Model theory of valued fields
Lecture Notes

Lou van den Dries

Fall Semester 2004

Contents

1 Introduction **2**

2 Henselian local rings **5**
2.2 Hensel's Lemma 6
2.3 Completion 9
2.4 Lifting the residue field 13
2.5 The Ax-Kochen Principle 15

3 Valuation theory **20**
3.1 Valuation rings and integral closure 26
3.2 Quantifier elimination 30
3.3 The complete extensions of ACF_{val} 37

4 Immediate Extensions **39**
4.1 Pseudoconvergence 39
4.2 Maximal Valued Fields 44
4.3 Henselization 48
4.4 Uniqueness of immediate maximal extensions 50

5 The Theorem of Ax–Kochen and Ershov **52**
5.1 Existence of cross-sections in elementary extensions 52
5.2 Extending the value group 53
5.3 AKE-theorem with lifting and cross-section 54

6 Unramified Mixed Characteristic **59**
6.1 The Teichmüller Map 59
6.2 Witt vectors 61
6.3 Coarsening 70
6.4 AKE for unramified mixed characteristic 71

1 Introduction

Conventions. Throughout, m, n range over $\mathbb{N} = \{0, 1, 2, \dots\}$, the set of natural numbers. Unless specified otherwise, "ring" means "commutative ring with 1" and given a ring R we let $U(R) := \{x \in R : xy = 1 \text{ for some } y \in R\}$ be its multiplicative group of units, and for $a_1, \dots, a_n \in R$ we denote the ideal $a_1R + \cdots + a_nR$ of R also by $(a_1, \dots, a_n)R$ or just by $(a_1, \dots, a_n)$. A ring is considered as an L-structure for the language $L = \{0, 1, +, -, \cdot\}$ of rings. Given a ring R and distinct indeterminates $t_1, \dots, t_n$, we let $R[t_1, \dots, t_n]$ and $R[[t_1, \dots, t_n]]$ denote the corresponding polynomial ring and formal power series ring, with

$$R \subseteq R[t_1, \dots, t_n] \subseteq R[[t_1, \dots, t_n]].$$

Note that every $f \in R[[t_1, \dots, t_n]]$ can be written as

$$f = a + t_1 f_1 + \cdots + t_n f_n$$

where $a \in R$ and each $f_i \in R[[t_1, \dots, t_i]]$. The element a is uniquely determined by f and is called the *constant term of* f, and denoted by $f(0)$. Throughout, $\boldsymbol{k}, \boldsymbol{k}_1, \boldsymbol{k}_2$ are fields, and we put $\boldsymbol{k}^\times := \boldsymbol{k} \setminus \{0\} = U(\boldsymbol{k})$. Given a prime number p the field $\mathbb{Z}/p\mathbb{Z}$ of p elements is usually denoted by $\mathbb{F}_p$.

The goal of this course is the famous Ax-Kochen-Ersov Theorem from the 1960's. We shall prove this result in various stronger forms, and discuss applications. We begin by stating some very special cases of the theorem. Let t be a single indeterminate.

1.1. *Suppose* $\boldsymbol{k}_1$ *and* $\boldsymbol{k}_2$ *have characteristic* 0*. Then*

$$\boldsymbol{k}_1[[t]] \equiv \boldsymbol{k}_2[[t]] \iff \boldsymbol{k}_1 \equiv \boldsymbol{k}_2.$$

□

The direction $\Rightarrow$ is easy and holds also when $\boldsymbol{k}_1$ and $\boldsymbol{k}_2$ have characteristic $p > 0$, but the direction $\Leftarrow$ lies much deeper, and is not yet known to be true when $\boldsymbol{k}_1$ and $\boldsymbol{k}_2$ have characteristic $p > 0$. (This is one of the main open problems in the subject.) Recall that $\mathbb{Q}^{\mathrm{alg}} \equiv \mathbb{C}$, as fields, where $\mathbb{Q}^{\mathrm{alg}}$ is the algebraic closure of $\mathbb{Q}$, so as a special case of 1.1 we have $\mathbb{Q}^{\mathrm{alg}}[[t]] \equiv \mathbb{C}[[t]]$. On the other hand, $\mathbb{Q}^{\mathrm{alg}}[[t_1, t_2]] \not\equiv \mathbb{C}[[t_1, t_2]]$ and $\mathbb{Q}^{\mathrm{alg}}[t] \not\equiv \mathbb{C}[t]$. This highlights the fact that 1.1 is a *one-variable* phenomenon about *power series rings*: it fails for two or more variables, and also fails for polynomial rings instead of power series rings.

