So, for some choice of $a = a_i$ we necessarily have that $|a - b| < \varepsilon$. □

One can easily extend the above results to the archimedean case after replacing the Gauss norm by its archimedean (non-multiplicative) analogue $|\sum_i a_i t^i| = \sum_i |a_i|$.

Exercise 1.7.18. Adjust formulations and proofs of Lemma 1.7.14, Corollary 1.7.15 and Theorem 1.7.17 to the archimedean case. For example, in the corollary one should relax the bound to $|g(a)| \le n|f - g| \cdot |f|^{n-1}$.

1.7.19. *Completed algebraic closure.* Now, we can finally prove that algebraic closedness is preserved by completions. In fact, even slightly more is true since inseparability of a polynomial is a closed condition which is destroyed by small deformations.

Corollary 1.7.20. *If k is a separably closed real valued field with a non-trivial valuation, then the completion $\widehat{k}$ is algebraically closed.*

Proof. Set $K = \widehat{k}$. It suffices to prove that any monic polynomial $f \in K[t]$ has a root in K. Let $d = \deg(f)$ and $a_1, \dots, a_d \in K^a$ the roots of f. Since k is dense in K, we can choose a family of monic polynomials $f_n \in k[t]$ such that $|f - f_n| < \min(1, \frac{1}{n^d}|f|^{1-d})$. Moreover, we can achieve that the linear terms of

f_n are non-zero (this is the only place where we use that the valuation is non-trivial). The non-vanishing of the linear term implies that f_n has a separable root $b_n \in k^s = k$. By Theorem 1.7.17 for each n there exists $i = i(n)$ such that $|b_n - a_i| < \frac{1}{n}$. In particular, at least one a_i satisfies infinitely many such inequalities and hence lies in the closure of k. □

Combining this with Corollary 1.7.8 we can now characterize the analogue of algebraic closure in the category of analytic fields.

Corollary 1.7.21. *If K is an analytic field, then $\widehat{K^a}$ is the minimal algebraically closed analytic extension of K. Furthermore, if the valuation is non-trivial, then $\widehat{K^s} = \widehat{K^a}$.*

1.7.22. *Examples.* The completed algebraic closure $\widehat{\mathbb{Q}_p^a}$ is usually denoted $\mathbb{C}_p$. Constructing it and proving that it is algebraically closed was one of main achievements of Kürschák work in 1913.

Lemma 1.7.23. *The field $\mathbb{C}_p$ is the minimal algebraically closed analytic field of mixed characteristic. Moreover, for any analytic algebraically closed field K of mixed characteristic there exists a unique embedding of analytic fields $\mathbb{C}_p \hookrightarrow K$.*

Proof. By Ostrowski theorem the valuation of K restricts to $|\ |_p^r$ on $\mathbb{Q}$, hence the embedding $\mathbb{Q} \hookrightarrow K$ factors uniquely through $\mathbb{Q}_p$. Since K is algebraically closed it factors uniquely through $\mathbb{C}_p$. □

The minimal analytic algebraically closed equicharacteristic fields are $\mathbb{F}_p^a$ and $\mathbb{Q}^a$ with trivial valuations. For non-trivial valuations there is the following weaker minimality claim, where the embedding is not unique at all.

Lemma 1.7.24. *If K is an analytic algebraically closed field K of equal characteristic and the valuation is non-trivial, then there exists an embedding of valued fields $\widehat{\mathbb{F}((t))^a} \hookrightarrow K$, where $\mathbb{F}$ is a trivially valued prime field.*

Proof. By Ostrowski's theorem the valuation of K is trivial on the prime field contained in K. So, we can simply take any $t \in K$ with $0 < |t| < 1$. □

To obtain a broader picture let us also outline some results that will be proved later.

Remark 1.7.25. (i) Let k be a trivially valued field and $K = k((t))$. After developing a theory of transcendental extensions we will show that $\mathrm{char}(k) = 0$ if and only if any k-endomorphism of the analytic field $\widehat{K^a}$ is an isomorphism. In particular, $\widehat{\mathbb{F}_p((t))^a}$ contains elements x transcendental over $\mathbb{F}_p((t))$ such that the embedding $\widehat{\mathbb{F}_p((x))^a} \hookrightarrow \widehat{\mathbb{F}_p((t))^a}$ is not an isomorphism. This surprising fact was independently rediscovered few times, and also its converse has a story of "proofs".

(ii) After developing a basic ramification theory we will prove that if $k = k^a$ and $\mathrm{char}(k) = 0$, then the Galois theory of $K = k((t))$ is very simple: $K^a = K(t^{1/\infty}) := \cup_n K(t^{1/n})$. In particular, $\widehat{K^a}$ consists of sums $\sum_{i=0}^{\infty} a_i t^{q_i}$, where $a_i \in k$ and (q_i) is a strictly increasing unbounded set of rational numbers.

(iii) If $\mathrm{char}(k) > 0$, then the Galois closure of K is much larger than $K(t^{1/\infty})$, and cannot be described so explicitly. The Galois theories of $\mathbb{Q}_p$ and $\mathbb{F}_p((t))$ are complicated and similar in many aspects. In particular, there is a natural isomorphism between the the absolute Galois groups of the fields $\mathbb{F}_p((t))$ (or its perfection $\cup_n \mathbb{F}_p((t^{1/p^n})))$ and $\cup_n \mathbb{Q}_p(\xi_{p^n})$, where ξ_{p^n} is a primitive root of unity of order p^n.

Exercise 1.7.26. (i) Show that any analytic field $k(\widehat{(t^{1/\infty})})$ is not spherically complete.

(ii) Let k be a field and let $\Gamma \subseteq \mathbf{R}$ be a divisible subgroup, for example, $\mathbb{Q}$. Let $K = k((t^\Gamma))$ be the set of *well-ordered formal series* $\sum_{i\in I} a_i t^i$, where $a_i \in k^\times$ and I is a well-ordered subset of Γ (i.e. any finite strictly decreasing subset of I is finite). In particular, $0 \in K$ is the empty sum. Provide K with the natural structure of a field and a non-archimedean real valuation such that $|k^\times| = 1$ and $|t^\gamma| = r^\gamma$ for a fixed $r \in (0,1)$. (The main point is to show that multipication involves only finite sums and preserves well-orderedness). Show that K is a spherically complete analytic field. (In fact, we will later show that if k is algebraically closed then K is also algebraically closed.)

(iii)** Prove claim (i) of the remark.

1.7.27. *Krasner's lemma.* Assume now that K is an analytic field and $\alpha \in K^a$ is algebraic over K. Let $\alpha = \alpha_1, \alpha_2, \dots, \alpha_d$ be the set of all roots of the minimal polynomial of α. The number $r_{\alpha,k} = \min_{2\le i\le d} |\alpha - \alpha_i|$, which is well defined by Theorem 1.7.7, will be called the *splitting radius* of α, and we will omit k from the notation when possible. Clearly, $r_\alpha = 0$ if and only if α is not separable over k. The following famous result is called Krasner's lemma, though it is essentially due to Ostrowski.

Theorem 1.7.28. *Assume that K/k is an extension of non-archimedean real valued fields and K is complete, and provide K^a with the valuation extending that of K. Assume further that $\alpha \in K^a$ is algebraic over k and K contains an element α_0 such that $|\alpha - \alpha_0| < r_\alpha$. Then $\alpha \in K$.*

Proof. Clearly $r_\alpha > 0$ and hence α is separable over k. We should prove that the minimal polynomial of α over K is linear. If $f(t)$ denotes this polynomial, then $f(t+\alpha_0)$ is an irreducible polynomial over K which vanishes at $\alpha - \alpha_0$ and has all other roots of the form $\alpha_i - \alpha_0$ for $i > 1$. On the other hand, all roots of $f(t+\alpha_0)$ are of the same absolute value by Theorem 1.7.7, while $|\alpha_1 - \alpha_0| < r \le |\alpha_i - \alpha_0|$ for $i > 1$. This implies that f is necessarily linear. $\square$

Remark 1.7.29. (i) In fact, in the classical formulation one only considers the case when K/k is algebraic, which is equivalent to the case $K = k(\alpha_0)$.

(ii) The geometric meaning of Krasner's lemma is that the Berkovich disc E in $\mathbf{A}^1_k$ with center at α and of radius smaller than r_α is defined over the extension $k(\alpha)$. In particular, $k(\alpha) \subseteq \mathcal{H}(x)$ for any point $x \in E$, including the (non-classical) points with non-algebraic $\mathcal{H}(x)/k$.

In our proof that algebraic closedness is preserved by completions we used a relatively implicit convergence process. Krasner's lemma provides a much better control. In fact, for any separable monic polynomial f it provides an explicit threshold δ_f so that any smaller deformation of f has the same Galois theory.

Corollary 1.7.30. *Assume that K is an analytic field and $f \in K[t]$ is a separable monic polynomial with roots $a_1, \dots, a_n \in K^a$, and set $r_f = \min_{1\le i<j\le n} |a_i - a_j|$ and $\delta_f = \min(1, r_f^n |f|^{1-n})$. Then for any monic polynomial g such that $|f - g| < \delta_f$ one can order the roots $b_1, \dots, b_n \in K^a$ of g so that $K(a_i) = K(b_i)$ for any $i \in \{1, \dots, n\}$.*

Proof. Combine Corollary 1.7.15 and Theorem 1.7.28. $\square$

Remark 1.7.31. Naturally, the minimal distance r_f between the roots affects the deformation threshold. For example, we know that the statement fails for inseparable polynomials because they can be approximated by separable ones with any precision. This situation is an instance of a general principle that smooth objects are stable under small deformations, while singularities can be destroyed/changed by arbitrarily small ones.

Exercise 1.7.32. Use Krasner's lemma to prove that $\mathbb{C}_p$ is not spherically complete.

1.8. **Extension of valuations: the non-complete case.** In this section we will use the theory developed in the complete case to study extensions of non-complete real valued fields. The main novelty is that extension of a valuation to l/k is not unique anymore, and we will see that they are parameterized by conjugacy classes of embedding $l \hookrightarrow \widehat{k}^a$.

1.8.1. *The set of extensions.* Let k be a real valued field, l/k an algebraic extension, and $V_{l/k}$ the set of real valuations on l extending the valuation of k. Any embedding of k-fields $l \hookrightarrow K^a$ induces a k-valuation on l, hence we obtain a map $\phi\colon \mathrm{Hom}_k(l, K^a) \to V_{l/k}$. Moreover, any $\sigma \in \mathrm{Aut}(K^a/K)$ acts on K^a by isometries because the extension of the valuation to K^a is unique, so the map ϕ factors through $\mathrm{Hom}_k(l, K^a)/\mathrm{Aut}(K^a/K)$.

Theorem 1.8.2. *Assume that k is a real valued field with $K = \widehat{k}$, and l/k is an algebraic extension. Then there always exists an extension of valuation to l, each such extension is induced by a k-embedding $l \hookrightarrow K^a$, and two embedding induce the same valuation if and only if they are conjugate over K. Equivalently, we have a natural bijection of non-empty sets* $\mathrm{Hom}_k(l, K^a)/\mathrm{Aut}(K^a/K) = V_{l/k}$.

Proof. Clearly, $\mathrm{Hom}_k(l, K^a)$ is non-empty, hence $V_{l/k}$ is non-empty too.

If l is provided with a k-valuation, then the analytic field $L = \widehat{l}$ is the completion of its subfield Kl. In particular, L embeds into $\widehat{K^a}$ as a real valued field, and we obtain that the valuation on l is induced from the corresponding embedding $l \hookrightarrow K^a$. This proves that ϕ is onto.

It remains to show that if two embeddings $i\colon l \hookrightarrow K^a$ and $j\colon l \hookrightarrow K^a$ induce the same valuation on l, then they are conjugated over K. Letting $L = \widehat{l}$ denote the completion of l with respect to the induced valuation, we obtain embeddings $\widehat{i}\colon L \hookrightarrow \widehat{K^a}$ and $\widehat{j}\colon L \hookrightarrow \widehat{K^a}$. Since $\widehat{K^a}$ is the minimal analytic algebraically closed field containing L, and such a field is unique by Corollary 1.7.21, the identity $L = L$ extends to an isomorphism $\sigma\colon \widehat{K^a} \xrightarrow{\sim} \widehat{K^a}$ such that $\widehat{j} = \sigma \circ \widehat{i}$. Since i and j coincide on k, the automorphism σ fixes k and, hence, also K. Therefore σ restricts to a K-automorphism of K^a which conjugates i and j. □

1.8.3. *Conjugation of extensions.* Note that the group $\mathrm{Aut}(l/k)$ acts on the k-valuation on the set $V_{l/k}$ via $|x|_\sigma = |\sigma(x)|$.

Corollary 1.8.4. *In the situation of Theorem 1.8.2 assume that l/k is normal. Then the group $\mathrm{Aut}(l/k)$ acts transitively on the set of $V_{l/k}$.*

Proof. Indeed, if l/k is normal, then by the usual Galois theory any two embeddings of l into any extension of k are conjugated by an element of $\mathrm{Aut}(l/k)$. Therefore $\mathrm{Aut}(l/k)$ acts transitively on $\mathrm{Hom}_k(l, K^a)/\mathrm{Aut}(K^a/K) = V_{l/k}$. □

Example 1.8.5. A classical example is obtained when $k = \mathbb{Q}$ with the archimedean valuation and l/k is finite. Then any archimedean valuation on l is obtained from an embedding $l \hookrightarrow \mathbb{C}$ and two embeddings induce the same valuation if and only they are conjugate over $\mathbb{R}$. If l is a Galois extension of $\mathbb{Q}$, then all its archimedean valuations are either real or complex.

1.8.6. *The tensor product formula.* Now we would like to reformulate the above Galois theoretic statement to something more concrete, and a very useful way is to combine all extensions of the valuation via the tensor product $l \otimes_k \widehat{k}$. In Galois theory one usually composes subfields of a given field. By an *abstract composite* lK we mean a k-field F with k-embeddings $l \hookrightarrow F$ and $K \hookrightarrow F$ such that F is generated by their images. A general theory of tensor products easily implies that the reduction $A = \mathrm{Red}(l \otimes_k K)$ (i.e. the quotient of A by the ideal of nilpotent elements) is a product of fields $\prod_{i=1}^n L_i$, where $L_1, \dots, L_n$ are precisely the isomorphism classes of abstract composites lK. Using this Theorem 1.8.2 can be reformulated for finite extensions as follows

Theorem 1.8.7. *Assume that k is a real valued field with $K = \widehat{k}$, and l/k is a finite extension. Then the set $V_{l/k}$ is finite, say $V_{l/k} = \{| \ |_1, \dots, | \ |_n\}$, and if L_i are the completions of l with respect $| \ |_i$, then there is natural isomorphism* $\mathrm{Red}(l \otimes_k K) = \prod_{i=i}^n L_i$ *of k-algebras.*

Proof. Any $\sigma \in \mathrm{Hom}_k(l, K^a)$ gives rise to a composite $\sigma(l)K$ of l and K, and two composites are isomorphic as abstract composites if and only if they are conjugate over K. In addition, σ induces a real valuation $| \ |_i$ on l, and clearly l is dense in $\sigma(l)K$. Since $\sigma(l)K$ is complete by Lemma 1.7.11, we obtain that $\sigma(l)K = L_i$. By Theorem 1.8.2 elements of $\mathrm{Hom}_k(l, K^a)$ induce the same valuation on l if and only if they are conjugate over K, and this implies that $L_1, \dots, L_n$ with embeddings $l \hookrightarrow L_i$ and $K \hookrightarrow L_i$ are precisely all isomorphism classes of abstract composites. So, general Galois theory implies the theorem. □

1.8.8. *The degree formula.* Now we can relate the degrees of extensions and bound the size of $V_{l/k}$.

Corollary 1.8.9. *Keep assumption of Theorem 1.8.7. Then*

$$[l : k] = \sum_{i=1}^n d_i [L_i : K],$$

where $d_i = 1$ whenever l/k or K/k is separable, and d_i are powers of $\mathrm{char}(k)$ *otherwise. In particular, there are at most $[l : k]$ extensions of the valuation of k to l.*

Proof. This follows from Theorem 1.8.7 and the following facts about the K-algebra $A = l \otimes_k K$ known from the usual theory of fields: $\dim_k(l) = \dim_K(A)$, the ring A is a product of local Artin rings A_i, where A_i is reduced whenever l/k is separable, and otherwise $L_i := \mathrm{Red}(A_i)$ is a field and $\dim_K(A_i) = p^n \dim_K(l_i)$, where $p = \mathrm{char}(k)$. □

Example 1.8.10. It is the classical fact in number theory that for a number field l one has that $l \otimes \mathbb{R}$ is the product of s copies of $\mathbb{R}$ and t copies of $\mathbb{C}$, where s is the number of real valuations with $\widehat{l} = \mathbb{R}$ (or embeddings of l into $\mathbb{R}$) and t is the number of real valuations with $\widehat{l} = \mathbb{C}$ (or pairs of conjugate embeddings $l \hookrightarrow \mathbb{C}$). In particular, $s + 2t = [l : \mathbb{Q}]$.

Exercise 1.8.11. (i) Take F a field of characteristic p and consider $K = F((t))$ with the t-adic valuation. Take $x = x(t) \in F$ a transcendental element, which is not a p-th power and let $k = F(t, x^p)$ with the real valuation induced from K. Show that k is a discrete valued field, whose completion is K. Show also that $l = F(t, x)$ is an inseparable extension of k, there is only one extension of the valuation to l and $\widehat{l} = K$. In particular, in this case $d_1 = p$. Finally, show that the extension l°/k° of rings of integers is not finitely generated.

(ii) Using Zorn's lemma one can obtain even worse examples. Show that there exists a maximal subfield E of K such that $k \subseteq E$ and $x \notin E$, and then necessarily K/E is algebraic and purely inseparable. Thus one obtains a non-complete field E whose completion K is algebraic and purely inseparable over it.

Remark 1.8.12. A pathological discrete valuation ring k° as above often appears as a counter-example to many properties one might naively expect. In particular, it is a simplest example of so called not quasi-excellent ring (in this case, its completion is not separable over it). Also, the integral closure of k° in the finite extension l is easily seen to be l°, but the integral ring extension l°/k° is not finite.

1.8.13. *Independence of valuations and weak approximation.* Real valuations on a ring A are called *equivalent* if each of them is a power of the other. It turns out that non-equivalent valuations satisfy a strong independence condition, often called the weak approximation theorem.

Theorem 1.8.14. *Assume that k is a field and $| \ |_i$, $1 \le i \le n$ is a finite set of pairwise non-equivalent non-trivial real valuations on k. Then for any elements $a_1, \dots, a_n \in k$ and a real number $\varepsilon > 0$ there exist $a \in k$ such that $|a - a_i|_i < \varepsilon$.*

Proof. It suffices to prove this when some a_i equals 1 and others vanish. Indeed, in this case for $r = n \max_{i,j} |a_i|_j$ we can choose $d_1, \dots, d_n \in k$ so that $r|d_i - 1|_i < \varepsilon$ and $r|d_j|_i < \varepsilon$ for $j \ne i$, and then $a = \sum_{i=1}^n a_i d_i$ is as required because for any i

$$|a - a_i|_i \le |a_i|_i \cdot |d_i - 1|_i + \sum_{j \ne i} |a_j|_i \cdot |d_j|_i \le r \max\left(|d_i - 1|_i, \max_{j \ne i} |d_j|_i\right) < \varepsilon.$$

So, in the sequel we can assume that $a_1 = 1$ and $a_i = 0$ for $2 \le i \le n$.

We claim that for any $i \in \{2, \dots, n\}$ there exists z_i with $|z_i|_1 < 1$ and $|z_i|_i > 1$. Assume this claim fails. Since the valuations $| \ |_1$ and $| \ |_i$ are not equivalent, there exist $x, y \in k$ such that $C_1 = \frac{\log |x|_1}{\log |y|_1}$ and $C_2 = \frac{\log |x|_i}{\log |y|_i}$ are different. Clearly we can replace either of x and y by its inverse, hence we can also assume that $|x|_1 > 1$ and $|y|_1 > 1$, and then by our assumption $|x|_i > 1$ and $|y|_i > 1$. Switching x and y if necessary we can assume that $C_1 < C_2$. Then for any choice of $m, n \in \mathbb{N}$ with $C_1 < \frac{m}{n} < C_2$ the element $z_i = \frac{x^n}{y^m}$ is as required.

Replacing $z_2, \dots, z_n$ by their powers $z_i^{l_i}$ with general enough $l_2, \dots, l_n \in \mathbb{N}$ we can achieve, in addition, that no $i, j, k \in \{2, \dots, n\}$ satisfy $|z_i|_k = |z_j|_k > 1$. Set $b_m = \sum_{i=2}^n z_i^m$. Clearly $\lim_m |b_m|_1 = 0$, and we claim that also $\lim_m |b_m|_i = \infty$ for $2 \le i \le n$. Indeed, $\max_j |z_j|_i > 1$, and if it is achieved for $j = k$, then $|z_j^m|_i = o(|z_k^m|_i)$ for $j \ne k$ and hence $|b_m|_i = |z_k^m|_i(1 + o(1))$ tends to infinity. It follows immediately that the sequence $|\frac{1}{1+b_m}|_1$ tends to 1 and $|\frac{1}{1+b_m}|_i$ tends to 0 when $2 \le i \le n$. So, we can take $a = \frac{1}{1+b_m}$ with a large enough m. $\square$

Importance of this theorem is reflected in the following result.

Corollary 1.8.15. *Assume that k is a field and $|\ |_i$, $1 \le i \le n$ is a finite set of pairwise non-equivalent real valuations on k and K_i are the completions of k with respect to $|\ |_i$, then*

(i) The field k is dense in the ring $K := \prod_{i=1}^n K_i$ provided with the product seminorm $|(x_1, \dots, x_n)| = \max_i |x_i|_i$.

(ii) The completion of k with respect to the norm $|x| = \max_i |x|_i$ is K.

Proof. Both claims are obviously equivalent, and (i) is nothing else but just a reformulation of Theorem 1.8.14. □

Example 1.8.16. (i) For example, the completion of $\mathbb{Q}$ with respect to the 10-adic norm is $\mathbb{Q}_{10} = \mathbb{Q}_2 \times \mathbb{Q}_5$.

(ii) In the situation of Theorem 1.8.7 let $|\ |_i$, $1 \le i \le n$ be the elements of $V_{l/k}$ and define the max norm on l by $|a|_{\max} = \max_i |a|_i$. Then $\prod_i L_i$ is the completion of l with respect to $|\ |_{\max}$.

1.8.17. *The max norm.* More generally, for a real valued field k we provide its algebraic closure k^a with the max norm $|\ |_{\max}$ obtained by maximizing all extensions of the valuation: $|x|_{\max} = \max_{|\ |_i \in V_{l/k}} |x|_i$. This is well defined since there only finitely many extensions of the valuation on $k(x)$ by Corollary 1.8.9. Our next goal is to obtain a nice formula for the max norm, which generalizes the formula for extended valuation in the analytic case. Note that in general the extension is not unique, so one should expect a simple formula for each extension separately.

1.8.18. *The spectral value.* For a monic polynomial $f(t) = t^d + c_1 t^{d-1} + \ldots + c_d$ over a non-archimedean valued field k we define its spectral value $\sigma(f) := \max_{1 \le i \le d} |c_i|^{1/i}$.

Lemma 1.8.19. *If f splits completely in k, say $f(t) = \prod_{i=1}^d (t - a_i)$, then $\sigma(f) = \max_i |a_i|$.*

Proof. Set $r = \max_i |a_i|$. Since $(-1)^n c_n$ is the sum of products of n roots of f, we have that $|c_n| \le r^n$. It remains to show that the equality is achieved for some n. Let n be the number of roots satisfying $|a_i| = r$, and order the roots so that $|a_i| = r$ for $1 \le i \le n$ and $|a_i| < r$ for $n+1 \le i \le d$. Then $(-1)^n c_n$ equals to the sum of $a_1 \dots a_n$, which is of valuation r^n, and other products, which are of smaller valuation. Thus, $|a_n| = r^n$, as required. □

Exercise 1.8.20. Prove the following properties of the spectral value:

(i) $\sigma(fg) = \max(\sigma(f), \sigma(g))$.

(ii) Assume that f, g, h have roots $\alpha, \beta, \gamma \in k^a$, respectively.

  (a) If $\gamma = \alpha + \beta$, then $\sigma(h) \le \max(\sigma(f), \sigma(g))$.

  (b) If $\gamma = \alpha\beta$, then $\sigma(h) \le \sigma(f)\sigma(g)$.

(iii) If $f = \prod_{i=1}^n (t - \alpha_i)$ and $g = \prod_{i=1}^n (t - \alpha_i^n)$, then $\sigma(g) = \sigma(f)^n$.

Note that the simplest proof is to use Lemma 1.8.19 and the fact that the valuation of k can be extended to k^a, but this can be also checked directly on the level of coefficients of f, g and h.

Remark 1.8.21. The exercise shows that the formula $|\alpha|_{\rm sp} := \sigma(f_\alpha)$ defines a power multiplicative norm on k^a called the *spectral norm*. This also follows from Theorem 1.8.23 below asserting that $|\ |_{\rm sp} = |\ |_{\max}$. A much more general instance of this phenomenon will be established in §1.10.

1.8.22. *The spectral norm.* The spectral value provides the promised formula for the max norm.

Theorem 1.8.23. *Assume that k is a non-archimedean real-valued field. Then for any $\alpha \in k^a$ with minimal polynomial $f_\alpha \in k[t]$ one has that $|\alpha|_{\max} = \sigma(f_\alpha)$.*

Proof. Let l be the splitting field of f_α, let $\alpha = \alpha_1, \dots, \alpha_m$ be all conjugates of α, and let $|\ |_1, \dots, |\ |_n$ be all elements of $V_{l/k}$. By Lemma 1.8.19 we have that $\sigma(f_\alpha) = \max_i |\alpha_i|_1$. Since all elements of $V_{l/k}$ are conjugate by Corollary 1.8.4, we obtain that $\max_i |\alpha_i|_1 = \max_j |\alpha|_j = |\alpha|_{\max}$, as required. □

Corollary 1.8.24. *Let k be a non-archimedean real valued field, and assume that k is henselian (for example, k is complete). Then for any irreducible monic polynomial $f = t^d + c_1 t^{d-1} + \dots + c_d \in k[t]$ over k, the inequality $|c_i|^{1/i} \le |c_d|^{1/d}$ holds for any i with $1 \le i \le d$.*

Proof. Let α be a root of k. Since the extension of the valuation to k^a is unique, all conjugates of α have the same absolute value and hence $|\alpha| = |c_d|^{1/d}$. In addition, since the valuation is unique $|\alpha| = |\alpha|_{\max} = \sigma(f) \ge |c_i|^{1/i}$. □

Remark 1.8.25. (i) The above corollary is a variation on the theme of Hensel's lemma. In fact, a particular case with $|c_d| = 1$ proved in Corollary 1.6.16 was used to extend the valuation first in the analytic case and then in general. So, our proof of Corollary 1.8.24 is based on it.

(ii) An alternative construction of the theory of extensions of valuation is as follows: first one solves Exercise 1.8.20 directly by computations with coefficients, obtaining an elementary proof that $|\ |_{\mathrm{sp}}$ is a norm. Then one shows the version 1.8.24 of Hensel's lemma over a complete k, and deduces that $|\ |_{\mathrm{sp}} = |a_d|^{1/d}$. In particular, $|\ |_{\mathrm{sp}}$ is a valuation. To large extent, this order of exposition is chosen in [BGR84, Chapter 3]. The notion of the spectral value of a polynomial is also taken from there. See [BGR84, Remark in §1.5.4] for the history of this notion.

1.9. **Henselian fields.**

1.9.1. *Henselian fields and extensions.* We say that an algebraic extension of real valued fields l/k is *henselian* if $|V_{l/k}| = 1$. A valued field k is called *henselian* if the extension k^a/k is henselian.

Remark 1.9.2. (i) For fields, the terminology is standard. We will see that in the non-archimedean case henselian fields are directly related to the Hensel's lemma, but the notion is valuable (though simple) in the archimedean case too.

(ii) Our terminology is not standard for algebraic extension, but we feel free to introduce it because this is an important class of extensions, and it seems no special name had been chosen so far.

Since valuations always extend through finite extension the following result is obvious.

Lemma 1.9.3. *Assume that k is a real valued field and $m/l/k$ is a tower of algebraic extensions, then*

(i) m/k is henselian if and only if l/k is henselian and m/l is henselian with respect to the extension of the valuation to l.

(ii) k is henselian if and only if l/k is henselian and l is henselian with respect to the extension of the valuation.

1.9.4. *A general criterion.* Recall that an algebraic extension l/k is called linearly disjoint from $\widehat{k}/k$ (for example, in $\widehat{k^a}$) if $[l\widehat{k} : \widehat{k}] = [l : k]$, and this happens if and only if $l \otimes_k \widehat{k}$ is a field, and then $l \otimes_k \widehat{k} = l\widehat{k}$. Moreover, if l/k is separable, then this happens if and only if $\widehat{k}/k$ does not contain non-trivial subextensions of the Galois closure l^{nor} of l/k. Combining this with Theorem 1.8.7 we obtain the following general criterion of henselianity.

Theorem 1.9.5. *Assume that k is a real valued field and l/k is an algebraic extension with the maximal separable subextension l_s/k. Then,*

(i) The extension l/k is henselian if and only if $\widehat{k}/k$ is linearly disjoint from l_s/k.

(ii) The field k is henselian if and only if it is separably closed in $\widehat{k}$.

Proof. First, any purely inseparable extension l/k is henselian, because any $x \in l$ satisfies $y = x^{p^n} \in k$ for $p = \mathrm{char}(k)$ and a large enough n, and hence $|x|_l = |y|^{1/p^n}$ defines the only extension of the valuation of k.

By Lemma 1.9.3, l/k is henselian if and only if l_s/k is, and this reduces the proof of (i) to the case when $l = l_s$ is separable over k. Furthermore, it is easy to see that l/k is henselian (resp. linearly disjoint from $\widehat{k}$) if and only if any finite subextension l_i/k is so. This reduces us further to the case when l/k is finite and separable. In this case $l \otimes_k \widehat{k}$ is a product of fields, and we obtain that $\mathrm{Red}(l \otimes_k \widehat{k})$ is a field if and only if $\widehat{k}/k$ is linearly disjoint from l/k. By Theorem 1.8.7 the former happens if and only if l/k is henselian.

By Lemma 1.9.3, k is henselian if and only if k^s/k is henselian. By claim (i) this happens if and only if $\widehat{k}/k$ is linearly disjoint from k^s/k, and since k^s/k is Galois, this happens if and only if k is separably closed in $\widehat{k}$. □

Remark 1.9.6. This theorem and some results below indicate that, from algebraic point of view, henselian fields behave rather similarly to complete ones, though one must be careful about inseparable extensions: Exercise 1.8.11(ii) provides an example of a henselian dvr which is not algebraically closed in its completion. In fact, henselian fields were called "quasi-complete" in [Ber93].

1.9.7. *Henselization.* For a real valued field k we define its *henselization* k^h to be the separable closure of k in $\widehat{k}$. This is the minimal valued extension l/k such that l is henselian:

Lemma 1.9.8. *Assume that l/k is an extension of valued fields and l is henselian. Then there exists a unique factorization $k \hookrightarrow k^h \hookrightarrow l$.*

Proof. We have that $\widehat{k} \subseteq \widehat{l}$ and l is separably closed in $\widehat{l}$, in particular, l contains the separable closure of k in $\widehat{k}$. We obtained an embeddings of valued fields $k \hookrightarrow k^h \hookrightarrow l$, and it is unique because k is dense in k^h. □

Remark 1.9.9. In the same venue as Remark 1.9.6, henselization can be viewed as an algebraic (and much finer) analogue of completion. In the sequel, we will study valuations of larger height, in which case completions are rather meaningless while henselizations make a perfect sense and are very useful. However, to obtain this generalization we will first have to provide a new characterization of henselization, and this will involve the theory of unramified extensions.

1.9.10. *Archimedean henselian fields.* Recall that a field l is *real closed* if and only if $\mathrm{char}(l) = 0$ and $l \subsetneq l^a = l(\sqrt{-1})$. By a theorem of Artin-Shreier these are precisely the fields F such that F^a/F is a non-trivial finite extension. Any archimedean valuation on k is induced from either $k \hookrightarrow \mathbb{R}$ or $k \hookrightarrow \mathbb{C}$. In the second case we assume that $k \nsubseteq \mathbb{R}$, and we say that the valuation is real or complex, accordingly. By Theorem 1.9.5(ii), k is henselian if and only if it is algebraically closed in $\mathbb{R}$ or $\mathbb{C}$, respectively, hence we obtain the following classification:

Lemma 1.9.11. *An archimedean real valued field k is henselian if and only if either the valuation is complex and k is algebraically closed, or the valuation is real and k is real closed.*

1.9.12. *Henselian fields and Hensel's lemma.* Now we are going to prove that in the non-archimedean case, a field is henselian if and only if it satisfies Hensel's lemma. We proved various versions of this lemma and its corollaries, and essentially any such statement can be used here. We do not try to make a full list, but prove this for quit a few most useful versions.

Theorem 1.9.13. *Assume that k is a non-archimedean real valued field. Then the following conditions are equivalent:*

(i) k is henselian.

(ii) For any $f \in k^\circ[t]$ and a factorization $\widetilde{f} = \overline{g}\overline{h}$ with $(\overline{g}, \overline{h}) = 1$ in $\widetilde{k}[\widetilde{t}]$, there exists a lifting $f = gh$ with $\widetilde{g} = \overline{g}$ and $\deg(g) = \deg(\overline{g})$.

(iii) Any $f \in k^\circ[t]$ splits as $f = gh$ with $|h - 1| < 1$ and $\deg(g) = \deg(\widetilde{g})$.

(iv) For any $f \in k^\circ[t]$ and a simple root $\overline{a} \in \widetilde{k}$ of $\widetilde{f}$ there exists a root $a \in k$ of f such that $\widetilde{a} = \overline{a}$.

(v) Any irreducible monic polynomial $f = t^d + a_1t^{d-1} + \ldots + a_d \in k[t]$ with $a_d \in k^\circ$ lies in $k^\circ[t]$.

(vi) Any irreducible monic polynomial $f = t^d + a_1t^{d-1} + \ldots + a_d \in k[t]$ satisfies $|a_i|^{1/i} \leq |a_d|^{1/d}$ for $1 \leq i \leq d$.

Proof. We can assume that the valuation is non-trivial since otherwise (i)–(vi) are automatically satisfied. Also, we record the obvious implications (vi)$\Longrightarrow$(v), (ii)$\Longrightarrow$(iv) and (ii)$\Longrightarrow$(iii), where the latter one is obtained by taking $\overline{h} = 1$.

Next, let us show that (i) implies everything else. If k is henselian, then (vi) is satisfied by Corollary 1.8.24. It remains to show that (i)$\Longrightarrow$(ii). Set $K = \widehat{k}$. By Hensel's lemma, there exists a required splitting $f = gh$ in $K[t]$, so we should only check that $g, h \in k[t]$. Recall that k is separably closed in K by Theorem 1.9.5(ii), and hence any irreducible polynomial $f \in k[t]$ splits in $K[t]$ as $f = g^{p^n}$, where g is irreducible and p is the characteristic exponent of k. In particular, it suffices to show that $(g, h) = 1$ because then the factorization $f = gh$ holds already in $k[t]$. Let $\alpha \in K^a$ be any root of g. Since $g = a_dt^d + \ldots$ with $|a_d| = 1$, it follows that $|\alpha| \leq 1$, and hence $\widetilde{\alpha}$ is a root of $\overline{g}$. By our assumption $\overline{h}(\widetilde{\alpha}) \neq 0$ and hence $h(\alpha) \neq 0$. This proves that $(g, h) = 1$, as required.

Now, we will show that if (i) fails, then all other claims fail too. Clearly, it suffices to deal with (iii), (iv) and (v). By Theorem 1.9.5, there exists $\alpha \in K \setminus k$ such that α is algebraic and separable over k. Set $l = k(\alpha)$ and let $L_1, \ldots, L_n$ be all completions of l with respect to the extended valuations. Moreover, we can take the first valuation $|\ |_1$ to be the one induced by the obvious embedding $i \colon l \hookrightarrow K$ and then $L_1 = K$. For a sequel use, we also extend $|\ |_1$ from l to k^a in an arbitrary way. Since l/k is separable, $l \otimes_k K$ is reduced and hence $l \otimes_k K = \prod_{i=1}^n L_j$ by Theorem 1.8.7. By the weak approximation theorem, see Theorem 1.8.14, there exists $a \in l$ such that $|a|_1 < 1$ and $|a-1|_j < 1$ for $2 \le j \le n$.

Set $a_1 = i(a) \in K$, let $a_1, \dots, a_d \in K^a$ be all conjugates of a_1 over k, and let $\sigma_j \colon k(a) \hookrightarrow K^a$ be the k-embedding sending a to a_j. Then $\sigma_1 = i|_{k(a)}$ induces the valuation $|\ |_1$ on $k(a)$ and for any $j > 1$ the induced valuation is one of $|\ |_2, \dots, |\ |_n$. In particular, this implies that $|a_j - 1|_1 < 1$ for $j > 1$. It follows that the minimal polynomial $f_a = \prod_{j=1}^d (t - a_j)$ of a satisfies $\widetilde{f_a} = \widetilde{t}(\widetilde{t} - 1)^{d-1}$, and hence the irreducible polynomial $f_a \in k[t]$ violates (iv).

In the same fashion, we can fix $\pi \in k$ with $|\pi| = r > 1$ and find $b = b_1 \in l$ such that $|b|_1 < r^{1-[l:k]}$ and its conjugates $b_2, \dots, b_d \in k^a$ satisfy $|b_j - \pi|_1 < r$. In this case, the minimal polynomial f_b is of the form $t^d + \dots + et + c$ with $|e| = |b_2 \dots b_d| = r^{d-1} > 1$ and $|c| = |b_1 \dots b_d| < r^{d-[l:k]} \le 1$, hence f_b violates (v). Finally, its rescaling $g = (b_2 \dots b_d)^{-1} f_b = (t - b_1) \prod_{j=2}^d (1 - b_j^{-1} t)$ satisfies $\widetilde{g} = \widetilde{t}$ because $\widetilde{b_1} = \widetilde{b_j^{-1}} = 0$. In particular, the irreducible polynomial g violates (iii). $\square$

1.10. **Basic properties of analytic spectrum.**

1.10.1. *Spectral seminorm.* For any seminormed ring A one defines the spectral seminorm ρ_A to be $\rho(a) = \liminf_n |a^n|^{1/n}$. Here some easy facts whose proof copies the well-known case from the classical functional analysis.

Exercise 1.10.2. (i) In fact, one even has that $\rho(a) = \lim_n |a^n|^{1/n}$, that is, the limit exists.

(ii) ρ_A is the maximal power-multiplicative seminorm on A dominated by $|\ |$, and ρ_A is non-archimedean if $|\ |$ is.

1.10.3. *The main theorem.* Here is the main theorem about Berkovich spectrum. It is a tremendous generalization of the theorem on extension of valuations and of the max norm formula. For the proof we refer to [Ber90, Theorems 1.2.1 and 1.3.1].

Theorem 1.10.4. *Let A be a seminormed ring and let $X = \mathcal{M}(A)$ denote its Berkovich spectrum. Then,*

(i) $X = \emptyset$ if and only if $A = 0$.

(ii) X is compact.

(iii) For any element $f \in A$ one has that $\rho(f) = \max_{x \in X} |f|_x$.

2. Valuations and valued fields

2.1. **Ordered groups.**

2.1.1. *Multiplicative and additive notation.* We will usually work with ordered groups written multiplicatively, but sometimes additive notation will also be used. It is important to remember that for most of what follows the correct translation between the two languages is an analogue of $-\log$ rather than the usual logarithm. The minus sign is responsible for numerous sign inversion that require some care, but it is this way that makes the theory of valuations most intuitive.

2.1.2. *Ordered groups.* In this notes an *ordered group* always means a totally ordered abelian group $(G, \leq)$, that is, an abelian group G provided with a total order $<$ such that if $a_1 \leq b_1$ and $a_2 \leq b_2$, then $a_1b_1 \leq a_2b_2$. After the trivial case $G = 1$, the main example is the group $\mathbb{R}^\times_{>0}$ of positive real numbers. On the additive side it corresponds to $\mathbb{R}$.

2.1.3. *Augmentation.* Sometimes it will be convenient to augment an ordered group G to an ordered monoid $\overline{G} = \{0\} \cup G$, by adding a minimal element 0 such that $0 \cdot G = 0$. By our convention, in the additive case, we augment ordered groups $(A, +)$ by maximal elements ∞.

2.1.4. *Lexicographic order.* For most of applications of this paper we will only the groups $(\mathbb{R}^\times_{>0})^n$ (or $\mathbb{R}^n$) provided with the lexicographic order and their subgroups. Nevertheless one can extend this construction as follows:

Exercise 2.1.5. Assume that $\{G_i\}_{i \in I}$ is a family of ordered groups indexed by a totaly ordered set I.

(i) Define a natural lexicographic order on $\oplus_{i \in I} G_i$ and show that it becomes an ordered group.

(ii) Assuming that I is well ordered (that is, any subset of I possesses a minimal element), define a natural lexicographic order on $\prod_{i \in I} G_i$ and show that it becomes an ordered group.