A stronger version of 1.1 is in terms of sentences:

1.2. *For every sentence* σ *in the language of rings, there is a sentence* $\overline{\sigma}$ *in that language, such that for all* $\boldsymbol{k}$ *of characteristic* 0*,*

$$\boldsymbol{k}[[t]] \models \sigma \iff \boldsymbol{k} \models \overline{\sigma}.$$

□

For the next result, let $\boldsymbol{k}[t_1,\dots,t_n]^{\rm alg}$ be the subring of $\boldsymbol{k}[[t_1,\dots,t_n]]$ consisting of all $f \in \boldsymbol{k}[[t_1,\dots,t_n]]$ that are algebraic over $\boldsymbol{k}[t_1,\dots,t_n]$.

1.3. *If $\boldsymbol{k}$ has characteristic 0, then $\boldsymbol{k}[t]^{\rm alg} \preccurlyeq \boldsymbol{k}[[t]]$.*

For any field $\boldsymbol{k}$ we have a weak version of 1.3 for n variables:

$$\boldsymbol{k}[t_1,\dots,t_n]^{\rm alg} \preccurlyeq_1 \boldsymbol{k}[[t_1,\dots,t_n]].$$

This is part of the Artin Approximation Theorems. Again, if $n \geq 2$, then $\boldsymbol{k}[t_1,\dots,t_n]^{\rm alg}$ is never an elementary substructure of $\boldsymbol{k}[[t_1,\dots,t_n]]$.

Next, let $\mathbb{C}[[t]]_{\rm conv}$ be the subring of $\mathbb{C}[[t]]$ consisting of the power series $f \in \mathbb{C}[[t]]$ that have a positive radius of convergence.

1.4. $\mathbb{C}[[t]]_{\rm conv} \preccurlyeq \mathbb{C}[[t]]$.

We also have $\mathbb{C}[[t_1,\dots,t_n]]_{\rm conv} \preccurlyeq_1 \mathbb{C}[[t_1,\dots,t_n]]$ for any n, but $\preccurlyeq_1$ cannot be replaced here by $\preccurlyeq$ for $n > 1$.

A key algebraic property of the power series rings $\boldsymbol{k}[[t_1,\dots,t_n]]$ is that they are *henselian local rings*. This property has a close connection to the theorems above, and distinguishes these power series rings from the polynomial rings $\boldsymbol{k}[t_1,\dots,t_n]$.

1.5 Definition. A ring R is *local* if it has exactly one maximal ideal. Given a local ring R, we denote its maximal ideal by $\mathfrak{m}$, and we let $\boldsymbol{k} = R/\mathfrak{m}$ be the residue field, with residue map

$$x \mapsto \bar{x} = x + \mathfrak{m} : R \to \boldsymbol{k}.$$

Local rings are exactly the models of a (finite) set of axioms in the language of rings, because a ring R is local iff its set of non-units is an ideal. (Even simpler, a ring R is local iff $1 \neq 0$ and its set of non-units is closed under addition.) Note also that an element x in a local ring is a unit iff $\bar{x} \neq 0$.

Examples.