2.1.6. *Cuts.* For any $a \in G$ let $G_{\geq a}$, $G_{>a}$, $G_{\leq a}$ and $G_{<a}$ denote the subset of all elements $x \in G$ such that $x \geq a$, $x > a$, $x \leq a$ and $x < a$, respectively.

Lemma 2.1.7. *Let G be an ordered group, then*

(i) If $\rhd$ is any relation from the set $\{<, >, \leq, \geq\}$ and $a_1, a_2, b_1, b_2 \in G$ satisfy $a_1 \rhd b_1$, $a_2 \rhd b_2$, then also $a_1b_1 \rhd a_2b_2$ is satisfied. In particular, the opposite order on G also defines an ordered group.

(ii) G is torsion free.

(iii) The set $G_{\leq 1}$ is a monoid and the sets $G_{\leq a}$ and $G_{<a}$ with $a \leq 1$ are ideals of $G_{\leq 1}$. The same is true for opposite inequalities.

Proof. Exercise. $\square$

Exercise 2.1.8. (i) Prove the lemma.

(ii) Show that ideals of $G_{\leq 1}$ are nothing else but *cuts*, that is, subsets I such that if $a \leq b$ and $b \in I$, then $a \in I$.

(iii) Show that $\mathbb{R}^\times$ and $\mathbb{C}^\times$ cannot be provided with an order.

2.1.9. *Divisible hull.* Let G be a torsion free group. In additive notation, $G \otimes_{\mathbb{Z}} \mathbb{Q}$ is the divisible hull of G, while in the multiplicative case we will use the notation $\sqrt{G}$. For example, if $G \subseteq \mathbf{R}^{\times}_{>0}$ then $\sqrt{G}$ is literally the set of all positive roots of elements of G.

Lemma 2.1.10. *If G is an ordered group, then the order extends to $\sqrt{G}$ uniquely.*

Proof. For $x, y \in \sqrt{G}$ there exists $n > 0$ such that $x^n, y^n \in G$ and then any extension of the order satisfies $x < y$ if and only if $x^n < y^n$. This shows that there is at most one extension, and one checks straightforwardly that this receipt does define an order on $\sqrt{G}$. $\square$

2.1.11. *Convex subgroups.* A subgroup H of an ordered group G is called *convex* if for any interval $I = [a, b]$ in G with $a, b \in H$ one has that $I \subseteq H$. Convex subgroups are analogs of normal subgroups in the theory of groups as the following simple result shows.

Exercise 2.1.12. Let H be a subgroup of an ordered group G.

(i) Show that H is convex if and only if for any $x \in H$ with $x \leq 1$, the interval $[x, 1]$ lies in H.

(ii) Show that H is convex if and only if for any pair of cosets xH, yH the same relation $x' \rhd y'$ with $\rhd \in \{<, >, =\}$ is satisfied for any $x' \in xH$ and $y' \in yH$. In particular, the order induces a structure of an ordered group on the quotient G/H if and only if H is convex.

2.1.13. *Composed order.* One can also compose order from short exact sequences. This reverses the above construction and generalizes lexicographic order on products $G_1 \times G_2$.

Exercise 2.1.14. Let $H \subseteq G$ be abelian groups and assume that H and G/H are ordered. Show that there exists a unique order on G such that H becomes a convex subgroup and the order on G/H coincides with the order induced from G.

2.1.15. *Comparable elements.* Let $x, y > 1$ be two elements of an ordered group G. We say that x *dominates* y and denote $y \prec x$ if $x \succ y^n$ for any n. We say that x and y are *comparable* and denote $x \sim y$ if neither of them dominates the other. Let Z (resp. Z') be the set of elements $z \in G_{>1}$ such that $z \prec x$ (resp. $z \preceq x$), and set $G_{\prec x} = Z \cup \{e\} \cup Z^{-1}$ and $G_{\preceq x} = Z' \cup \{e\} \cup Z'^{-1}$.

Lemma 2.1.16. *Let G be an ordered group and $x > 1$ an element of G. Then $G_{\prec x}$ and $G_{\preceq x}$ are convex subgroups of G.*

Proof. Straightforward. $\square$

2.1.17. *Height of ordered groups. Height* $\mathrm{ht}(G)$ of an ordered group G is the cardinal of the set of its proper convex subgroups. Other names often appearing in the literature are *rank* or a *convex rank.*

Exercise 2.1.18. (i) The set of convex subgroups of G is totally ordered by inclusion.

(ii) A totally ordered set I is the set of convex subgroups of some ordered group G if and only if all cuts in I are principal (that is, of the form $I_{\leq a}$ or $I_{\geq a}$).

(iii) Let G be an ordered group with a convex subgroup H and ordered quotient G/H. Then $\mathrm{ht}(G) = \mathrm{ht}(H) + \mathrm{ht}(G/H)$.

(iv) Find the height of $\mathbb{R}^n$ provided with the lexicographic order.

(v) Show that $\mathrm{ht}(G) = n < \infty$ if and only if $n+1$ is the maximal length of a chain $x_0 = 1 < x_1 \prec x_2 \prec \dots$.

(vi) If $H \hookrightarrow G$ is an embedding of ordered groups and G/H is torsion, then the map $\Gamma \mapsto \Gamma \cap H$ induces a bijection between the sets of convex subgroups of G and H.

For convenience, we formulate the following result using additive notation.

Lemma 2.1.19. *Any ordered group $(A, +)$ of height $n < \infty$ can be embedded as an ordered subgroup into $\mathbb{R}^n$.*

Proof. The case $n = 0$ is obvious. If $n = 1$, then fix any $x \in G_{>0}$. For any y consider the sets of rational numbers $S_y^- = \{\frac{m}{n} | \ mx < ny\}$ and $S_y^+ = \{\frac{m}{n} | \ mx > ny\}$. Both are non-empty because A has no non-trivial convex subgroups and hence $G_{\prec x} = 0$ and $G_{\preceq x} = G$. Clearly, $S_y^\pm$ are convex and their union omits at most one element of $\mathbb{Q}$, hence they define a real number r_y as a Dedekind cut. It is now straightforward to check that sending y to r_y defines an ordered embedding $G \to \mathbb{R}$.

Now, we will act by induction on n. First, it follows from Exercise 2.1.18(v) that the divisible $G_\mathbb{Q}$ (see Lemma 2.1.10) also has height n. Therefore it suffices to embed $G_\mathbb{Q}$ into $\mathbb{R}^n$, and we can assume that G is divisible. Since $n > 1$, there exists a non-proper convex subgroup H. Then $\mathrm{ht}(H) = l \in \{1, \dots, n-1\}$ and $\mathrm{ht}(G/H) = n - l$ by Exercise 2.1.18(iii). Since G/H is ordered, it is torsion free and hence G is divisible and we obtain a non-canonical splitting $G \xrightarrow{\sim} G/H \oplus H$. We claim that the order corresponds to the lex order on the target. Indeed, $x < y$ in G if and only if the images x_h, y_h in H satisfy $x_h < y_h$, and if $x_h = y_h$, then $x - x_h < y - x_h$ in H (where we view x_h as an element of G via the splitting $G/H \hookrightarrow G$). By induction, $H \hookrightarrow \mathbb{R}^l$ and $G/H \hookrightarrow \mathbb{R}^{n-l}$, so their lex sum embeds into $\mathbb{R}^n$. ☐

Remark 2.1.20. In fact, we already proved that if G is of height one, then for $x \in G_{>0}$ there exists unique ordered embedding $G \hookrightarrow \mathbb{R}$ sending x to 1.

2.2. **Valuations.**

2.2.1. *Multiplicative semivaluations and valuations.* In the definition of non-archimedean real-valuations one only uses multiplication and order on $\mathbb{R}$, while addition plays no role. Therefore, this notion extends as follows: a *semivaluation* on a ring A is a multiplicative homomorphism $| \ |\colon A \to \overline{\Gamma} = \Gamma \cup \{0\}$, where $\Gamma = (\Gamma, \cdot)$ is an ordered group, and $|a + b| \geq \max(|a|, |b|)$ for any $a, b \in A$. The kernel of $| \ |$ is a prime ideal, and a semivaluation with a trivial kernel is called a *valuation*.

2.2.2. *Additive valuations.* Additive valuations are defined similarly, but this time $\Gamma = (\Gamma, +)$ is an additive ordered group, $\overline{\Gamma} = \Gamma \cup \{\infty\}$, and the strong triangle inequality is reversed to $\nu(a + b) \geq \min(\nu(a), \nu(b))$. Naturally, additive valuations are denoted like $\nu\colon A \to \overline{\Gamma}$ rather than $| \ |$. As we remarked earlier, they should be thought off as $-\log$ of multiplicative ones.

2.2.3. *Group of values.* By an abuse of notation, for a semivaluation $| \ |\colon A \to \overline{\Gamma}$ we denote by $|A|$ the subgroup of Γ generated by $\mathrm{Im}(| \ |) \setminus \{0\}$. In most of the notes A will be a field, and then we will use the non-abused notation $|A^\times|$ instead.

2.2.4. *Equivalence of valuations.* Since the group Γ is not fixed in the theory of general valuations, the natural notion of equivalence also plays with Γ. Namely, semivaluations $|\ |\colon A\to\overline{\Gamma}$ and $|\ |'\colon A\to\overline{\Gamma}'$ are called *equivalent* if there is an isomorphism of ordered groups $\phi\colon |A|\xrightarrow{\sim}|A|'$ such that $|\ |'=\phi\circ|\ |$.

Remark 2.2.5. The smallest element $|\ |\colon A\to|A|\cup\{0\}$ of the equivalence class is unique up to an isomorphism, and it encodes the information we really care of. Nevertheless, it is often convenient to consider semivaluations with a larger Γ. For example, this was the case of real semivaluations. In addition, in order to extend a valuation through finite field extensions one might want to extend Γ as well.

2.2.6. *Height of valuations.* By *height* or *convex rank* of a semivaluation we mean the height of the ordered group $|A|$.

Lemma 2.2.7. *A semivaluation $A\to\overline{\Gamma}$ is equivalent to a real semivaluation if and only if its height does not exceed one.*

Proof. By Lemma 2.1.19, $|A|$ embeds into $\mathbf{R}^\times_{>0}$ if and only if its height is at most one. The lemma follows. $\square$

2.2.8. *Rational rank.* We also define the *rational rank* of a semivaluation to be the dimension of the (exponential) $\mathbb{Q}$-vector space $\sqrt{|A|}$.

Lemma 2.2.9. *If a semivaluation on a ring A is of finite height h, then its rational rank is at least h.*

Proof. This is a statement about the ordered group $\Gamma=|A|$. Let $\Gamma_0=0\subsetneq\Gamma_1\subsetneq\dots\subsetneq\Gamma_h=\Gamma$ be all isolated subgroups of Γ. For $i\in\{1,\dots,h\}$ choose $r_i\in\Gamma_i\setminus\Gamma_{i-1}$. Then $r_1,\dots,r_h$ are linearly independent because $r_i^n\in\Gamma_i\setminus\Gamma_{i-1}$ for any $i\in\{1,\dots,h\}$ and $n>0$. $\square$

Exercise 2.2.10. Show that the above claim fails for infinite ranks. (Hint: take $|A|$ of the form $\mathbb{Z}^{\mathbb{Q}}$ with lex order induced by $\mathbb{Q}$.)

2.2.11. *Discrete valuations.* A valuation on a field k is called *discrete* if $|k^\times|$ is a cyclic group. In particular, any such valuation is of height 1.

2.2.12. *Valued fields.* By a valued field we mean a field k provided with a valuation $|\ |\colon k\to\overline{\Gamma}$. Similarly to the real-valued case, we introduce the *ring of integers* $k^\circ=\{x\in k|\ |x|\le 1\}$, also called the *valuation ring* of k, and note that k° is a local ring with maximal ideal $k^{\circ\circ}=\{x\in k|\ |x|<1\}$ and residue field $\widetilde{k}=k^\circ/k^{\circ\circ}$.

2.3. **Extensions of valued fields.**

2.3.1. *The definition.* An extension of valued fields is an embedding $k\hookrightarrow l$ such that the restriction of $|\ |_l$ onto k is equivalent to $|\ |_k$. Clearly, this happens if and only if the extension respects the associated valuation rings, that is, $k^\circ=k\cap l^\circ$. For any such extension, $k^\circ\hookrightarrow l^\circ$ is a local homomorphism (that is, $k^{\circ\circ}\hookrightarrow l^{\circ\circ}$), hence an extension of residue fields $\widetilde{k}\hookrightarrow\widetilde{l}$ arises. In addition, an embedding of group of values $|k^\times|\hookrightarrow|l^\times|$ is well defined up to a unique isomorphism.

2.3.2. *The invariants $f_{l/k}$ and $e_{k/l}$.* The most basic way to study an extension l/k of valued fields is via the induced extensions $|l^\times|/|k^\times|$ and $\widetilde{l}/\widetilde{k}$. In particular, we define the cardinals $f_{l/k} = [\widetilde{l} : \widetilde{k}]$ and $e_{l/k} = \#(|l^\times|/|k^\times|)$. They are analogues of the degree of an extension.

Lemma 2.3.3. *Assume that l/k is an extension of valued fields, $A = \{a_i\}_{i\in I}$ is a family of elements of $l^\times$ such that the map $A \to |l^\times|/|k^\times|$ is injective, and $B = \{b_j\}_{j\in J}$ is a family of elements of k° such that the reduction family $\widetilde{B} = \{\widetilde{b}_j\}_{j\in J}$ of elements of $\widetilde{l}$ is linearly independent over $\widetilde{k}$. Then the family $AB = \{a_ib_j\}_{i\in I, j\in J}$ is orthogonal over k. In particular, it is linearly independent over k.*

Proof. Assume, conversely that there is a linear combination $s = \sum_{i\in I', j\in J'} s_{ij}$ with $|s| < r = \max_{i,j} |s_{ij}|$, where $s_{ij} = a_ib_jc_{ij}$ for $c_{ij} \in k$ and finite $I' \subseteq I$, $J' \subseteq J'$. Fix $i_0 \in I', j_0 \in J'$ such that $r = |s_{i_0j_0}|$. Then $r \in |a_{i_0}|\cdot|k^\times|$ and by our assumption on A, if a pair $(i,j) \in I' \times J'$ satisfies $r = |s_{ij}|$, then necessarily $i = i_0$. It follows that already $s_{i_0} = \sum_{j\in J'} s_{i_0j}$ satisfies $|s_{i_0}| < r$.

By our assumption, $\widetilde{b}_j \neq 0$ and hence $|b_j| = 1$. Dividing s_{i_0} by $a_{i_0}c_{i_0j_0}$ we obtain a linear combination $s' = \sum_{j\in J'} c'_jb_j$ such that $c'_j = c_{i_0j}/c_{i_0j_0} \in k^\circ$, $c'_{j_0} = 1$, and $|s'| < 1$. It follows that the reduction $0 = \sum_{j\in J'} \widetilde{c}'_j\widetilde{b}_j$ yields a non-trivial linear dependence on $\widetilde{B}$, a contradiction. □

2.3.4. *Fundamental inequality.* As an easy corollary of the previous lemma we obtain a bound on e and f in terms of the degree. This is often called the fundamental inequality. Note that we prove it for cardinals rather than for finite numbers.

Corollary 2.3.5. *Any extension of valued fields l/k satisfies the inequality*

$$e_{l/k}f_{l/k} \leq [l : k].$$

Proof. Choose any basis $\overline{B}$ of $\widetilde{l}$ over $\widetilde{k}$ and lift it to a family $B \subset l$, and choose any family $A \subset l^\times$ which maps bijectively onto $|\widetilde{l}^\times|/|\widetilde{k}^\times|$. The family AB is linearly independent over k by Lemma 2.3.3, hence $[l : k] \geq |AB| = e_{l/k}f_{l/k}$. □

2.3.6. *The invariants $F_{l/k}$ and $E_{k/l}$.* One can also define analogues of transcendence degrees as follows: $F_{l/k} = \mathrm{tr.deg.}(\widetilde{l}/\widetilde{k})$ and $E_{l/k} = \dim_{\mathbb{Q}}(\sqrt{|l^\times|}/\sqrt{|k^\times|})$. In addition, we will denote the rational rank of k by E_k.

Lemma 2.3.7. *Assume that l/k is an extension of valued fields, $A = \{a_i\}_{i\in I}$ is a family of elements of $l^\times$ such that the images of a_i in $\sqrt{|l^\times|}/\sqrt{|k^\times|}$ are linearly independent over $\mathbb{Q}$, and $B = \{b_j\}_{j\in J}$ is a family of elements of k° such that the reduction family $\widetilde{B} = \{\widetilde{b}_j\}_{j\in J}$ is algebraically independent over $\widetilde{k}$. Then the family of monomials $\prod_{i\in I'} a_i^{n_i} \cdot \prod_{j\in J'} b_j^{m_j}$ in l is orthogonal over k. In particular, the homomorphism $k[A \cup B] \to l$ is injective and the family $A \cup B$ is algebraically independent over k.*

Proof. The argument is essentially the same as in the proof of Lemma 2.3.3, so we outline main points. First, one assumes that there is a linear combination $s = \sum_{n,m} c_{nm}a^nb^m$ of monomials $a^n = \prod a_i^{n_i}$, $b^m = \prod b_j^{m_j}$ with coefficients $c_{mn} \in k$ such that $|s| < r = \max_{n,m} |s_{nm}|$ for $s_{nm} = c_{nm}a^nb^m$. Fix m_0, n_0 so that $|s_{n_0m_0}| = r$. By our assumption on $|A|$, if $|s_{nm}| = |s_{n_0m_0}|$, then necessarily $n = n_0$. It follows that already $s_{n_0} = \sum_m s_{n_0m}$ satisfies $|s_{n_0}| < r$. Dividing by $c_{n_0m_0}a^{n_0}$

we obtain a linear combination $s' = \sum_m c'_m b^m$ such that $c'_m \in k^\circ$, $c'_{m_0} = 1$ and $|s'| < 1$. Therefore, the reduction $0 = \sum_m \widetilde{c}'_m \widetilde{b}^m$ provides a non-trivial algebraic dependency on $\widetilde{B}$, a contradiction. $\square$

Remark 2.3.8. The notation $e_{l/k}$ and $f_{l/k}$ are classical. There is no usual notation for the transcendental invariants, so we choose notation which stresses the analogy and indicates that the transcendental invariants measure larger extensions.

2.3.9. *Abhyankar's inequality.* Again, as a corollary we obtain a bound on the invariants, but this time in terms of the transcendence degree. This result is often called Abhyankar's inequality.

Corollary 2.3.10. *Any extension of valued fields l/k satisfies the inequality $F_{l/k} + E_{l/k} \le \mathrm{tr.deg.}(l/k)$ of cardinals.*

Proof. Choose any transcendence basis $\overline{B}$ of $\widetilde{l}$ over $\widetilde{k}$ and lift it to a family $B \subset l$, and choose any family $A \subset l^\times$ which maps bijectively onto a $\mathbb{Q}$-basis of $\sqrt{|l^\times|}/\sqrt{|k^\times|}$. The family $A \cup B$ is algebraically independent over k by Lemma 2.3.3, hence $\mathrm{tr.deg.}(l/k) \ge |A \cup B| = E_{l/k} + F_{l/k}$. $\square$

2.3.11. *Algebraic extensions.* As an application, we obtain the following result for algebraic extensions. In particular, $E_{l/k} = F_{l/k} = 0$ algebraic extensions, hence we obtain the following result.

Corollary 2.3.12. *if l/k is an algebraic extension of valued fields, then $\widetilde{l}/\widetilde{k}$ is an algebraic extension and $|l^\times|/|k^\times|$ is a torsion group. In particular, the map $\mathrm{Conv}(|l^\times|) \to \mathrm{Conv}(|k^\times|)$ is a bijection and $\mathrm{ht}(k) = \mathrm{ht}(l)$.*

Proof. The first claim is equivalent to the equalities $E_{l/k} = F_{l/k} = 0$, which hold by Anhyankar's inequality. The second claim follows from Exercise 2.1.18 (vi). $\square$

2.3.13. *Transcendental defect.* If $\mathrm{tr.deg.}(l/k)$ is finite, then we define the *transcendental defect* of l/k to be $D_{l/k} = \mathrm{tr.deg.}(l/k) - E_{l/k} - F_{l/k}$. By Abhyankar's inequality this is a non-negative number.

2.3.14. *Transitivity of invariants.* Multiplicativity and additivity of usual invariants, such as degree and transcendence degree, imply the following result.

Lemma 2.3.15. *Assume that $m/l/k$ is a tower of extensions of valued fields. Then $f_{m/k} = f_{m/l}f_{l/k}$, $e_{m/k} = e_{m/l}e_{l/k}$, $F_{m/k} = F_{m/l} + F_{l/k}$, $E_{m/k} = E_{m/l} + E_{l/k}$, and $E_l = E_k + E_{l/k}$. If $\mathrm{tr.deg.}(l/k) < \infty$, then also $D_{m/k} = D_{m/l} + D_{l/k}$.*

Corollary 2.3.16. *Assume that k is a valued field which has a finite transcendence degree n over its prime subfield. Then $\mathrm{ht}(k) \le E_k \le n + 1$.*

Proof. We have proved the first inequality in Lemma 2.2.9. If l is the prime subfield of k, then $E_l \le 1$ by Ostrowski's classification. Therefore, by Abhyankar's inequality and the above lemma $E_k = E_l + E_{l/k} \le 1 + n$. $\square$

Corollary 2.3.17. *Any valued field k is a filtered limit of valued subfields of finite height.*

Proof. Clearly, k is the filtered union of subfields k_i finitely generated over the prime subfield of k. By the above corollary $\mathrm{ht}(k_i) < \infty$. $\square$

2.3.18. *Immediate extensions.* An extension l/k is called *immediate* if $\widetilde{k} = \widetilde{l}$ and $|\widetilde{k}^\times| = |\widetilde{l}^\times|$. In other words, $e_{l/k} = f_{l/k} = 1$. More generally, we say that l/k is *transcendentally immediate* if $\widetilde{l}/\widetilde{k}$ is algebraic and $|\widetilde{l}^\times|/|\widetilde{k}^\times|$ is torsion. In other words, $E_{l/k} = F_{l/k} = 0$.

Example 2.3.19. (i) If $m/l/k$ is a tower of extensions of valued fields, then m/k is immediate (resp. transcendentally immediate) if and only if m/l and l/k are so.

(ii) The completion $\widehat{k}/k$ of a real valued field is an immediate extension.

(iii) Any algebraic extension is transcendentally immediate.

2.3.20. *Invariants of the algebraic closure.* Naturally, maximal algebraic extension of a valued field induces a maximal algebraic extension of the residue field and group of values.

Lemma 2.3.21. *(i) If l is an algebraically closed valued field, then the residue field $\widetilde{l}$ is algebraically closed and the group of values $|l^\times|$ is divisible.*

(ii) If k is a valued field and $l = k^a$ is provided with an extension of the valuation of k, then $\widetilde{l} = (\widetilde{k})^a$ and $|l^\times| = \sqrt{|k^\times|}$.

Proof. Since $l^\times$ is divisible, its image $|l^\times|$ is also divisible. The field $\widetilde{l}$ is algebraically closed because any polynomial $\overline{f}(t) \in \widetilde{l}[t]$ can be lifted to a polynomial $f(t) \in l^\circ[t]$ of the same degree, and then any root $\alpha \in l$ of $f(t)$ satisfies $|\alpha| \leq 1$, and hence $\widetilde{\alpha} \in \widetilde{l}$ is a root of $\overline{f}$. We have proved (i), and combining it with Corollary 2.3.12 one also obtains (ii). $\square$

2.4. **Valuation rings.** In this section we will see that the ring k° determines the valuation and study its basic properties.

2.4.1. *The definition.* A *valuation ring* is an integral domain R such that for any $c \in \mathrm{Frac}(R) \setminus R$ one has that $c^{-1} \in R$. If K is a field and $R \subseteq K$ is a valuation ring such that $\mathrm{Frac}(R) = K$, then one says that R is *a valuation ring of* K. There is an enormous amount of equivalent characterizations of this property, and for now we list few most basic ones.

Lemma 2.4.2. *Let R be a domain with fraction field K. Then the following properties are equivalent:*

(i) R is a valuation ring.

(ii) For any $a, b \in R$ either $a|b$ or $b|a$.

(ii)' For any $a, b \in K$ either $a|b$, in the sense that $b \in aR$, or $b|a$.

(iii) The divisibility relation induces a total order on the group $K^\times/R^\times$.

(iv) The set of principal ideals of R is totally ordered by inclusion.

(iv)' The set of all ideals of R is totally ordered by inclusion.

(v) R is local and any finitely generated ideal in R is principal.

Proof. Clearly, (i)$\Longleftrightarrow$(ii)', and this is also equivalent to (ii) because any $c \in K$ is of the form a/b. In addition, (ii) is clearly equivalent to (iii) and (iv). Obviously, (iv)'$\Longleftrightarrow$(iv). Conversely, assume that (iv) holds but (iv)' fails, say I and J are two ideals not contained one in another. Choose $a \in I \setminus J$ and $b \in J \setminus I$. Then either $a \in (b) \subseteq J$ or $b \in (a) \subseteq I$, a contradiction.

It remains to prove that (ii)$\Longleftrightarrow$(iv). Assume (ii) holds. If $I = (a_1, \ldots, a_n)$ is a finitely generated ideal, then one a_i divides all the rest by and hence $I = (a_i)$. In addition, if a, b are non-invertible, then one of them divides the sum $a + b$, and hence $a + b \neq 1$. This proves that R is local. Conversely, assume that (v) holds. For any pair a, b the ideal (a, b) is principal, say $(a, b) = (c)$. Hence $(\frac{a}{c}, \frac{b}{c}) = (1)$, and since R is local, this implies that either $\frac{a}{c}$ or $\frac{b}{c}$ is a unit u. This proves that either $(a, b) = (a)$ and then $a|b$, or $(a, b) = (b)$ and then $b|a$. $\square$

The following corollary is an analogue of the fact that a norm on a vector space is determined by its unit ball.

Corollary 2.4.3. *For any field k there is a one-to-one correspondence between valuation rings of k and equivalence classes of valuations on k.*

Proof. If k is provided with a valuation, then k° is a obviously a valuation ring of k which depends only on the equivalence class of the valuation. Conversely, if R is a valuation ring of k, then $\Gamma = k^\times / R^\times$ is an ordered group by Lemma 2.4.2. The induced map $|\ |\colon k \to \overline{\Gamma}$ satisfies the strong triangle inequality because for any $a, b \in K$ either $a|b$ or $b|a$ and hence either a or b divides $a + b$. Thus, $|\ |$ is a valuation, and it is a straightforward check that the above constructions are inverse one to another. $\square$

Remark 2.4.4. The above corollary allows one to view a valued field as a field k with a fixed valuation ring k° of k. In particular, extensions of valued fields are precisely extensions l/k that agree with the valuation rings in the sense that $k^\circ = k \cap l^\circ$. In particular, the valuation induced on a subfield F of k is described by the ring $F \cap k^\circ$, which is obviously a valuation ring.

2.4.5. *Spectrum.* Recall that an ideal in a monoid M is a subset I such that $MI = I$. As for rings, an ideal is prime if and only if $S = M \setminus I$ is closed under multiplication. In particular, S is non-empty, but I can be empty.

Lemma 2.4.6. *If k is a valued field with group of values $\Gamma = |k^\times|$, then $|\ |$ induces a bijection between ideals of k° and ideals of the monoid $\Gamma_{\le 1}$. Furthermore, an ideal $I \subseteq k^\circ$ is prime if and only if the ideal $|I| := \{|x|\colon\ 0 \neq x \in I\}$ is prime in $\Gamma_{\le 1}$, and the latter happens if and only if $|I| = \Gamma_{\le 1} \setminus \Gamma'$ for a convex subgroup $\Gamma' \subseteq \Gamma$.*

Proof. Exercise. $\square$

2.4.7. *Coarsening of a valuation.* Let R be a valuation ring with field of fractions K and induced valuation $|\ |\colon K \twoheadrightarrow \overline{\Gamma}$. Any convex subgroup $\Gamma_v \subsetneq \Gamma$ with quotient $\Gamma^v = \Gamma/\Gamma_v$ gives rise to a composed valuation $|\ |^v\colon K \to \overline{\Gamma} \to \overline{\Gamma}^v$. This valuation looses information, so we call it the *coarsening* of $|\ |$ associated with the quotient Γ^v of Γ. The valuation ring R^v of $|\ |^v$ is obtained by inverting the multiplicative set S_v all elements $x \in R$ with $|x| \in \Gamma_v$. Note that $p_v = R \setminus S_v$ is the prime ideal corresponding to Γ_v.

Conversely, any *overring* of R, that is a ring A with $R \subseteq A \subseteq K$, is a valuation ring and the associated group of values $K^\times/A^\times$ is a quotient of $\Gamma = K^\times/R^\times$. So, combining these constructions with Lemma 2.4.6 we obtain the following result, where orders of involved sets can be increasing or decreasing.

Lemma 2.4.8. *Let K be a valued field with ring of integers R and group of values Γ. Assigning $|\ |^v$, R^v, S_v and p_v to a convex subgroup $\Gamma_v \subseteq \Gamma$ gives rise to bijections between the ordered sets of*

(1) *convex subgroups of Γ,*

(2) *coarsenings of* $|\ |$,
(3) *overrings of* R,
(3') *localizations of* R,
(4) *multiplicative subsets* $S \subseteq R \setminus \{0\}$ *such that if* $x|y$ *and* $y \in S$ *then* $x \in S$,
(5) *prime ideals of* R.

2.4.9. *The overring criterion.* Using overrings one can provide a non-trivial alternative description of valuation rings, which explains their geometric meaning. Recall that given a ring A and local subrings $A_i \subseteq A$, $i = 1, 2$ with maximal ideals m_i, one says that A_1 *dominates* A_2 if $A_2 \subseteq A_1$ and $m_2 = m_1 \cap A_2$.

Theorem 2.4.10. *Let R be a domain with field of fractions K. Then the following conditions are equivalent:*
(i) R is a valuation ring.
(ii) R is local and any overring of R in K is a localization of R.
(iii) R is a maximal local ring in K with respect to domination.

Proof. We know that (i)$\Longrightarrow$ by the previous paragraph. In addition, (ii)$\Longrightarrow$(iii) because any non-trivial localization of R inverts some elements of the maximal ideal and hence does not dominate R. To close the circle we will prove that if R is local with maximal ideal m, but R is not a valuation ring, then (iii) fails too. By Lemma 2.4.2, there exists elements $a, b \in R$ such that neither of them divides the other. Set $x = \frac{a}{b}$ and let $A = R[x]$ denote the R-subalgebra of K generated by x. By Corollary 2.4.14 that we will prove below, up to a switch of a and b we can assume that $mA \neq (1)$. Then the localization of A at mA is a local ring dominating R. Since $x \in A \setminus R$, we obtain that R is not maximal. $\square$

Before completing the proof we explain the geometric meaning of the argument and the main reason valuation rings show up in basic algebraic geometry. This remark assumes some familiarity with algebraic geometry.

Remark 2.4.11. (i) The reader might have noticed that the black box result whose proof we postponed is equivalent to the following: the blow up X' of $X = \mathrm{Spec}(R)$ along the non-principal ideal (a, b) is glued from the two charts $X'_a = \mathrm{Spec}(R[\frac{a}{b}])$ and $X'_b = \mathrm{Spec}(R[\frac{b}{a}])$, and our result simply claims that the closed point of X has a preimage in X', that is, m lifts to either $R[\frac{a}{b}]$ or $R[\frac{b}{a}]$. This is an absolutely standard claim in algebraic geometry since $X' \to X$ is projective and hence proper. However, the proof is in fact not so trivial. Harthorne's proof uses the valuative criterion, hence it is based on our Theorem 2.4.10 or its sibling. Grothendieck's proof in [Gro67] does no involve valuations, but uses quit a bit machinery on graded rings.

(ii) The main geometric property of valuation rings is that these are precisely local domains R such that $S = \mathrm{Spec}(R)$ does no possess non-trivial blow ups. Even more than that spectra of valuation rings are precisely the points of the birational topology generated by open covers and birational proper morphisms. In particular, these explains why they appear in valuative criteria. Valuations also lie in the basis of Zariski's and Nagata's approaches to birational geometry. We will expand on this topic later.

2.4.12. *Lifting ideals to overrings.* The result we have used about lifting of ideals is based on the following

Lemma 2.4.13. *Assume that R is a domain with field of fractions K, and $x \in K^\times$ is an element not integral over R. Then $A = R[x^{-1}]$ contains a maximal ideal n such that $x^{-1} \in n$, and for any such ideal $n \cap R$ is a maximal ideal of R.*

Proof. Note that $x \notin A$ because otherwise $x = \sum_{i=0}^n a_i x^{-i}$ and multiplying by x^n we obtain an integral equation for x over R. Thus x^{-1} is not invertible in A, and hence lies in a maximal ideal $n \subseteq A$. So A/n is a field, and since $x^{-1} \in n$, we have that $A/n = R/(n \cap R)$, and hence $n \cap R$ is a maximal ideal. □

Corollary 2.4.14. *Assume that (R, m) is a local domain with field of fractions K, and $x \in K^\times$ is an element. Then either $mR[x] \neq (1)$ or $mR[x^{-1}] \neq (1)$.*

Proof. If x is integral over R, then $R[x]$ is a finite R-module, and hence $mR[x] \neq R[x]$ by Nakayama's lemma. If x is not integral over R, then by Lemma 2.4.13 $A = R[x^{-1}]$ contains a maximal ideal n such that $n \cap R$ is a maximal ideal of R, and hence coincides with m. In particular, $mA \neq (1)$. □

2.4.15. *Valuation rings and the integral closure.* As an application, we can now prove the following important result.

Theorem 2.4.16. *Let K be a field and $A \subseteq K$ a subring with the integral closure $B = \mathrm{Nor}_K(A)$ in K. Then*

(i) B coincides with the intersection of all valuation rings of K containing A.

(ii) If A is local, then B coincides with the intersection of all valuation rings of K dominating A.

Proof. Any valuation ring R is integrally closed. Indeed, if $x \in \mathrm{Frac}(R) \setminus R$ satisfies $x^d + a_1 x^{d-1} + \ldots + a_d = 0$ with $a_i \in R$, then $|x| > 1$ and $|a_i| \leq 1$ for the induced valuation, and this implies that $|x^d| > |a_i x^i|$ for $1 \leq i \leq d$, which is impossible. As a consequence we obtain that the intersections of the valuation rings in the theorem contain $\mathrm{Nor}_K(A)$.

To prove the converse we should show that if $x \in K$ is not integral over A, then there exists a valuation ring of K containing or dominating A, respectively, and such that $x \notin A$. By Lemma 2.4.13 there exists a maximal ideal n of $A[x^{-1}]$ such that $x \notin n$, and then $m = n \cap A$ is a maximal ideal of A. Let A' be the localization of $A[x^{-1}]$ at n and $m' = nA'$ its maximal ideal. Then (A', m') is a local ring such that $x^{-1} \in m'$ and A' contains or dominates A, respectively. By Theorem 2.4.10 there exists a valuation ring R of K which dominates A'. Then R contains or dominates A, and x^{-1} lies in the maximal ideal of R and hence $x \notin R$. □

2.5. **Independence and extension of valuations.**

2.5.1. *Two valuations.* Let $|\ |_1$ and $|\ |_2$ be two valuation an a field K with associated valuation rings R_i and groups of values Γ_i. Let $R = R_1 R_2$ denote the subring of K generated by R_1 and R_2. If $R = K$, then one says that $|\ |_1$ and $|\ |_2$ are *independent*. By Lemma 2.4.6, the valuation $|\ |$ associated with R is the finest joint coarsening of $|\ |_i$. In particular, for any $a \in K$ the images of $|a|_1$ and $|a|_2$ in $\Gamma = |K^\times|$ are equal, which is a non-trivial compatibility condition if $R \neq K$. We will later see that this is the only restriction, so a general pair is "maximally independent up to a natural constraint".

Lemma 2.5.2. *Keep the above notation and let G_i be the kernels of $\Gamma_i \to \Gamma$. Then for any $g_i \in G_i$ there exists $a \in K$ such that $|a|_1 \geq g_1$ and $|a|_2 \leq g_2$.*

Proof. First assume that $g_1 > 1$, $g_2 = 1$. Choose any $x \in K$ with $|x|_1 = g_1$, then $x \in R$ and hence $x = \sum_{i=1}^n a_i b_i$ with $a_i \in R_1$, $b_i \in R_2$. Then there exists i such that $b = b_i$ satisfies $|b|_1 \ge g_1$. Replacing b by $b-1$, if needed, we preserve $|b|_1$ and achieve that $|b|_2 = 1$.

If $g_2 \ge 1$ we can take $a = b$. Otherwise, in the same way we find $c \in K$ such that $|c|_1 = 1$ and $|c|_2 \ge g_2^{-1}$ and set $a = b/c$. □

2.5.3. *Finitely many valuations.* To go further we should extend the above to finitely many valuations.

Lemma 2.5.4. *Assume that $R_1, \dots, R_n$ is a finite set of valuation rings of a field K such that neither of them contains the other, and let $|\ |_i \colon K^\times \twoheadrightarrow \Gamma_i$ be the associated valuations. Set $R'_i = R_1 R_i$ for $i \ge 2$ and $R'_1 = \cap_{i=2}^n R'_i$, and let $|\ |'_i \colon K^\times \twoheadrightarrow \Gamma'_i$ be the associated valuations and $G_i = \mathrm{Ker}(\Gamma_i \twoheadrightarrow \Gamma'_i)$. Then for any elements $g_i \in G_i$, $1 \le i \le n$ there exists $x \in K$ such that $|x|_1 \le g_1$ and $|x|_i \ge g_i$ for $2 \le i \le n$.*

Proof. Throughout the proof $i \in \{2, \dots, n\}$. By our assumptions $R_i \subsetneq R'_i$, hence G_i are non-trivial. Since $R_1 \subsetneq R'_i$, the rings R'_i are ordered by inclusion and hence R'_1 coincides with some R'_i. Therefore, G_1 is also non-trivial. Enlarging g_i and decreasing g_1 we can assume that $g_1 < 1$ and $g_i > 1$. By Lemma 2.5.2 there exist x_i such that $|x_i|_1 \le g_1$ and $|x_i|_i > g_i$. The same argument as in the proof of Theorem 1.8.14 shows that for generic enough $l_2, \dots, l_n > 0$ the element $x = \sum_{i=2}^n x_i^{l_i}$ satisfies $|x|_j = \max_{2 \le i \le n} |y_i^{l_i}|_j \ge g_j$ for $2 \le j \le m$. Clearly, $|x|_1 \le g_1$, hence x is as required. □

2.5.5. *The independence theorem.* Now we can prove a general independence result, which is an algebraic description of the ring $\cap_i R_i$ and its spectrum.

Theorem 2.5.6. *Let K be a field and let $R_1, \dots, R_n$ be valuation rings of K numbered so that $R_1, \dots, R_l$ are precisely the valuation rings from this set which are not contained in other ones. Then $R = \cap_{i=1}^n R_i$ is a semi-local ring, each prime ideal $m_i = m_{R_i} \cap R$ satisfies $R_{m_i} = R_i$, and m_i is prime if and only if $i \le l$. In particular, sending a prime ideal $p \subset R$ to R_p one obtains a bijection between* $\mathrm{Spec}(R)$ *and the set of valuation rings containing one of R_i.*

Proof. Let $i \in \{1, \dots, l\}$. We should prove that: (1) $R_i = R_{m_i}$, (2) m_i is maximal, (3) each maximal ideal $m \subset R$ is one of m_i. The rest follows since each R_j with $j > l$ is a localization of one of R_i with $i \le l$. In the sequel, we will only work with $R_1, \dots, R_l$. Without limitation of generality, it suffices to prove (1) and (2) for $i = 1$.

(1) Clearly $R_{m_1} \subseteq R_1$, so we should prove that any $x \in R_1$ also lies in R_{m_1}. Replacing x by $x+1$ if needed we can assume that $|x|_1 = 1$. In the terminology of Lemma 2.5.4 this implies that $|x|_i \in G_i$ for $i > 1$, hence by the same lemma there exists $t \in K$ such that $|t|_1 \le 1$ and $|t|_i \ge |x|_i$ for $i \in \{2, \dots, l\}$. In addition, G_i are non-trivial, hence we can also achieve that $|t|_1 < 1$ and $|t|_i > 1$ for $2 \le i \le l$. Set $s = \frac{1}{1+t}$, then $s \in R \backslash m_1$ and $|xs|_i \le 1$ for $1 \le i \le l$. In particular, $xs \in \cap_{i=1}^l R_i = R$ and $x = \frac{xs}{s} \in R_{m_1}$.

(2) We should prove that R/m_1 is a field, that is any $y \in R \setminus m_1$ is invertible modulo m_1. Applying the argument of (1) to $x = y^{-1} \in R_1$ one finds $s \in R$ such that $sx \in R$ and $|s-1|_1 < 1$. Then $sxy - 1 \in m_1$, and therefore sx is the inverse of y modulo m_1.