1. Fields are exactly the local rings with $\mathfrak{m} = 0$.

2. $\boldsymbol{k}[[t_1,\dots,t_n]]$ is a local ring with $\mathfrak{m} = (t_1,\dots,t_n)$. This follows by the above decomposition of any $f \in R$ as a sum $f(0) + t_1 f_1 + \cdots + t_n f_n$, and by noting that $f \in U(R)$ iff $f(0) \neq 0$. The kernel of the ring morphism $f \mapsto f(0) : R \to \boldsymbol{k}$ is $\mathfrak{m}$, so this morphism induces a field isomorphism $R/\mathfrak{m} \to \boldsymbol{k}$. We shall usually identify the residue field $R/\mathfrak{m}$ with $\boldsymbol{k}$ via this isomorphism.

3. Let p be a prime number and k a positive integer. Then $\mathbb{Z}/p^k\mathbb{Z}$ is a local ring. The integers $a_0 + a_1 p + \cdots + a_{k-1}p^{k-1}$ with $a_i \in \{0,1,\dots,p-1\}$ are in one-to-one correspondence with their images in $\mathbb{Z}/p^k\mathbb{Z}$. The maximal ideal of this ring is generated by the image of p. The elements of this ring behave somewhat like power series in the "variable" p truncated at p^k.

4. Letting $k \to \infty$ in (3) we get the ring $\mathbb{Z}_p$ of p-adic integers. Its elements can be represented as infinite series $\sum_{i=0}^{\infty} a_i p^i$, where all $a_i \in \{0, 1, \ldots, p-1\}$. A precise definition is given in the next section.

All local rings in these examples are henselian, as we shall see in the next section. The localizations

$$\mathbb{Z}_{p\mathbb{Z}} = \{\frac{a}{b} : a, b \in \mathbb{Z}, b \notin p\mathbb{Z}\} \subseteq \mathbb{Q}, \quad (p \text{ a prime number}),$$

are examples of local rings that are not henselian.

1.6 Definition. Let R be a local ring. We say that R is *henselian* if for any polynomial $f(X) \in R[X]$ and any $\alpha \in R$ such that

$$f(\alpha) \in \mathfrak{m}, \qquad f'(\alpha) \notin \mathfrak{m},$$

there is $a \in R$ with $f(a) = 0$ and $a \equiv \alpha \mod \mathfrak{m}$.

1.7. Remark. By Lemma 2.1 below there can be at most one such a.

The henselian property means that non-singular zeros in the residue field can be lifted to the ring itself: let R be a local ring, $f(X) \in R[X]$, $\alpha \in R$; then

$$\begin{aligned} f(\alpha) \in \mathfrak{m} \text{ and } f'(\alpha) \notin \mathfrak{m} \quad &\iff \quad \bar{f}(\bar{\alpha}) = 0 \text{ and } \bar{f}'(\bar{\alpha}) \neq 0 \\ &\iff \quad \bar{\alpha} \text{ is a non-singular zero of } \bar{f}(X). \end{aligned}$$

(Here we let $\bar{f}(X)$ be the image of $f(X)$ in $\boldsymbol{k}[X]$ obtained by replacing each coefficient of f by its residue class.) Note that the henselian local rings are exactly the models of a certain set of sentences in the language of rings: this set consists of the axioms for local rings and has in addition for each $n > 0$ an axiom expressing the henselian property for polynomials of degree $\leq n$.
The Ax-Kochen-Ersov Theorem concerns a particular class of henselian local rings, namely henselian valuation rings. The rings $\boldsymbol{k}[[t]]$, $\boldsymbol{k}[[t]]^{\text{alg}}$, $\mathbb{C}[[t]]_{\text{conv}}$, and $\mathbb{Z}_p$ are indeed valuation rings, unlike $\boldsymbol{k}[[t_1, \ldots, t_n]]$ for $n > 1$, and $\mathbb{Z}/p^k\mathbb{Z}$ for $k > 1$.

1.8 Definition. A *valuation ring* is a domain R whose set of ideals is linearly ordered by inclusion.

Exercises. Prove the following:

1. Each valuation ring is a local ring.
2. Let R be a domain with fraction field K. Then R is a valuation ring iff for every $a \in K^\times$ either $a \in R$ or $a^{-1} \in R$.
3. $\boldsymbol{k}[[t]]$ is a valuation ring.
4. $\boldsymbol{k}[[t_1, \ldots, t_n]]$ is not a valuation ring if $n > 1$.