(3) Assume that m is a maximal ideal not contained in $\{m_1, \dots, m_l\}$. By Chinese remainder theorem there exists $x \in m \setminus \cup_{i=1}^l m_i$. Then $|x|_i = 1$ for $1 \le i \le l$, and hence $x \in \cap_{i=1}^l R_i^\times = R^\times$, a contradiction. $\square$

Remark 2.5.7. (i) The theorem implies that on the level of sets $\mathrm{Spec}(R)$ is glued from the sets $S_i = \mathrm{Spec}(R_i)$ by identifying the subsets $S_{ij} = \mathrm{Spec}(R_iR_j)$ in $\mathrm{Spec}(R_i)$ and $\mathrm{Spec}(R_j)$. In fact, using a minimal amount of algebraic geometry one can define a scheme S by gluing S_i along open subschemes S_{ij}, and then the above theorem is essentially equivalent to showing that S is affine. Since $\Gamma(\mathcal{O}_S) = R$, the latter means that $S = \mathrm{Spec}(R)$, and in this way it would suffice to check that each R_i is a localization of R.

(ii) A domain is called *Prüfer* if its localization at prime ideals are valuation ring. Theorem 2.5.6 implies that R is a semilocal Prüfer ring if and only if it is the intersection of finitely many valuation rings of $\mathrm{Frac}(R)$.

2.5.8. *The set $V_{l/k}$.* If k is a valued field and l/k is a field extension, we denote the set of all equivalence classes of extensions of the valuation to l by $V_{l/k}$. This coincides with the set of all valuation rings of l that dominate k°.

2.5.9. *The extension theorem.* Now, we can give an algebraic description of the set of extensions of a valuation through finite and even algebraic extensions.

Theorem 2.5.10. *Assume that k is a valued field and l/k is an algebraic extension. Let $R = \mathrm{Nor}_l(k^\circ)$ be the integral closure of k° in l and let $\{m_i\}_{i\in I}$ be the set of maximal ideals of R. Then,*

(i) Each localizations R_{m_i} is a valuation ring dominating k° and this gives rise to a bijection $I = V_{l/k}$. In particular, $V_{l/k}$ is non-empty.

(ii) If l/k is normal, then $\mathrm{Aut}(l/k)$ acts transitively on $V_{l/k}$.

Proof. A colimit argument reduces this to the case when l/k if finite. By Theorem 2.4.16 $R = \cap_{V_{l/k}} R_i$, in particular, $V_{l/k} \ne \emptyset$. In addition, the maps $\mathrm{Spec}(R_i) \to \mathrm{Spec}(k^\circ)$ are bijections by Corollary 2.3.12 and Lemma 2.4.8, hence no R_i is a localization of another one. We claim that $|V_{l/k}| < \infty$. Since we already proved that valuations extend through finite extensions, it suffices to prove this for a larger finite extension of k. Thus, we can assume that l/k is normal, and then it suffices to prove (ii).

First, if l/k is purely inseparable of degree p^n, then any $x \in l$ satisfies $x^{p^n} \in k$. Therefore, the set l° of all $x \in l$ such that $x^{p^n} \in k^\circ$ is a valuation ring. Since $l^\circ \subseteq R$ this implies that $R = l^\circ$ is the only extension of the valuation to l. Let l_s is the separable closure of k in l. Then we have proved that $V_{l_s/k} = V_{l/k}$, hence it remains to prove (ii) for the Galois extension l_s/k. For shortness of notation, assume $l = l_s$. Take any $R_1 \in V_{l/k}$ and set $R' = \cap_{g\in G} gR_1$, where $G = G_{l/k}$. Then for any $\alpha \in R'$ the minimal polynomial $f_\alpha = \prod_{g\in G}(t - g\alpha)$ over k lies in $R_1[t] \cap k[t] = k^\circ[t]$. This proves that the embedding $R \hookrightarrow R'$ is an equality. By Theorem 2.5.6, if $V_{l/k}$ contains a valuation ring R_2 not of the form gR_1, then $R_2 \cap (\cap_{g\in G} gR_1)$ is strictly smaller than R, which is impossible. So, G acts on $V_{l/k}$ transitively. $\square$

2.5.11. *Algebraic closure of a valued field.* One of the most important corollaries is that valued algebraic closure is unique up to a (non-unique) isomorphism.

Corollary 2.5.12. *Assume that k_1/k and k_2/k are extensions of valued fields such that on the level k_1 and k_2 are algebraic closures of k on the level of valued field. Then there exists an isomorphism $k_1 \widetilde{\to} k_2$ of valued k-fields.*

Remark 2.5.13. The corollary shows that one can work with valued algebraic closures precisely as one works with algebraic closures in Galois theory. The only subtle thing is that on a fixed algebraic closure k^a there might exist many non-equivalent extensions of valuations $|\ |_i$. This happens because the automorphism group D_i of $(k^a, |\ |_i)$ is the stabilizer of $|\ |_i$ in $G = \mathrm{Aut}(k^a/k)$, and for non-henselian fields, D_i is smaller than G. The group D_i is called the *decomposition group* of the extended valuation $|\ |_i$.

2.5.14. *Multiplicity of extended valuation.* Assume that k is a valued field, l/k a finite extension, and $|\ |_1, \dots, |\ |_m$ the valuations of $V_{l/k}$. Since any $|\ |_i$ can be extended to k^a, it follows from Corollary 2.5.12 that $|\ |_i$ is induced from a fixed valuation $|\ |$ on k^a via an embedding $l \hookrightarrow k^a$. Let $n = [l : k]$ and let $\sigma_1, \dots, \sigma_n$ be the k-embeddings of l into k^a, where each embedding appears p^l-times for the inseparability index p^l. Let n_i be the number of times $|\ |_i$ appears as the valuation induced via σ_j for $1 \le j \le n$. We call n_i the *multiplicity* the valuation $|\ |_i$ in l/k. In addition, if $l_i = (l, |\ |_i)$ is the corresponding valued extension of k then we call $n_{l_i/k} = n_i$ the *multiplicity of the extension.* Obviously, $n = \sum_{i=1}^m n_i$.

More generally, for any algebraic extension of valued fields l/k we define $n_{l/k} = \max_i n_{l_i/k}$, where l_i/k run through finite subextensions of l/k. This can be a finite number or infinity.

Exercise 2.5.15. (i) For any algebraic tower of extensions of valued fields $m/l/k$ one has that $n_{m/k} = n_{m/l} n_{l/k}$.

(ii) If L/k is an extension of valued fields and l, K are two subextensions such that $L = lK$, then $n_{L/K} \le n_{l/k}$.

2.5.16. *The defect.* For a finite extension of valued fields we also introduce the *defect* $d_{l/k} = \frac{n_{l/k}}{e_{l/k} f_{l/k}}$. We will later show that $d_{l/k}$ is either 1 or a power of the residual characteristic of k, but even proving that $d_{l/k} \ge 1$ will be a difficult task for valuations of arbitrary height. At this point we only know that $d_{l/k}$ is a rational number and it is multiplicative in towers because the invariants n, e and f are. We also define the defect of an arbitrary algebraic extension to be the maximum of defects over its subextensions.

Note that for a finite extension l/k and all extension of the valuation to l the equality $[l : k] = \sum_i e_{l_i/k} f_{l_i/k} d_{l_i/k}$ holds in a tautological way, but it is useless until we at least prove that $d_{l_i/k} \ge 1$.

2.5.17. *Basic types of extensions.* Using invariants one can introduce the following basic classes of algebraic extensions of valued fields. In Chapter 3, we will study them extensively and explain why they naturally arise in the Galois theory of valued fields. By $p = \mathrm{exp.char}(\widetilde{k})$ we denote the residual characteristic exponent, that is, $p = 1$ is $\mathrm{char}(\widetilde{k}) = 0$ and $p = \mathrm{char}(\widetilde{k})$ otherwise.

(1) L/k is *strictly unramified* if $n_{L/k} = 1$.
(2) L/k is *unramified* if $n_{l/k} = e_{l/k}$ and $\widetilde{l}/\widetilde{k}$ is separable for any finite subextension l/k.
(3) L/k is *tame* if $n_{l/k} = e_{l/k} f_{l/k}$, $\widetilde{l}/\widetilde{k}$ is separable, and $(p, f_{l/k}) = 1$ for any finite subextension l/k.

Each of these classes has a natural complementary class of extensions as follows.

(1) Henselian extensions L/k. Note that L/k is henselian if $n_{l/k}$ equals to separability degree of l/k for any finite subextension l/k.
(2) L/k is *totally ramified* if it is henselian and $\widetilde{L}/\widetilde{k}$ is purely inseparable.
(3) L/k is *purely wild* if it is henselian, $\widetilde{L}/\widetilde{k}$ is purely inseparable, and $|L^\times|/|k^\times|$ is a p-torsion group.

Note that if $p = 1$, that is the residual characteristic is zero, then there are no non-trivial purely wild extensions.

2.5.18. *Some complements.* The following results will not be used, so we leave them as exercises.

Exercise 2.5.19. Assume that K/k is an extension of valued fields and l/k is an algebraic extension such that $L = l \otimes_k K$ is a field.

(i) Show that the map $\psi\colon V_{L/K} \to V_{l/k}$ induced by restriction of the valuation is surjective.

(ii) Show that ψ is not injective in general. (Hint: take $k = (\mathbb{Q}, |\ |_3)$, $l = k(\sqrt{3})$ and $K = k(\sqrt{21})$. Then l/k and K/k are henselian, but $L = lK/k$ is not henselian because it contains $k(\sqrt{7})$, which is not henselian over k. In particular, L/l and L/K are not henselian.)

(iii)* Show that ψ is bijective whenever k is separably closed in K.

2.5.20. *The max formula.* If k is a valued field, then by Lemma 2.3.21(ii), up to equivalence, any extended valuation on k^a can be viewed as a valuation $k^a \to \sqrt{|k|}$. In particular, we can define a non-archimedean power-multiplicative map $|\ |_{\max}\colon k^a \to \sqrt{|k|}$ by the formula $|\alpha|_{\max} = \max_{i \in V_{l/k}} |\alpha|_i$. Note that the maximum is achieved because $|V_{k(\alpha)/k}| < \infty$. By a slight abuse of language, we will call it the *max-norm*, similarly to the real valued case. In fact, the theory we developed in the real valued case generalizes straightforwardly, so we will refer to that case for details. As in that case, for any $\alpha \in k^a$ with minimal polynomial $f_\alpha(t) = t^d + \sum_{i=1}^d a_i t^{d-1}$ we also define the spectral norm $|\alpha|_{\mathrm{sp}} = \sigma(f) = \max_i |a_i|$.

Theorem 2.5.21. *For any valued field k there is an equality $|\ |_{\mathrm{sp}} = |\ |_{\max}$ of functions $k^a \to \sqrt{|k|}$.*

Proof. The proof copies the proof of Theorem 1.8.23. First, for any fixed valuation $|\ | \in V_{k^a/k}$ one checks that $|\alpha|_{\mathrm{sp}} = \max_j |\alpha|_j$, where $\alpha_1, \dots, \alpha_n$ are the roots of f_α. This verbatim the same computation as in the proof of Lemma 1.8.19. Then, using that by Theorem 2.5.10(ii) $\mathrm{Aut}(k^a/k)$ acts transitively on $V_{k^a/k}$, one obtains that $\max_j |\alpha|_j = \max_{i \in V_{k^a/k}} |\alpha|_i$. □

2.6. **Henselian valued fields.**

2.6.1. *Henselian fields and extensions.* As in the case of real valued fields, an algebraic extension of valued fields l/k is *henselian* if $|V_{l/k}| = 1$. A valued field k is called *henselian* if the extension k^a/k is henselian.

Lemma 2.6.2. *Assume that k is a real valued field and $m/l/k$ is a tower of algebraic extensions, then*

(i) m/k is henselian if and only if l/k is henselian and m/l is henselian with respect to the extension of the valuation to l.

(ii) k is henselian if and only if l/k is henselian and l is henselian with respect to the extension of the valuation.

(iii) If l/k is purely inseparable, then it is henselian. In particular, if k is separably closed, then it is henselian.

Proof. Claims (i) and (ii) follow from the fact that $V_{l/k}$ is non-empty by Theorem 2.5.10(i). If l/k is purely inseparable, then it is normal, and by Theorem 2.5.10(ii) $\mathrm{Aut}(l/k) = 1$ acts transitively on $V_{l/k}$. Thus $|V_{l/k}| = 1$, as claimed. □

2.6.3. *Krasner's lemma.* Krasner's lemma that we earlier proved for complete fields in fact only needs the assumption that a field k is henselian. As in the real valued case, for any $\alpha \in k^a$ we set $r_\alpha = \inf_{i>1} |\alpha - \alpha_i|$ where $\alpha = \alpha_1$ and $f_\alpha = \prod_i (t - \alpha_i)$.

Theorem 2.6.4. *Assume that K/k is an extension of valued fields with a henselian K, and provide K^a with the valuation extending that of K. Assume further that $\alpha \in K^a$ is algebraic over k and K contains an element α_0 such that $|\alpha - \alpha_0| < r_\alpha$. Then $\alpha \in K$.*

Proof. We just copy the proof of Theorem 1.7.28. Clearly α is separable over k. Let f be the minimal polynomial of α over K. Then $f(t + \alpha_0)$ is an irreducible polynomial over K which vanishes at $\alpha - \alpha_0$ and has all other roots of the form $\alpha_i - \alpha_0$ for $i > 1$. Since all roots of $f(t - \alpha_0)$ are conjugated over K and there is a unique extension of the valuation to K^a, all these roots have the same valuation. It remains to note that $|\alpha_1 - \alpha_0| < r \le |\alpha_i - \alpha_0|$ for $i > 1$, and hence $f(t + \alpha_0) = t - (\alpha - \alpha_0)$. In particular, $\alpha \in K$. □

2.6.5. *Application to existence of roots.* As a corollary we will now prove for general henselian field a criterion on existence of roots.

Corollary 2.6.6. *Assume that k is a henselian field, $a \in k$ an element and d a natural number invertible in $\widetilde{k}$. Then k contains a root $a^{1/d}$ if and only if there exists $c \in k$ such that $|a - c^d| < |a|$.*

Proof. Fix a root $\alpha = a^{1/d} \in k^a$ and set $\beta = \frac{c}{\alpha}$. Since $|\alpha^d - c^d| < |\alpha^d|$, we have that $|\beta^d - 1| < 1$, and hence $\widetilde{\beta}$ is a d-th root of unity. It follows that there exists a d-th root of unity $\xi \in k^a$ such that $|\beta - \xi| < 1$ and hence also $|c - \xi\alpha| < |\alpha|$. Replacing α by $\xi\alpha$ for simplicity we can assume that $|c - \alpha| < |\alpha|$.

We claim that $\alpha \in k$ by Krasner's lemma. Indeed, it suffices to check that if $\alpha' \ne \alpha$ is a conjugate of α, then $|\alpha - \alpha'| = |\alpha|$. But $\alpha' = \alpha\xi$ for a d-th root of unity $\xi \ne 1$, and since the polynomial $t^d - 1$ is separable over $\widetilde{k}$, we have that $\widetilde{\xi} \ne 1$. Thus $|\xi - 1| = 1$ and so $|\alpha - \alpha'| = |\alpha|$. □

Exercise 2.6.7. * Assume now that k is of mixed characteristic and $d = p^n m$, where $p = \mathrm{char}(\widetilde{k})$ and $(p, m) = 1$. Show that $a^{1/d} \in k$ if and only if there exists $c \in k$ such that $|a - c^d| < |p|^{(np+1-n)/(p-1)} \cdot |a|$. Also, in the case of an analytic k prove this directly by computing the convergence radius of the binomial series of $(1 + t)^{1/d}$.

2.6.8. *A criteria of henselianity of extensions.* Next, we work out some criteria for being henselian, and we start with the case of extensions.

Theorem 2.6.9. *Let k be a valued field and let l/k be an algebraic extension. Then the following conditions are equivalent:*
(i) l/k is henselian.
(ii) The max norm on l is a valuation.
(iii) The ring $R = \mathrm{Nor}_l(k^\circ)$ is local.
(iv) There exists no $x \in R$ such that both x and $1-x$ are non-invertible.

Proof. By independence of valuations, neither extension of the valuation of k to l dominate other ones. So, the equivalence (i)$\Longleftrightarrow$(ii) follows from Theorem 2.5.21. The equivalence (ii)$\Longleftrightarrow$(iii) is due to Theorem 2.5.10(i), and the equivalence (iii)$\Longleftrightarrow$(iv) is a simple basic fact in commutative algebra. □

The following exercise makes the latter criterion more practical.

Exercise 2.6.10. Prove that $x \in \mathrm{Nor}_l(k^\circ)$ is invertible if and only if $\mathcal{N}r_{l/k}(x)$ is invertible in k°. (Hint: use the Galois action.)

2.6.11. *Hensel's lemma.* Now we are going to extend the Hensel's lemma to henselian valued fields. In fact, it even extends to arbitrary henselian extensions using the following notion. We say that a polynomial $f(t) \in k[t]$ over a valued field k is *henselian* if its splitting field is henselian.

Theorem 2.6.12. *Let k be a valued field and $f(t) \in k^\circ[t]$ an irreducible henselian polynomial with integral coefficients. Then the reduction $\widetilde{f}$ is either a constant or a constant times a power of an irreducible polynomial.*

Proof. Let l be the splitting field of f and $f(t) = c\prod_i(t-\alpha_i)$ the splitting of f in $l[t]$. Since the valuation of k extends uniquely to l, the values of $|\alpha_i|$ coincide. In particular, either $|\alpha_i| > 1$ for any i, and then the reduction is easily seen to be constant, or $\alpha_i \in l^\circ$ for any i. In the latter case, the reduction $\widetilde{f}$ splits as $\widetilde{c}\prod_i(t-\widetilde{\alpha}_i)$. It remains to note that $\mathrm{Aut}(l/k)$ acts transitively on the set $\{\alpha_i\}$ and preserves the valuation, hence it descends to a $\widetilde{k}$-action on $\widetilde{l}$ which acts transitively on the set of roots of $\widetilde{f}$. This implies that $\widetilde{f}$ is as required. □

Exercise 2.6.13. Deduce the usual versions of Hensel's lemma. For example, if f is a henselian polynomial and its reductions splits as $\widetilde{f} = \overline{g}\overline{h}$ with corpime factors, then f splits as $f = gh$ with $\widetilde{g} = \overline{g}$ and $\deg(g) = \deg(\widetilde{g})$.

2.6.14. *Specialization of the Galois group.* If l/k is a henselian extension of valued fields, then the action of $\mathrm{Aut}(l/k)$ preserves the valuation, and hence it acts on l° and $\widetilde{l}$. In particular, a homomorphism $\mathrm{Aut}(l/k) \to \mathrm{Aut}(\widetilde{l}/\widetilde{k})$ arises.

Lemma 2.6.15. *If l/k is a normal finite henselian extension of valued fields, then the homomorphism $\phi\colon \mathrm{Aut}(l/k) \to \mathrm{Aut}(\widetilde{l}/\widetilde{k})$ is surjective and $\widetilde{l}/\widetilde{k}$ is normal.*

Proof. Let F be the separable closure of $\widetilde{k}$ in $\widetilde{l}$. By the primitive element theorem there exists $\overline{\alpha} \in \widetilde{l}$ such that $F = \widetilde{k}(\overline{\alpha})$. Choose any $\alpha \in l^\circ$ with $\widetilde{\alpha} = \overline{\alpha}$. The same argument as in the proof of Theorem 2.6.12 shows that if $\alpha = \alpha_1, \dots, \alpha_n$ are the conjugates of α, then $\widetilde{\alpha}_1, \dots, \widetilde{\alpha}_n$ are the conjugates of $\widetilde{\alpha}$. Therefore, the image of ϕ acts transitively on the set of conjugates of $\widetilde{\alpha}$, and this implies that ϕ is onto. Moreover, this proves that all elements $\widetilde{\alpha}_i$ are in $\widetilde{l}$, and hence $\widetilde{l}/\widetilde{k}$ is normal. □

2.6.16. *Criteria of henselianity of a field.* Now we can extend Theorem 1.9.13 to the case of general valued fields.

Theorem 2.6.17. *Assume that k is a non-archimedean valued field. Then the following conditions are equivalent:*

(i) k is henselian.

(ii) For any $f \in k^\circ[t]$ and a factorization $\widetilde{f} = \overline{g}\overline{h}$ with $(\overline{g}, \overline{h}) = 1$ in $\widetilde{k}[\widetilde{t}]$, there exists a lifting $f = gh$ with $\widetilde{g} = \overline{g}$ and $\deg(g) = \deg(\overline{g})$.

(iii) Any $f \in k^\circ[t]$ splits as $f = gh$ with $|h-1| < 1$ and $\deg(g) = \deg(\widetilde{g})$.

(iv) For any monic $f \in k^\circ[t]$ and a simple root $\overline{a} \in \widetilde{k}$ of $\widetilde{f}$ there exists a root $a \in k$ of f such that $\widetilde{a} = \overline{a}$.

(v) Any irreducible monic polynomial $f = t^d + a_1t^{d-1} + \ldots + a_d \in k[t]$ with $a_d \in k^\circ$ lies in $k^\circ[t]$.

(vi) Any irreducible monic polynomial $f = t^d + a_1t^{d-1} + \ldots + a_d \in k[t]$ satisfies $|a_i|^{1/i} \le |a_d|^{1/d}$ for $1 \le i \le d$.

Proof. We can assume that the valuation is non-trivial, and the implications (vi)$\Longrightarrow$(v), (ii)$\Longrightarrow$(iv), and (ii)$\Longrightarrow$(iii) are clear. Furthermore, (i) implies (ii) by Theorem 2.6.12 (and Exercise 2.6.13), and (i) implies (vi) by Theorem 2.5.21. So far, this is the same argument as in the proof of Theorem 1.9.13.

It remains to show that if k is not henselian, then (iii), (iv) and (vi) fail. This time we cannot use completions, so a new argument is needed. Fix a finite non-henselian extension L/k. By Lemma 2.6.2, we can replace L by the separable closure of k in it, we can assume that L/k is separable. Then, replacing L by its Galois closure over k we can assume that L/k is Galois. Fix an extension of th evaluation to L, and denote it also by $|\ |$. Let $G = G_{L/k}$, let H be the subgroup of elements $h \in G$ that preserve $|\ |$, and let $l = L^H$. Let $|\ |_1, \ldots, |\ |_n$ be the elements of $V_{l/k}$ with $|\ |_1 = |\ |$. Embeddings of l into L are parameterized by the elements of G/H. The trivial embedding induces the valuation $|\ |_1$, and, by the definition of H, other embeddings induce valuations $|\ |_i$ with $i > 1$.

The remaining argument proceeds as in the proof of Theorem 1.9.13. By independence of valuations, see Lemma 2.5.4, there exists $a \in l$ such that $|a|_1 < 1$ and $|a-1|_j < 1$ for $2 \le j \le n$. It follows that if $a_1 = a, a_2, \ldots, a_d$ are all conjugates of a, then $|a_1| < 1$ and $|a_i - 1| < 1$ for $i \ge 2$. In particular, the minimal polynomial f_a satisfies $\widetilde{f_a} = t(t-1)^{d-1}$ and hence violates (iv). Polynomials violating (iii) and (v) are constructed similarly – see the last paragraph from the proof of Theorem 1.9.13. □

2.7. **Henselization.**

In Chapter 1 we have used completions to construct henselizations of real valued fields. In this section, we will provide an algebraic construction which applies to arbitrary valued fields as well. Then we will use henselizations to extend to the general case results that were proved for real valued fields using completions.

2.7.1. *Liftings of simple roots.* For brevity, we used independence of valuations to prove all criteria of henselianity, but the only one where it was really important is criterion (iv). It is the most non-trivial and useful criterion, which will be used to construct henselizations of valued field. The key observation is the following result.

Lemma 2.7.2. *Assume that k is a valued field, $f \in k^\circ[t]$ is an irreducible monic polynomial with integral coefficients such that the reduction $\widetilde{f}$ has a simple root*

$\overline{\alpha}$. *Let $l = k(\alpha)$ be the simple extension generated by a root α of f. Then there exists a unique extension $|\ |_l$ of the valuation of k to l such that $\widetilde{\alpha} = \overline{\alpha}$. Moreover, if k^a is provided with a valuation extending that of k, then there exists a unique k-embedding $l \hookrightarrow k^a$ inducing $|\ |_l$ on l.*

Proof. By Theorem 2.5.10(ii) any other valuation from $V_{k^a/k}$ is obtained by conjugating $|\ |$ by an element of $\mathrm{Aut}(k^a/k)$. Since any valuation on l extends to a valuation on k^a, it follows that any valuation on l is induced from $|\ |$ via a k-embedding $\sigma\colon l \hookrightarrow k^a$. If $f = \prod_i (t - \alpha_i)$ is the splitting of f in $k^a[t]$, then $\alpha_i = \sigma(\alpha)$ determines σ. A standard argument, shows that $|\alpha_i| \leq 1$, hence $\widetilde{f} = \prod_i (\widetilde{t} - \widetilde{\alpha}_i)$ and we can renumber the roots so that $\widetilde{\alpha}_1 = \overline{\alpha}$ and $\widetilde{\alpha}_i \neq \overline{\alpha}$ for $i > 1$. Then it is clear that the only valuation on l, such that $\overline{\alpha}$ is the reduction of α, corresponds to the embedding sending α to α_1. □

Corollary 2.7.3. *Assume that k is a valued field and provide k^a with an extended valuation. Then there exists a minimal k-subfield $l \subseteq k^a$ such that any monic polynomial $f(t) \in l^\circ[t]$ with a simple root $\overline{\alpha}$ of the reduction $\widetilde{f}(\widetilde{t})$ there exists a root $\alpha \in l^\circ$ of f such that $\widetilde{\alpha} = \overline{\alpha}$.*

Proof. Let $\{(f_i, \overline{\alpha}_i)\}$ be the set of all irreducible monic polynomials in k° and simple roots $\overline{\alpha}_i$ of $\widetilde{f}_i$. By Lema 2.7.2 there exists a unique subfield $k(i) = k(\alpha_i)$ of k^a such that $f(\alpha_i) = 0$ and $\widetilde{\alpha}_i = \overline{\alpha}_i$. Take l_1 to be the composite of all k_i. In the same way define l_2 by adjoining to l_1 all liftings of simple roots of irreducible monic polynomials from $l_1^\circ[t]$, etc. The field $l = \cup_i l_i$ is as required. □

In fact, one can shorten the above construction, but this requires an additional work and will not be needed.

Exercise 2.7.4. * Similarly to the construction of the algebraic closure in Galois theory, show that in fact $l = l_1$ and the subsequent extensions are trivial.

2.7.5. *Henselization.* The valued extension l of k which was defined in Corollary 2.7.3 is usually denoted k^h/k and called the *henselization* of k. This is justified by the following result.

Theorem 2.7.6. *Let k be a valued field. Then the valued field k^h is the minimal henselian valued field containing k^h. Namely, for any embedding of valued fields $k \hookrightarrow K$ with a henselian target factors through $k \hookrightarrow k^h$ uniquely.*

Proof. By the equivalence (i)$\Longleftrightarrow$(iv) in Theorem 2.6.17, the field k^h is henselian. Moreover, by the same theorem any extension K/k with a henselian K contains any subfield $k(\alpha)$ such that $\widetilde{\alpha}$ is a simple root of $\widetilde{f}_\alpha$. Therefore, in the situation of Corollary 2.7.3, we see that $k \hookrightarrow K$ factors through l_1. In the same way, $l_1 \hookrightarrow K$ factors through l_2, and so on, proving the theorem. □

Exercise 2.7.7. (i) Show that $n_{k^h/k} = 1$. In particular, k^h/k is separable.

(ii) Show that k^h/k is the maximal valued algebraic extension l/k such that $n_{l/k} = 1$.

(iii) Let $|\ |$ denote the extended valuation from k^h to k^s and let $D \subset \mathrm{Gal}(k^s/k)$ be the decomposition group of $|\ |$. Show that $k^h = (k^s)^D$.

Remark 2.7.8. This provides another way to construct k^h. Namely, one fixes any extension of the valuation to k^s, and then takes k^h to be the fixed field of its decomposition group.

Exercise 2.7.9. Let $D \subsetneq \mathrm{Gal}(k^s/k)$ be the decomposition group of a valuation. Show that D coincides with its normalizer, and explain why this is equivalent to the fact that k^h has no automorphisms over k preserving the valuation.

2.7.10. *A description of* $V_{l/k}$. Henselization is a finer analogue of completion, and we wil now use it to extend some results about real valued fields. We start with a Galois-theoritc description of the set $V_{l/k}$.

Theorem 2.7.11. *Assume that k is a valued field and let k^a be the valued algebraic closure. For any algebraic extension l/k there always exists an extension of valuation to l, each such extension is induced by a k-embedding $l \hookrightarrow k^a$, and two embedding induce the same valuation if and only if they are conjugate over k^h. Equivalently,* $\mathrm{Hom}_k(l, k^a)/\mathrm{Aut}(k^a/k^h) = V_{l/k}$.

Proof. We should only prove that valuations obtained from $\sigma_1, \sigma_2 \in \mathrm{Hom}_k(l, k^a)$ are equivalent if and only if they are conjugate over k^h. Since the decomposition group $D = \mathrm{Aut}(k^a/k^h)$ preserves the valuation, if σ_i are conjugate, then the induced valuations coincide. Conversely, assume that they induce the same valuation on l. Let l^h be the henselization of h with respect to this valuations, and consider the induced embeddings $\sigma_i^h \colon l^h \hookrightarrow k^a$. By uniqueness of the valued algebraic closure there exists an automorphism τ of k^a such that $\tau \circ \sigma_1^h = \sigma_2^h$. Since τ fixes k and preserves the valuation, it also fixes k^h. Thus, $\tau \in \mathrm{Aut}(k^a/k^h)$, as required. $\square$

2.7.12. *The tensor product formula.* As a corollary, we again obtain a tensor product formula, and this time one even does not have to apply reduction.

Theorem 2.7.13. *Assume that k is a valued field, l/k is a finite extension, $|\ |_i$, $1 \le i \le d$ are the elements of $V_{l/k}$, and $l_i = (l, |\ |_i)$ are the corresponding valued fields. Then $l \otimes_k k^h = \prod_{i=1}^d l_i^h$ and $n_{l_i/k} = [l_i^h : k^h]$.*

Proof. Since k^h/k is separable, $l \otimes_k k^h = \prod_{F \in C} F$, where C is the set of isomorphism classes of abstract composites lk^h. Note that each composite F possesses a canonical valuation by the henselianity of k^h and $F = l^h$, where l is provided with the induced valuation. Indeed, $k^h \subseteq l^h$, hence $F = lk^h \subseteq l^h$, and since F is henselian this is an equality.

An element $\sigma \in \mathrm{Hom}_k(l, k^a)$ gives rise to a composite $\sigma(l)k^h$, and two such composites are isomorphic as abstract composites if and only if they are conjugate over k^h. So, $\mathrm{Hom}_k(l, k^a)/\mathrm{Aut}(k^a/k^h) = C$, and by Theorem 2.7.11 we obtain that $C \xrightarrow{\sim} V_{l/k}$, where a composite F is sent to the valuation it induces on l. At this stage we already obtain that

$$l \otimes_k k^h = \prod_{F \in C} F = \prod_{i=1}^{d} l_i^h.$$

Let $n = [l : k]$ and $\sigma_1, \dots, \sigma_n$ be the elements of $\mathrm{Hom}_k(l, k^a)$ repeated p^m times, where p^m is the inseparability degree of l/k. Then each composite F is obtained as $\sigma_i(l)k^h$ precisely $[F : k^h]$ times. On the other hand, this is precisely the number of times the corresponding valuation on l is induced from σ_i. This proves that $n_{l_i/k} = [F : k^h] = [l_i^h : k^h]$. $\square$

2.8. **Compositions and limit argument.** In this section we will develop a technique, which often allows to reduce various problems about valued fields to the case of real valued ones, and we will immediately test it on extensions of valuations. The technique is two-step: first one reduces to finite height by a limit argument, and then one inducts on height by composing valuations of smaller height.

2.8.1. *Limits and finite extensions.* The following simple result can be viewed as a part of Galois theory, so we only indicate a proof.

Lemma 2.8.2. *Assume that a field k is a filtered union of its subfields k_i, $i \in I$. Then for any finite extension l/k there exists $i_0 \in I$ and an extension l_{i_0}/k_{i_0} such that $l = l_{i_0} \otimes_{k_{i_0}} k$. Moreover, in this case $l_i = l_{i_0} \otimes_{k_{i_0}} k_i$ is a field, $l = l_i \otimes_{k_i} k$, and the separable and inseparable degrees of l_i/k_i are equal to those of l/k for any $i \geq i_0$.*

Proof. Choose any basis $x_1, \dots, x_n$ of l over k and consider the multiplication table $x_\alpha x_\beta = \sum_{\gamma=1}^n c_{\alpha\beta\gamma} x_\gamma$ with $c_{\alpha\beta\gamma} \in k$. Then we can take any k_{i_0} such that all $c_{\alpha\beta\gamma}$ lie in k_{i_0} and set $l_{i_0} = k(x_1, \dots, x_n)$. $\square$

2.8.3. *The limit principle.* Lemma 2.8.2 is an illustration of the following general limit principle: any algebraic construction over k which operates with finitely many elements is already defined over some k_i. We will mainly use this in the case of valued fields. In this case, one can always take k_i to be of finite height, see Corollary 2.3.17, reducing nearly all algebraic problems about valued fields to the case of a finite height.

2.8.4. *Continuity of invariants of valued extensions.* As a first instance of the limit principle, we will prove that all numerical invariants of valued extensions are compatible with filtered unions.

Theorem 2.8.5. *Let $k = \cup_{i \in I} k_i$, l/k, i_0 and l_i be as in Lemma 2.8.2, and assume that k is valued and k_i are provided with the induced valuation. Then there exists $i_1 \geq i_0$ such that for any $i \geq i_1$ the natural restriction map $V_{l/k} \to V_{l_i/k_i}$ is a bijection, and for any valuation of $V_{l/k}$ on the induced valuation on l_i, one has that $n_{l/k} = n_{l_i/k_i}$, $e_{l/k} = e_{l_i/k_i}$, $f_{l/k} = f_{l_i/k_i}$, $d_{l/k} = d_{l_i/k_i}$ and $\widetilde{l} = \widetilde{k} \otimes_{\widetilde{k}_i} \widetilde{l}_i$. In particular, l/k is henselian, unramified, tame, totally ramified, etc., if and only if each l_i/k_i with $i \geq i_1$ is so.*

Proof. Fix a valued algebraic closure k^a and fix the induced valuation on its subfields k_i^a. The restriction maps $\Psi_i \colon \mathrm{Hom}_k(l, k^a) \to \mathrm{Hom}_{k_i}(l_i, k_i^a)$ are surjective by the usual Galois theory, hence they are bijective for $i \geq i_0$. (We use that the separable degrees of l/k and l_i/k_i coincide for $i \geq i_0$.) By Theorem 2.7.11, the map $\psi_i \colon V_{l/k} \to V_{l_i/k_i}$ is obtained by dividing both sides of Ψ_i by the action of the decomposition groups. If two embeddings $l \hookrightarrow k^a$ are conjugate by an element of the decomposition group, then the same is true for their restrictions $l_i \hookrightarrow k_i^a$, hence ψ_i is surjective. Since $l = \cup_i l_i$, if two embeddings induce different valuations on l, then they also induce different valuations on l_i for i large enough. This proves that ψ_i is also injective for i large enough.

Now, fix a k-valuation on l and provide all its subfields with the induced valuation. Recall that $n_{l/k}$ equals to the size of the corresponding fiber of the map $\mathrm{Hom}_k(l, k^a) \to V_{l/k}$ times the inseparability degree. Using analogous description of n_{l_i/k_i} and the above paragraph we obtain that $n_{l/k} = n_{l_i/k_i}$.

Note that $\widetilde{l} = \cup_i \widetilde{l}_i$, and hence there exists i_1 such that $\widetilde{l} = \widetilde{k}\widetilde{l}_{i_1}$. It follows that $\widetilde{l}_i = \widetilde{k}_i\widetilde{l}_{i_1}$ for $i \geq i_1$, and hence $e_{l_i/k_i} = [\widetilde{l}_i : \widetilde{k}_i]$ decreases monotonically with i. Increasing i_1 we can assume that $[\widetilde{l}_i : \widetilde{k}_i] = [\widetilde{l}_{i_1} : \widetilde{k}_{i_1}]$ for each $i \geq i_1$, and then also $[\widetilde{l} : \widetilde{k}] = [\widetilde{l}_i : \widetilde{k}_i]$. Thus, $e_{l/k} = e_{l_i/k_i}$ and the composite coincides with the tensor product: $\widetilde{l} = \widetilde{k} \otimes_{\widetilde{k}_i} \widetilde{l}_i$. The equality $f_{l/k} = f_{l_i/k_i}$ is even easier, so we skip the argument, and the equality $d_{l/k} = d_{l_i/k_i}$ follows from the others. □

2.8.6. *Unions and henselization.* As an application we obtain a very important property of henselization.

Corollary 2.8.7. *Assume that a valued field k is a filtered union of its valued subfields, say $k = \cup_{i\in I} k_i$. Then $k^h = \cup_{i\in I} k_i^h$. In particular, if k_i are henselian for $i \geq i_0$, then k is henselian.*

Proof. Clearly, $K = \cup_{i\in I} k_i^h$ is a subfield of k^h. Any finite extension of K is henselian by Lemma 2.8.2 and Theorem 2.8.5, hence K is henselian and we actually have that $K = k^h$. □

Remark 2.8.8. It may freely happen that each k_i is not henselian, but k is. This happens because being a henselian field is a property that addresses all finite extensions of k and it cannot be determined by finitely many conditions.

Exercise 2.8.9. Show that the henselization $l = k^h$ of $k = (\mathbb{Q}, |\ |_p)$ is infinite over k. In particular, l is henselian, but it is a filtered limit of fields l_i which are finite over k, and hence are not henselian. (Hint: for example, if $p > 2$, then l contains any element of the form $\sqrt{1+pn}$, and if $p = 2$, then l contains any element of the form $\sqrt{1+8n}$.)

2.8.10. *Disassembling valuations.* Assume that k is a valued field with $\Gamma = |k^\times|$. Since we will play with many valuations, it will be convenient to denote the ring of integers by $\mathcal{O} = k^\circ$. Given an element $v \in \mathrm{Spec}(\mathcal{O})$, let Γ_v be the corresponding convex subgroup and $\Gamma^v = \Gamma/\Gamma_v$. Denote by $|\ |^v \colon k \to \overline{\Gamma}^v$ the corresponding coarsening, then the ring of integers $\mathcal{O}^v$ of the valued field $k^v = (k, |\ |^v)$ is the localization of $\mathcal{O}$ at v. The image of $\mathcal{O}$ in the residue field $\widetilde{k}^v$ will be denoted $\mathcal{O}_v$.

Lemma 2.8.11. *Keep the above notation, then $\mathcal{O}_v$ is a valuation ring and denoting by k_v the field $\widetilde{k}^v$ provided with the induced valuation $|\ |_v$ one has that $|k_v^\times|_v = \Gamma_v$. In addition, $\mathcal{O}$ is the preimage of $\mathcal{O}_v$ under the map $\mathcal{O}^v \twoheadrightarrow k_v$.*

Proof. Exercise. □

2.8.12. *Composing valuations.* Since valuation is determined by the valuation ring, Lemma 2.8.11 implies that $|\ |$ is determined by the coarse valuation $|\ |^v$ and the induced valuation on $|\ |_v$ the residue field. Therefore, we say that $|\ |$ is *composed* from these two valuations. Conversely, one can compose valuations as follows.

Lemma 2.8.13. *Assume that $K_1 = (K, |\ |_1)$ is a valued field and the residue field k is provided with a valuation $|\ |_2$. Then the preimage K° of k° in K_1° is a valuation ring, and the induced valuation $|\ |$ on K is composed from $|\ |_1$ and $|\ |_2$. In particular, there is an exact sequence $1 \to |K^\times|_1 \to |K^\times| \to |k^\times|_2 \to 1$.*

Proof. Exercise. □

2.8.14. *The composition principle.* Assume that $|\ |$ is composed from $|\ |^v$ and $|\ |_v$. The composition principle states that constructions over the valued field k reduce to constructions over the valued fields k^v and k_v, which agree on the field $k_v = \widetilde{k}^v$ provided with the trivial valuation.

2.8.15. *Composed valuations and algebraic extensions.* Now we will test the composition principle on algebraic extensions. Assume that a valuation $|\ |$ on k is composed from $|\ |^v$ and $|\ |_v$, and l/k is an algebraic extension of valued fields. Since the map $\mathrm{Spec}(l^\circ) \to \mathrm{Spec}(k^\circ)$ is a bijection, there is a unique coarsening l_v such that l_v/k_v is an extension of valued fields, and then an extension of valued fields $\widetilde{l}_v/\widetilde{k}_v$ arises.