2 Henselian local rings

In this section we establish basic facts about henselian local rings, prove that complete local rings are henselian (Hensel's Lemma), show that under certain conditions the residue field of a henselian local ring can be lifted, and give a baby version of the Ax-Kochen Principle.

2.1. Lemma. *Let R be a local ring, $f(X) \in R[X]$, and $\alpha \in R$, such that*

$$f(\alpha) \in \mathfrak{m}, \qquad f'(\alpha) \notin \mathfrak{m}.$$

Then there is at most one $a \in R$ such that $f(a) = 0$ and $a \equiv \alpha \mod \mathfrak{m}$.

Proof. Suppose $a \in R$ satisfies $f(a) = 0$ and $a \equiv \alpha \mod \mathfrak{m}$. Then $f'(a) \equiv f'(\alpha) \mod \mathfrak{m}$, hence $f'(a)$ is a unit. Taylor expansion in $x \in \mathfrak{m}$ around a gives

$$\begin{aligned} f(a+x) = f(a) + f'(a)x + bx^2 &= f'(a)x + bx^2 \quad (b \in R) \\ &= f'(a)x\left[1 + f'(a)^{-1}bx.\right] \end{aligned}$$

Since $f'(a)\left[1 + f'(a)^{-1}bx\right] \in U(R)$, this gives: $f(a+x) = 0$ iff $x = 0$. □

2.2. Lemma. *Let R be a local ring. The following are equivalent.*

(1) R is henselian.

(2) Each polynomial $1 + X + cd_2X^2 + \cdots + cd_nX^n$, with $n \geq 2$, $c \in \mathfrak{m}$ and $d_2, \ldots, d_n \in R$, has a zero in $U(R)$.

(3) Each polynomial $Y^n + Y^{n-1} + cd_2Y^{n-2} + \cdots + cd_n$, with $n \geq 2$, $c \in \mathfrak{m}$ and $d_2, \ldots, d_n \in R$, has a zero in $U(R)$.

(4) [Newton Version] *Given a polynomial $f(X) \in R[X]$, $\alpha \in R$, and $c \in \mathfrak{m}$ such that $f(\alpha) = cf'(\alpha)^2$, there is $a \in R$ such that $f(a) = 0$ and $a \equiv \alpha \mod cf'(\alpha)$.*

The "Newton version" (4) gives extra precision in the henselian property when $f'(\alpha) \notin \mathfrak{m}$, but (4) is devised to deal also with the case $f'(\alpha) \in \mathfrak{m}$.

Proof. (1)⇒(2). Assume (1) and let $f(X) = 1 + X + cd_2X^2 + \cdots + cd_nX^n$ with $c \in \mathfrak{m}$ and $d_2, \ldots, d_n \in R$. Then for $\alpha = -1$ we have: $f(\alpha) \equiv 0 \mod \mathfrak{m}$ and $f'(\alpha) \equiv 1 \mod \mathfrak{m}$. Thus $f(X)$ has a zero in $-1 + \mathfrak{m} \subseteq U(R)$, by (1).

(2)⇔ (3). Use the substitution $X = 1/Y$.

(2)⇒(4). For f, α, c as in the hypothesis of (4), let $x \in R$ and consider the expansion:

$$\begin{aligned} f(\alpha + x) &= f(\alpha) + f'(\alpha)x + \sum_{i \geq 2} b_i x^i \\ &\qquad \text{where the } b_i \in R \text{ do not depend on } x \\ &= cf'(\alpha)^2 + f'(\alpha)x + \sum_{i \geq 2} b_i x^i \end{aligned}$$

Set $x = cf'(\alpha)y$ where $y \in R$. Then

$$f(\alpha + cf'(\alpha)y) = cf'(\alpha)^2 \left[1 + y + \sum_{i \geq 2} cd_i y^i\right],$$

where the $d_i \in R$ do not depend on y. Assuming (2), choose $y \in R$ such that

$$1 + y + \sum cd_i y^i = 0.$$

This yields an $a = \alpha + cf'(\alpha)y$ as required.