Lemma 2.8.16. *Keep the above notation, then there restriction of valuation induces a surjective map $\psi\colon V_{l/k} \twoheadrightarrow V_{l^v/k^v}$ and the fiber over $w \in V_{l^v/k^v}$ with the induced valued field $l_w = (\widetilde{l}^v, |\ |_w)$ is canonically bijective to V_{l_w/k_v}. In particular, l/k is henselian if and only if l^v/k^v and l_v/k_v are henselian.*

Proof. Extending $|\ |$ to l is equivalent to first extending $|\ |^v$ to l, and then extending $|\ |_v$ through the induced extension $\widetilde{l}^v/k_v$. Thus, the fibers of ψ are of the form V_{l_w/k_v}. In particular, the fibers are non-empty. □

Corollary 2.8.17. *Assume that k is a valued field, whose valuation is composed from $|\ |^v$ and $|\ |_v$. Then k is henselian if and only if both k^v and k_v are henselian.*

Proof. This follows from the previous lemma and the fact that by Lemma 2.3.21 any algebraic extension of k_v is the reduction of a valued algebraic extension of k^v. □

2.8.18. *Invariants and composition.* Computing invariants of extensions of valued fields with composed valuations is subtler.

Theorem 2.8.19. *In the situation of §2.8.15*

$$e_{l/k} = e_{l_v/k_v}, \quad f_{l/k} = f_{l_v/k_v} f_{l^v/k^v}, \quad d_{l/k} = d_{l_v/k_v} d_{l^v/k^v}, \quad \frac{n_{l/k}}{e_{l/k}} = \frac{n_{l_v/k_v}}{e_{l_v/k_v}} \frac{n_{l^v/k^v}}{e_{l^v/k^v}}.$$

Proof. The first equality follows from the observation that $\widetilde{k} = \widetilde{k}_v$ and $\widetilde{l} = \widetilde{l}_v$. By Lemma 2.8.13 the groups of values of l^v, l and l_v form an exact sequence, and the group of values of k^v, k and k_v form an exact subsequence. Therefore we obtain an exact sequence of quotients

$$1 \to |(l^v)^\times|^v/|(k^v)^\times|^v \to |l^\times|/|k^\times| \to |l_v^\times|_v/|k_v^\times|_v \to 1,$$

and hence $f_{l/k} = f_{l_v/k_v} f_{l^v/k^v}$.

The equality for the defects follows from the other ones, so it remains to prove the last equality. Fix an extension of $|\ |$ to k^a, and let $|\ |^v$ be its appropriate coarsening. Since $e_{l/k} = e_{l_v/k_v}$ we should prove that $\frac{n_{l^v/k^v}}{n_{l/k}} = \frac{e_{l_v/k_v}}{n_{l^v/k^v}}$. Letting $\Sigma \subseteq \Sigma^v$ denote the sets of k-embeddings $l \hookrightarrow k^a$ compatible with the valuations of l and l^v, respectively, we have that $\frac{n_{l^v/k^v}}{n_{l/k}} = \frac{|\Sigma^v|}{|\Sigma|}$. Let $D \subseteq D^v$ and D denote the decomposition subgroups of $\mathrm{Aut}(k^a/k)$ corresponding to $|\ |$ and $|\ |^v$. Then D^v acts on Σ^v transitively and Σ is an orbit of D. Since all orbits are conjugated by elements of D,[3]

□

[3]Complete the argument.

Corollary 2.8.20. *In the situation of §2.8.15, l/k is defectless, unramified or tame if and only if both l^v/k^v and l_v/k_v are so, and l/k is strictly unramified if and only if l^v/k^v is unramified and l_v/k_v is strictly unramified.*

2.9. **The fundamental inequality.**

2.9.1. *The formulation.* First, let us formulate the result and briefly discuss it.

Theorem 2.9.2. *Assume that k is a valued field and l/k is a finite extension, and let $l_1, \ldots, l_m$ be the valued field structures on l corresponding to the elements of $V_{l/k}$. Then,*

(i) $1 \le d_{l_i/k}$.
(ii) $e_{l_i/k} f_{l_i/k} \le n_{l_i/k}$.
(iii) $\sum_{i=1}^m e_{l_i/k} f_{l_i/k} \le [l : k]$.

The proof will be completed in §2.9.4. Now we only note that (i) and (ii) are tautologically equivalent, and (iii) follows from them because $[l : k] = \sum_{i=1}^m n_{l_i/k}$. On the other hand, it is (iii) that is called the fundamental inequality after an article of Cohen and Zariski, where it appeared for the first time. Note also that we have already established the case of henselian extensions in Corollary 2.3.5, so the only problem is "to separate different valuations".

2.9.3. *The real valued case.* Assume that k is real-valued. Then k^h is a subfield of $\widehat{k}$, and since $\widehat{k}/k$ is immediate, we obtain that the extension k^h/k is immediate too, that is, $\widetilde{k} = \widetilde{k}^h$ and $|k| = |k^h|$. The same is true for l_i, so we obtain that $e_{l_i^h/k} = e_{l_i/k}$, $f_{l_i^h/k^h} = f_{l_i/k}$. Therefore

$$n_{l_i/k} = [l_i^h : k] \ge e_{l_i^h/k^h} f_{l_i^h/k^h} = e_{l_i/k} f_{l_i/k},$$

where the first equality holds by Theorem 2.7.13.

2.9.4. *The general case.* Now, let us prove Theorem 2.9.2 in general. Assume, to the contrary, that there exists a finite extension of valued fields l/k such that $d_{l/k} < 1$. Recall that by Corollary 2.3.17 k is a filtered union of its subfields of finite height, say $k = \cup_{i \in I} k_i$. By Theorem 2.8.7 there exists i and a finite extension l_i/k_i such that $d_{l_i/k_i} = d_{l/k} < 1$. Replacing l/k by l_i/k_i we can assume that the fields are of finite height. Furthermore, if the height is larger than 1, then k is composed of valued fields k^v and k_v of smaller heights. By Theorem 2.8.19, $d_{l/k} = d_{l^v/k^v} d_{l_v/k_v}$, hence either $d_{l^v/k^v} < 1$ or $d_{l^v/k^v} < 1$. By decreasing induction on the height there exists a finite extension of fields of height at most 1 such that $d_{l/k} < 1$. Obviously, this cannot happen for the trivial valuations, and the case of height 1 was ruled out in the §2.9.3. This completes the proof.

2.9.5. *Application to henselization.* As an immediate corollary we obtain the following important result about the henselization.

Corollary 2.9.6. *Any strictly unramified extension of valued fields is immediate. In particular, for any valued field k the henselization k^h/k is an immediate extension.*

Proof. If $n_{L/k} = 1$, then by the fundamental inequality any finite subextension l/k satisfies $1 = n_{l/k} \ge e_{l/k} f_{l/k}$. Hence $e_{l/k} = f_{l/k} = 1$, and we obtain that l/k is immediate. Obviously, this implies that L/k is immediate. □

Remark 2.9.7. (i) The original proof of the fundamental inequality and the proof in the Commutative Algebra of Bourbaki also contain an argument which inducts on the height of valuation. The real valued case is easier because one can either use completions or at least use that all valuations are completely independent.

(ii) Using a more advanced commutative algebra one can directly prove that henselizations are immediate extensions. From this one easily obtains an alternative proof of the fundamental inequality – just repeat the argument for the real valued case.

2.9.8. *Defectless extensions and stable fields.* An extension of valued fields l/k is called *defectless* if $d_{l/k} = 1$. A valued field k is called *stable* or *defectless* if for any its finite valued extension is defectless.

Lemma 2.9.9. *A valued field k is stable if and only if for any finite extension l/k the fundamental inequality is an equality.*

The lemma is a tautology. A really interesting and subtle question is to provide non-trivial examples of stable fields. Probably, the most important result of this type is that stability is preserved by transcendental extensions $k(x)/k$ with generalized Gauss valuation. This will be proved in Chapter 5.

3. Basic ramification theory

3.1. **Ramification filtration.**

3.1.1. *The absolute case.* Let k be a valued field and $G = G_k = \mathrm{Gal}_{k^s/k}$ its absolute Galois group. Fix an extended valuation on k^a and let $D \subseteq G$ be the decomposition group. As we noticed earlier, another choice of the valuation on k^a would lead to replacing D with its conjugate. The *inertia* subgroup $I \subseteq D$ is the kernel of the specialization homomorphism $G \to \mathrm{Aut}(\widetilde{k^a}/\widetilde{k}) = G_{\widetilde{k}}$. An element $\sigma \in D$ is in I if and only if it satisfies $|\sigma(a) - a| < 1$ for any $a \in (k^a)^\circ$. Finally, the *wild inertia* or the *logarithmic inertia* group $W \subseteq I$ consists of all elements $\sigma \in D$ such that $|\sigma(a) - a| < |a|$ for any $a \in k^a$. This happens if and only if σ acts trivially on the graded reduction $\widetilde{k}_{\mathrm{gr}}$.

The filtration $W \subseteq I \subseteq D \subseteq G$ is called the *basic ramification filtration* of G. One can naturally filter the group W further by so-called higher ramification groups, but this topic will be studied in Chapter 4.

3.1.2. *Galois extensions.* More generally, for any Galois extension of valued fields l/k one can define a filtration on $G_{l/k} = \mathrm{Gal}_{l/k}$ precisely in the same way: the decomposition group $D_{l/k}$ is the stabilizer of the valuation of l, the inertia group $I_{l/k}$ consists of elements that also act trivially on the residue field $\widetilde{l}$, and the logarithmic inertia $W_{l/k}$ consists of elements satisfying $|\sigma(a) - a| < |a|$ for any $a \in l$. In the sequel, we will show that the basic filtration on $G_{l/k}$ is induced from the basic filtration on G_k.

3.2. **Strictly unramified extensions.** For an algebraic extension of valued fields l/k set $l_h = l \cap k^h$. Clearly, l_h/k is the maximal strictly unramified subextension of l/k. However, in general l/l_h does not have to be of a complimentary class.

Exercise 3.2.1. Give an example of a finite extension l/k such that l/l_h is not henselian. (Hint: the smallest such example has invariants $[l : k] = 3$ and $n_{l/k} = 2$, in particular, $l_h = k$ in this case.)

Lemma 3.2.2. *If l/k is a Galois extensions of valued fields, then the homomorphism $\mathrm{Gal}_k \twoheadrightarrow \mathrm{Gal}_{l/k}$ induces a surjective homomorphism of decomposition groups $D_k \twoheadrightarrow D_{l/k}$, and l_h is the fixed field of $D_{l/k}$ in l.*

Proof. Clearly, D_k is taken to $D_{l/k}$. Furthermore, since the valued algebraic closure is unique up to isomorphism, any valued k-automorphism σ of l extends to a valued k-automorphism of $l^a = k^a$. This implies that the restriction is surjective, and the claim about $l_h = l \cap k^h$ then follows from a general Galois theory. □

3.3. **Unramified extensions.**

3.3.1. *The key result.* The key result about unramified extensions of henselian fields is that any separable extension of residue fields admits a minimal lift, which is automatically unique.

Theorem 3.3.2. *Assume that k is a henselian valued field, and $\bar{l}/\widetilde{k}$ is a separable algebraic extensions. Then there exists a unique unramified extension l/k such that $\widetilde{l} = \bar{l}$ as extensions of $\widetilde{k}$, and for any valued extension F/k the reduction induces a bijection $\mathrm{Hom}_k(l, F) = \mathrm{Hom}_{\widetilde{k}}(\widetilde{l}, \widetilde{F})$.*

Proof. Since $\bar{l}$ is a filtered union of its subfields $\bar{l}_i$ finite over $\widetilde{k}$, it suffices to lift each $\bar{l}_i$ to an unramified extension l_i/k and prove the theorem for l_i. Then the tower of embeddings $\bar{l}_i \hookrightarrow \bar{l}_j$ lifts uniquely to a tower of embeddings $l_i \hookrightarrow l_j$ and the field $l = \cup_i l_i$ is as required. Therefore, it suffices to prove the theorem for a finite extension $\bar{l}/\widetilde{k}$.

Since $\bar{l}/\widetilde{k}$ is finite separable, it is generated by a root $\overline{\alpha}$ of an irreducible monic polynomial $\overline{f} \in \widetilde{k}[t]$ of degree $d = [\bar{l} : \widetilde{k}]$. Lift $\overline{f}$ to a monic polynomial $f \in k^\circ[t]$ and let l/k be the extension generated by a root α of f. By the construction, $\bar{l} \subseteq \widetilde{l}$ and $[l : k] \le \deg(f) = d$. Therefore, by the fundamental inequality we obtain that $\widetilde{l} = \bar{l}$ and l/k is an unramified extension of degree d.

Note that $\mathrm{Hom}_k(l, F)$ and $\mathrm{Hom}_{\widetilde{k}}(\widetilde{l}, \widetilde{F})$ can be identified with the sets of roots of f in F and of $\widetilde{f} = \overline{f}$ in $\widetilde{F}$, respectively, and the reduction map $\phi\colon \mathrm{Hom}_k(l, F) \to \mathrm{Hom}_{\widetilde{k}}(\widetilde{l}, \widetilde{F})$ corresponds to taking reduction of a root. Since $\widetilde{f}$ has d distinct roots in $\widetilde{k}^a$, all d roots of f in k^a have distinct reductions. This implies that ϕ is injective and the splitting radius $r_{k,\alpha}$ equals 1. To prove that ϕ is surjective we should show that any root $\overline{\alpha} \in \widetilde{F}$ of $\widetilde{f}$ lifts to a root $\alpha \in F$ of f. In other words, we should prove that the lift $\alpha \in F^a$ lies in F. But any $a \in F^\circ$ with $\widetilde{a} = \overline{\alpha}$ satisfies $|a - \alpha| < 1 = r_{k,\alpha}$, and hence $\alpha \in F$ by Krasner's lemma, see Theorem 2.6.4. □

Now, let us deduce various corollaries from the theorem.

Corollary 3.3.3. *If k is henselian and l/k is unramified, then l is the minimal valued extension of k whose residue field contains $\widetilde{l}$, reduction induces an isomorphism $\mathrm{Aut}(l/k) = \mathrm{Aut}(\widetilde{l}/\widetilde{k})$, and l/k is Galois if and only if $\bar{l}/\widetilde{k}$ is.*

Proof. The minimality is clear: any embedding $\widetilde{l} \hookrightarrow \widetilde{F}$ lifts to an embedding $l \hookrightarrow F$ by Theorem 3.3.2. Applying the claim to $F = l$, we obtain isomorphism of the automorphism groups. The last claim easily reduces to the case of a finite l/k, and then follows from the fact that l/k is Galois if and only if $|\mathrm{Aut}(l/k)| = [l : k]$. □

3.3.4. *Strict henselization.* Another immediate corollary of Theorem 3.3.2 is that for any henselian k there exists a maximal unramified extension k^u, namely the unramified extension whose residue field is $\widetilde{k}^s$. In addition, the extension k^u/k is Galois with $\mathrm{Gal}_{k^u/k} = \mathrm{Gal}_{\widetilde{k}^s}$. Furthermore, for any valued field k we set $k^u = (k^h)^u$ and call it the *strict henselization* of k. A valued field is called strictly henselian if $k^u = k$. As we will immediately prove, this happens if and only if k has no non-trivial unramified extensions.

Corollary 3.3.5. *If k is a valued field, then k^u is the maximal unramified extension of k and the extension k^u/k^h is Galois with $\mathrm{Gal}_{k^u/k^h} = \mathrm{Gal}_{\widetilde{k}}$.*

Proof. The second claim is clear since k^h/k is immediate, and hence $\widetilde{k}$ is the residue field of k^h. The extensions k^h/k and k^u/k^h are unramified, hence k^u/k is unramified. Finally, if l/k is unramified, then l^h/k is unramified and hence l^h/k^h is unramified. The latter implies that $l^h \subseteq k^u$. □

3.3.6. *Filtration on extensions.* The filtration $k^a/k^u/k$ induces filtration on all algebraic extensions l/k. Namely, setting $l_u = l \cap k^u$ we obtain a tower $l/l_u/k$.

Corollary 3.3.7. *If l/k is an algebraic extension of henselian valued fields, then l_u is the only intermediate field such that l/l_u is totally ramified and l_u/k is unramified.*

Proof. It immediately follows from Theorem 3.3.2 that l_u is the unramified extension of k whose residue field is the separable closure of $\widetilde{k}$ in $\widetilde{l}$. Therefore, l/l_u induces a purely inseparable extension of residue fields, that is, l/l_u is totally ramified. □

3.3.8. *Filtration on Galois groups.* To accomplish the picture, let us look at the Galois side.

Corollary 3.3.9. *Assume that l/k if a Galois extension of henselian valued fields. Then l_u/k is Galois, $\widetilde{l}/\widetilde{k}$ is normal, and Gal_{l/l_u} is the inertia subgroup $I_{l/k}$ of $\mathrm{Gal}_{l/k}$. In particular, $I_{l/k}$ is normal and $\mathrm{Gal}_{l/k}/I_{l/k} = \mathrm{Aut}_{\widetilde{l}/\widetilde{k}}$.*

Proof. Any k-automorphism of k^a takes l to itself, hence it also takes its maximal unramified subextension l_u to itself. Thus, l_u/k is normal and hence Galois. In addition, $\widetilde{l}_u/\widetilde{k}$ is Galois with Galois group $\mathrm{Gal}_{l_u/k}$, and $\widetilde{l}/\widetilde{l}_u$ is purely inseparable by previous corollaries. In particular, $\widetilde{l}/\widetilde{k}$ is normal. Finally, $\mathrm{Gal}_{l_u/k} = \mathrm{Gal}_{l/k}/\mathrm{Gal}_{l/l_u}$ is mapped isomorphically onto $\mathrm{Aut}_{\widetilde{l}/\widetilde{k}}$ by Corollary 3.3.3, and hence Gal_{l/l_u} is precisely the inertia subgroup. □

3.4. **Tame extensions.** The study of tame extensions is similar, and could even be joined with the study of unramified extensions at cost of considering graded reduction. We will try to stress this similarity in our exposition.

3.4.1. *Existence of roots.* This time Krasner's lemma will be used through the following result.

Lemma 3.4.2. *Assume that k is a strictly henselian field, $a \in k$ an element, and d a natural number invertible in $\widetilde{k}$. Then k contains a root $a^{1/d}$ if and only if $|a|^{1/d} \in |k^\times|$.*

Proof. Clearly, the condition is necessary. Conversely, assume that $|a| = |b^d|$ for $b \in k$. It suffices to prove that $c = ab^{-d}$ is a d-th power in k, that is, the polynomial $f(t) = t^d - c$ has a root in k. Since $|c| = 1$ and $\widetilde{k}$ is separably closed, the reduction

$t^d - \widetilde{c}$ has d distinct roots in $\widetilde{k}$. So, by Hensel's lemma $f(t)$ even splits completely in $k[t]$. □

3.4.3. *The key result.* This time the key result concerns liftings of "separable" extensions of the group of values.

Theorem 3.4.4. *Assume that k is a strictly henselian valued field, $p = \mathrm{exp.char}(\widetilde{k})$, and $H \subseteq \sqrt{|k^\times|}$ is a subgroup such that $H/|k^\times|$ has no p-torsion. Then there exists a unique tame extension l/k such that $|l^\times| = H$. In addition, l/k is Galois with $\mathrm{Gal}_{l/k} = \mathrm{Hom}(H/|k^\times|, k^\times)$, and an algebraic extension F/k contains l if and only if $|H| \subseteq |l^\times|$.*

Proof. Assume first that H is generated over $|k^\times|$ by a single element r and let d be the smallest positive number such that $r^d \in |k^\times|$, say $r^d = |a|$ for $a \in k$. By our assumption $(d,p) = 1$. The extension $l = k(a^{1/d})$ satisfies $[l : k] \le d \le e_{l/k}$, hence the inequalities are equalities and we obtain that l/k is a tame extension with $|l^\times| = H$. Since k is strictly henselian and the polynomial $t^d - 1$ is separable over $\widetilde{k}$, all roots of unity of degree d lie in k. Then the usual theory of cyclic extensions implies that l/k is Galois and $\mathrm{Gal}_{l/k}$ is as claimed. Finally, since F is strictly henselian too, Lemma 3.4.2 implies that $l \subseteq F$ if and only if $H \subseteq |F^\times|$.

Next, we assume that $H/|k^\times|$ is finite. In this case the quotient is of the form $\prod_{i=1}^n \mathbb{Z}/d_i\mathbb{Z}$, and by the above case each factor corresponds to an extension $l_i = k(a_i^{1/d_i})$. The composite l of $l_1, \dots, l_n$ is an extension of k of degree bounded by $d = \prod_i d_i$. Since $H \subseteq |l^\times|$, we obtain that l/k is tame of degree d. In particular, $[l_i : k] = d_i$ and $G_{l/k} = \prod_{i=1}^l G_{l_i/k}$. Now, all assertions about l/k follow from the assertions about l_i/k.

Finally, if H is arbitrary, then it is a filtered union of subgroups H_j finitely generated over $|k^\times|$. We have proved that each H_j corresponds to a unique tame extensions l_j/k, and taking $l = \cup_j l_j$ one obtains a tame extension satisfying all assertions of the theorem. □

3.4.5. *Tame closure.* For any valued field k let $|k^\times|^{\mathbb{Z}_{(p)}}$ denote the group obtained from $|k^\times|$ by extracting all roots of elements of order prime to $p = \mathrm{exp.char}(\widetilde{k})$ and let k^t be the tame extension of k^u such that $|(k^t)^\times| = |k^\times|^{\mathbb{Z}_{(p)}}$. We call k^t the *tame closure* of k, and say that k is tamely closed if $k^t = k$. As we will immediately prove, this happens if and only if k has no non-trivial tame extensions.

Corollary 3.4.6. *If k is a valued field, then k^t is the maximal tame extension of k and the extension k^t/k^u is Galois with Gal_{k^t/k^u} being the dual group of $|k^\times|^{\mathbb{Z}_{(p)}}/|k^\times|$.*

Proof. The second claim follows from Theorem 3.4.4 because k^u/k is unramified and hence $|(k^u)^\times| = |k^\times|$. The extensions k^u/k and k^t/k^u are tame, hence k^t/k is tame. Finally, if l/k is tame, then l^u/k is tame and hence l^u/k^u is tame. Since $|(l^u)^\times|/|k^\times|$ has no p-torsion, $|(l^u)^\times| \subseteq |k^\times|^{\mathbb{Z}_{(p)}}$, and hence $l^u \subseteq k^t$ by Theorem 3.4.4. □

3.4.7. *Filtration on extensions.* The filtration $k^a/k^t/k$ induces filtration on all algebraic extensions l/k by setting $l_t = l \cap k^t$.

Corollary 3.4.8. *If l/k is an algebraic extension of henselian valued fields, then l_t is the only intermediate field such that l/l_t is purely wild and l_u/k is tame.*

Proof. It immediately follows from Theorem 3.4.4 that l_t is the tame extension of k such that $\widetilde{l_t}$ is the separable closure of $\widetilde{k}$ in $\widetilde{l}$ and $|l_t^\times|$ is the maximal subgroup of $|l^\times|$ whose quotient by $|k^\times|$ has no p-torsion. Therefore, l/l_t induces a purely inseparable extension of residue fields and any element of $|l^\times|/|l_t^\times|$ is killed by a power of p. In other words, l/l_t is purely wild. □

3.4.9. *Filtration on Galois groups.* Finally, let us look again at the Galois side.

Theorem 3.4.10. *Assume that l/k if a Galois extension of henselian valued fields. Then l_t/k is Galois and Gal_{l/l_t} is the wild inertia subgroup $W_{l/k}$ of $\mathrm{Gal}_{l/k}$.*

Proof. Any k-automorphism of k^a takes l to itself, hence it also takes its maximal tame subextension l_t to itself. So, l_t/k is Galois, and it remains to show that $\mathrm{Gal}_{l/l_t} = W_{l/k}$.

Let us show that any $\sigma \in \mathrm{Gal}_{l/l_t}$ lies in $W_{l/k}$, that is, $|\sigma(\alpha)-\alpha| < |\alpha|$ for any $\alpha \in l$. For a sequel use, we fix any extension of σ to an element of $\mathrm{Aut}(k^a/l_t)$ and denote it also by σ. Since l/l_t is purely wild, both $e = e_{l/l_t}$ and $f = f_{l/l_t}$ are powers of p. Choose $b \in l_t$ such that $|\alpha^e| = |b|$, and let $\beta = \alpha^e/b$. Since $\widetilde{l}/\widetilde{l_t}$ is purely inseparable of degree f, we have that $\widetilde{\beta}^f \in \widetilde{l_t}$ and hence $|\beta^f - c| < 1$ for an element $c \in l_t$. We obtain that $|\alpha^{ef} - a| < |\alpha^{ef}|$ for $a = b^f c \in l_t$, and since ef is a p-th power, this implies that $|\alpha - a^{1/ef}| < |\alpha|$ and hence also $|\sigma(\alpha) - \sigma(a^{1/ef})| < |\alpha|$. Note that σ takes $a^{1/ef}$ to $\xi a^{1/ef}$, where $\xi^{ef} = 1$. Therefore, $|\xi - 1| < 1$ and we have that $|\sigma(a^{1/ef}) - a^{1/ef}| < |a^{1/ef}| = |\alpha|$. Summarizing we obtain

$$|\sigma(\alpha)-\alpha| \le \max\left(\left|\sigma(\alpha)-\sigma(a^{1/ef})\right|, \left|\sigma(a^{1/ef}) - a^{1/ef}\right|, \left|a^{1/ef}-\alpha\right|\right) < |\alpha|.$$

Conversely, we should show that if $\sigma \in \mathrm{Gal}_{l/k}$ does not lie in Gal_{l/l_t}, then there exists $\alpha \in l$ such that $|\sigma(\alpha) - \alpha| = |\alpha|$. Assume to the contrary that such α does not exist. Since the image of σ in $\mathrm{Gal}_{l_t/l}$ is non-trivial it suffices to prove the latter claim for tame extensions. So, we can assume for simplicity that l/k is tame. Furthermore, replacing σ with its power we can assume that its order d is a prime number. Replacing k with l^σ we can further assume that $[l : k]$ is of Galois of prime degree d. If l/k is unramified, then σ acts non-trivially on $\widetilde{l}$ yielding a contradiction. In the remaining possible case, l/k is tame and so $d \ne p$. Find $\alpha \in l$ such that $|\alpha| \notin |k^\times|$. Then the same argument as was used few times shows that there exists $a \in k$ such that $|\alpha^d - a| < |a|$. It follows that $|\alpha - a^{1/d}| < |\alpha|$ in l^u. Since l/k is totally ramified, $\mathrm{Gal}_{l^u/k^u} = \mathrm{Gal}_{l/k}$. Any primitive d-th root of unity ξ satisfies $|\xi - 1| = 1$, hence $|\sigma(a^{1/d}) - a^{1/d}| = |a^{1/d}|$ and it follows that $|\sigma(\alpha) - \alpha| = |\alpha|$, a contradiction. □

3.5. **Wild inertia.**

3.5.1. *The key result.* Finally, let us study the bottom layer of the basic ramification filtration.

Theorem 3.5.2. *If k is a tamely closed field and $p = \mathrm{exp.char}(\widetilde{k})$, then k^a/k is a p-extension. In particular, if k is of residual characteristic zero, then it is tamely closed if and only if it is algebraically closed.*

Proof. If k^a/k is not a p-extension, then k^s/k is not a p-extension and using an l-Sylow subgroup we can find a tower of extensions $F/E/k$ such that F/E is Galois of a prime degree $l \ne p$. Note that E is tamely closed, in particular, it contains a primitive l-th root of unity ξ, and by Galois theory $F = E(\alpha)$, where $a = \alpha^l \in E$. Since E is tamely closed, $|E|$ is l-divisible and using Lemma 2.6.6 we obtain that a is an l-th power in E. This implies that $E = F$, a contradiction. $\square$

Here is an immediate corollary.

Corollary 3.5.3. *For any valued field k with $p = \exp.\mathrm{char}(\widetilde{k})$, the wild inertia group W_k is a pro-p-group. In particular, if $\mathrm{char}(\widetilde{k}) = 1$, then $W_k = 1$.*

Remark 3.5.4. This is the only information about W_k which is easy to obtain, and a finer description is often difficult. On the other hand, this implies that finite purely wild Galois extensions are solvable, the fact which allows to reduce various problems to the case of wild extensions of degree p.

Corollary 3.5.5. *If k is tamely closed, then any finite extension l/k splits into a tower of extensions of degree p and if l/k is of degree p then it is normal.*

Proof. It suffices to prove this separately for the purely inseparable extension l/l_s and the separable extension l_s/k. The first is obvious, and the second follows from the basic theory of p-groups: if G is a p-group and H is a subgroup, then there exists a chain $H = H_0 \subset H_1 \subset \ldots \subset H_n = G$ such that H_i is of index p in H_{i+1}, and if H is of index p in G, then it is normal. $\square$

Corollary 3.5.6. *If l/k is a finite extension of valued fields, then there exists a composite $l' = k'l$ such that k'/k is a finite tame extension, in particular, l'/k' is tame, and the extension l'/k' splits into a tower $l = l_0 \subset l_1 \subset \ldots \subset l_n = l$ of n purely wild extensions of degree p.*

3.5.7. *Applications to defect.* As another corollary we can finally bound the defect.

Corollary 3.5.8. *For any finite extension of valued fields l/k, the defect $d_{l/k}$ is a power of $p = \exp.\mathrm{char}(\widetilde{k})$.*

Proof. Note that $d_{l/k} = d_{l^h/k^h}$, hence we can assume that k is henselian. The extension l_t/k is defectless, hence $d_{l/k} = d_{l/l_t}$. In particular, replacing k by l_t we can also assume that l/k is purely wild. But in this case $e = e_{l/k}$ and $f = f_{l/k}$ are powers of p for obvious reasons, and $[l : k]$ is a power of p by Theorem 3.5.2. Since $ef \le [l : k]$ by the fundamental inequality, it follows that $d_{l/k} = [l : k]/ef$ is a natural power of p. $\square$

Remark 3.5.9. Unfortunately this qualitative result does not tell anything about the structure of extensions with defect. In a sense, it is just a "result of luck" – all involved numbers turned out to be powers of p for wildly ramified extensions, and then already the fundamental inequality implies that the defect is natural, and even a power of p.

3.6. **Wild extensions of degree p.**
In this section we will study wild extensions of henselian valued fields of degree p.

3.6.1. *The defectless case.* This case is very easy, but we will formulate results in a way that suggests how to proceed in the case with defect. For completeness, we also consider tame extensions when the same argument applies.

Lemma 3.6.2. *Assume that l/k is a defectless extension of henselian valued fields of prime degree q. Then,*

(i) For any $x \in l \setminus k$ the infimum $r_k(x) = \inf_{c \in k} |x - c|$ is achieved for some c_0 and $x - c_0$ is k-orthogonal.

(ii) If $x \in l$ is k-orthogonal, then $1, x, \ldots, x^{p-1}$ is a k-orthogonal basis.

(iii) If $x \in l$ is k-orthogonal and $q = \mathrm{char}(\widetilde{k})$, then there exists $a \in k$ such that $|x^p - a| < |a|$ and $|a| \leq |c^p - a|$ for any $c \in k$.

Proof. By Lemma 2.3.3 l/k possesses an orthogonal basis $B = \{b_0 = 1, b_1, \ldots, b_{q-1}\}$, where either $\widetilde{B}$ is the basis of $\widetilde{l}/\widetilde{k}$ or $|B|$ maps bijectively onto $|l^\times|/|k^\times|$. If $x = \sum c_i b_i$ with $c_i \in k$, then $c = c_0$ is as required in (i). A similar argument works in (ii), so we skip the details. We leave (iii) as an exercise. □

3.6.3. *Immediate case: the strategy of almost orthogonalization.* When l/k has defect the strategy is still to take any $\alpha \in l \setminus k$ and translate it by an appropriate $c \in k$. This time we cannot achieve that $\alpha - c$ becomes k-orthogonal, but we can make it "orthogonal enough". In particular, we will see in the end that the whole basis $1, (\alpha - c), \ldots, (\alpha - c)^{p-1}$ may become arbitrary close to being k-orthogonal. The main point will be to study how the minimal polynomial of $\alpha - c$ varies when $|\alpha - c|$ approaches $r_k(\alpha) := \inf_{c \in k} |\alpha - c|$

3.6.4. *Stabilization of the minimal polynomial.* For a polynomial $f(t) = \sum_{i=0}^d c_i t^i$ over a field k and a natural l we define the n-th *divided derivation* $f^{[n]}(t) = \sum_{i=n}^d \binom{i}{n} c_i t^{i-n}$. If $n!$ is invertible in k, then this is the rescaled derivation $f^{(n)}(t)/n!$, and the same formal expression provides a good intuition about $f^{[n]}$ in general. In particular, all natural formulas one would expect hold true. We say that α and its minimal polynomial are *stable* over k if any root β of a non-zero divided derivation $f^{[i]}$ of f satisfies $|\beta| > |\alpha|$. The following result clarifies the terminology.

Lemma 3.6.5. *If k is a henselian field and $\alpha \in k^a$ is stable over k, then for any $c \in k$ with $|c| \leq |\alpha|$, the element $\alpha + c$ is stable over k and the absolute values of the coefficients of the minimal polynomials of α and $\alpha + c$ are equal.*

Proof. If $f(t)$ is the minimal polynomial of α, then $f(t + c) = \sum f^{[i]}(c) t^i$. Since each non-zero $f^{(i)}(c)$ has no roots β with $|\beta| \leq |\alpha|$, it follows easily that $|f^{(i)}(c)| = |f^{(i)}(0)|$ whenever $|c| \leq |\alpha|$. The claim follows. □

Now, we establish stabilization in the immediate case.

Lemma 3.6.6. *Assume that l/k is an immediate extension of henselian valued fields of degree $p = \mathrm{char}(\widetilde{k})$ and $\alpha \in l \notin k$ is an element. Then there exists $c_0 \in k$ such that $\alpha - c_0$ and its minimal polynomial $f_{c_0}(t)$ are stable over k. Furthermore, in this case, $\alpha - c$ and f_c are stable for any $c \in k$ with $|\alpha - c_0| \leq |\alpha - c|$.*

Proof. Since l/k is immediate, $r = \inf |\alpha - c|$ is not achieved. Note that $f^{[p]} = 1$ has no roots, hence if $\beta \in k^a$ is a root of a non-zero $f^{[i]}$, then $[k(\beta) : k] \leq i < p$ and hence $k(\beta)/k$ is a defectless extension. In particular, $\inf_{c \in k} |\beta - c|$ is achieved and hence $|\alpha - \beta| > r$. It follows that there exists c_0, such that any root β of a non-zero derivation $f^{(i)}$ satisfies $|\alpha - \beta| > |\alpha - c_0|$. Since taking divided derivations is compatible with translation of the coordinate, it follows that $\alpha - c_0$ is stable, and then $\alpha - c$ is stable for any $c \in k$ with $|c - c_0| \leq |\alpha - c|$, which happens if and only if $|\alpha - c_0| \leq |\alpha - c|$. □

3.6.7. *Inequalities on the coefficients.* Next, let us study basic properties of stable polynomials.

Lemma 3.6.8. *Let l/k be as above and assume that $\alpha \in l/\setminus k$ and its minimal polynomial $f(t) = t^p + \sum_{i=0}^{p-1} c_i t^i$ are stable. Then $|c_j\alpha^{j-i}| \le |c_i|$ whenever $0 \le i \le j \le p-1$.*

Proof. Any root β of $f^{[i]}(t) = \sum_{j\ge i} c_j \binom{j}{i} t^{j-i}$ satisfies $|\beta| > |\alpha|$ and $|\binom{j}{i}| = 1$. The claim follows easily. □

Corollary 3.6.9. *Keep assumptions of Lemma 3.6.8. Then the minimal polynomial $f_\alpha(t) = t^p + \sum_{i=0}^{p-1} c_i t^i$ and $r = r_k(\alpha)$ satisfy the inequalities $|c_1| \le r^{p-1}$ and $|c_i| < r^{p-i}$ for $2 \le i \le p-1$.*

Proof. Translating α by elements of k we can make $|\alpha|$ arbitrarily close to r, while the stability of f_α and the values $|c_i|$ are preserved. By Lemma 3.6.8 $|c_i\alpha^i| < |c_0| = |\alpha^p|$ for $1 \le i \le p-1$, hence the limit argument proves that $|c_i| \le r^{p-i}$. Moreover, for $i > 1$ we have that $|c_i\alpha^{i-1}| \le |c_1| \le r^{p-1}$, and since $|\alpha| > r$, this implies that $|c_i| < r^{p-i}$. □

3.6.10. *Applications to immediate extensions.* Finally, we can describe the main outcome of almost orthogonalization.

Theorem 3.6.11. *Assume that l/k is an immediate extension of henselian valued fields of degree $p = \mathrm{char}(\widetilde{k})$, then*

(i) Any element of $\alpha_0 \in l \setminus k$ possesses a translation $\alpha \in \alpha_0 + k$ with minimal polynomial $f_\alpha = t^p + \sum_{i=0}^{p-1} c_i t^i$ such that $|p\alpha| < r := r_k(\alpha)$, $|c_i| < r^p/|\alpha|^i$ for $2 \le i \le p-1$, and either (a) $|c_1| = r^{p-1}$, or (b) $|c_1| < r^p/|\alpha|$.

(ii) Set $g(t) = t^p + c_0$ in case (b) and $g(t) = t^p + c_1 t + c_0$ in case (a), and let $\beta \in k^a$ be a root of g. Then $|\alpha - \beta| \le r$, $|g(\alpha)| \le r^p = \inf_{a\in k} |g(a)|$, and the latter infimum is not achieved.

Proof. By Lemma 3.6.6 translating α one can make it stable over k, and then the conditions of Corollary 3.6.9 are satisfies. Then decreasing $|\alpha|$ by an additional translation, we keep the absolute values of $|c_i|$ and can make $|\alpha|$ as close to r as needed. Clearly, this suffices to fulfil all conditions of (i). Furthermore, since $f(\alpha) = 0$, we obtain that $g(\alpha) = -\sum_{i=i_0}^{p-1} c_i t^i$, where i_0 is 1 in (b) and 2 in (a), and hence $|g(\alpha)| < \max(|c_i\alpha|^i) = r^p$.

Loosely speaking, the other claims in (ii) follows from the additivity of $t^p + c_1 t$ up to negligible terms. It is easy to see that $|\beta| = |c_0|^{1/p} = |\alpha|$, and hence $|(\alpha-\beta)^p - (\alpha^p - \beta^p)| \le |p\alpha^p| < r^p$. Therefore, if $|g(\alpha)| > r^p$, then $|g(\alpha)| = |g(\alpha) - g(\beta)| = |(\alpha-\beta)^p + c(\alpha-\beta)|$, where $c = c_1$ in case (a) and $c = 0$ otherwise. In either case, $|\alpha - \beta| \le r$ as otherwise we would have $|g(\alpha)| = |\alpha - \beta|^p > r^p$. The same computation with $a \in k$ instead of β establishes the last claim. □

3.6.12. *Rings of integers.* We say that an extension is *monogenic* if l° is generated over k° by a single element, say $l^\circ = k^\circ[x]$. Usually this is too restrictive, and we say that l/k is *almost monogenic* if there exists x such that l° is a union of subrings of the form $k^\circ[ax+b]$ with $a, b \in k$. In this case, we call x an *almost generator* of l° over k°. Note that the union is automatically filtered and $|a|$ is bounded from above by the inverse of $r_k(x)$.

Lemma 3.6.13. *Any defectless extension l/k of henselian valued fields of prime degree q is almost monogeneous. Furthermore, l/k is monogeneous if and only if either $f_{l/k} = q$ or $k^{\circ\circ}$ is a principal ideal.*

Proof. In the first case, $l^\circ = k^\circ[\alpha]$, where $\alpha \in l^\circ$ is such that $\widetilde{\alpha}$ is a primitive element of $\widetilde{l}/\widetilde{k}$. In the second case, $\widetilde{l} = \widetilde{k}[\pi]$, where $(\pi) = l^{\circ\circ}$. $\square$

4. Higher ramification

5. Transcendental extensions

References

[Ber90] Vladimir G. Berkovich, *Spectral theory and analytic geometry over non-Archimedean fields*, Mathematical Surveys and Monographs, vol. 33, American Mathematical Society, Providence, RI, 1990. MR 1070709 (91k:32038)

[Ber93] ———, *Étale cohomology for non-Archimedean analytic spaces*, Inst. Hautes Études Sci. Publ. Math. (1993), no. 78, 5–161 (1994). MR 1259429 (95c:14017)

[BGR84] S. Bosch, U. Güntzer, and R. Remmert, *Non-Archimedean analysis*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 261, Springer-Verlag, Berlin, 1984, A systematic approach to rigid analytic geometry. MR 746961 (86b:32031)

[Bou72] Nicolas Bourbaki, *Elements of mathematics. Commutative algebra*, Hermann, Paris; Addison-Wesley Publishing Co., Reading, Mass., 1972, Translated from the French. MR 0360549 (50 #12997)

[Gro67] A. Grothendieck, *Éléments de géométrie algébrique.*, Inst. Hautes Études Sci. Publ. Math. (1960-1967).

[Kür13] Josef Kürschák, *Über Limesbildung und allgemeine Körpertheorie*, J. Reine Angew. Math. **142** (1913), 211–253. MR 1580869

[Roq02] Peter Roquette, *History of valuation theory. I*, Valuation theory and its applications, Vol. I (Saskatoon, SK, 1999), Fields Inst. Commun., vol. 32, Amer. Math. Soc., Providence, RI, 2002, pp. 291–355. MR 1928376

Einstein Institute of Mathematics, The Hebrew University of Jerusalem, Giv'at Ram, Jerusalem, 91904, Israel

E-mail address: temkin@math.huji.ac.il