(4)⇒(1). Clear. □

Exercises. Let R be a henselian local ring, $m > 0$, and suppose $\operatorname{char} \boldsymbol{k}$ does not divide m (this includes the case $\operatorname{char} \boldsymbol{k} = 0$). Show that for $a \in U(R)$:

$$a \text{ is an } m\text{-th power in } R. \iff \bar{a} \text{ is an } m\text{-th power in } \boldsymbol{k}.$$

2.2 Hensel's Lemma

Hensel's Lemma says that *complete* local rings are henselian. Here is the idea of the proof. Let R be a local ring, and think of the elements in $\mathfrak{m}$ as *infinitesimals* (very small). Let $f(X) \in R[X]$ and $\alpha \in R$ be such that $f(\alpha) \in \mathfrak{m}$ and $f'(\alpha) \notin \mathfrak{m}$, so $f(\alpha)$ is tiny compared to $f'(\alpha)$. If $f(\alpha) \neq 0$ we can apply Newton's method to perturb α by a tiny amount x to make $f(\alpha + x)$ much smaller than $f(\alpha)$: Taylor expansion in $x \in R$ around α yields

$$\begin{aligned} f(\alpha + x) &= f(\alpha) + f'(\alpha)x + \text{terms of higher degree in } x \\ &= f'(\alpha)\left(f'(\alpha)^{-1} f(\alpha) + x + \text{terms of higher degree in } x\right) \end{aligned}$$

Setting $x = -f'(\alpha)^{-1} f(\alpha)$ yields $x \in \mathfrak{m}$ and

$$f(\alpha + x) = f'(\alpha)[\text{multiple of } f(\alpha)^2]$$

By the occurrence of $f(\alpha)^2$ as a factor in the above expression, this choice of x will make $f(\alpha+x)$ much smaller than $f(\alpha)$, provided we have a suitable norm on R by which to measure size. The process above can now be repeated with $\alpha + x$ in the role of α. Iterating this process indefinitely and assuming R is *complete* with respect to our norm, we can hope to obtain a sequence converging to some $a \in R$ such that $f(a) = 0$ and $a \equiv \alpha \mod \mathfrak{m}$. A precise version of this limit process occurs in the proof of Hensel's Lemma 2.7.

2.3 Definition. Let R be a ring. A *norm* on R is a function $|\ | : R \to \mathbb{R}^{\geq 0}$ such that for all $x, y \in R$:

(i) $|x| = 0 \iff x = 0, \quad |1| = |-1| = 1,$

(ii) $|x+y| \le |x| + |y|$,

(iii) $|xy| \le |x||y|$.

It follows easily that $|-x| = |x|$ for all $x \in R$, and thus we obtain a metric $d(x,y) = |x-y|$ on R; we consider R as a metric space with this metric if the norm $|\ |$ is clear from context. Note that then the operations

$$+, \cdot, - : R^2 \to R \quad \text{and} \quad |\ | : R \to \mathbb{R}$$

are continuous. We say that R is *complete* if it is complete as a metric space. If condition (ii) holds in the strong form

$$|x+y| \le \max\{|x|, |y|\},$$

then we call the norm an *ultranorm* (or ultrametric norm, or nonarchimedean norm). Note that then $|x+y| = \max\{|x|, |y|\}$ if $|x| \ne |y|$. When our norm is an ultranorm, then convergence of infinite series $\sum a_n$ is an easy matter:

2.4. Lemma. *Suppose the ring R is complete with respect to the ultranorm $|\ |$. Let (a_n) be a sequence in R. Then*

$$\lim_{n\to\infty} \sum_{i=0}^{n} a_i \text{ exists in } R \iff \lim_{n\to\infty} |a_n| = 0.$$

We leave the proof as an exercise. If the limit in this lemma exists, it is denoted by $\sum_{n=0}^{\infty} a_n$.

Example. Let A be a ring with $1 \ne 0$, and $R := A[[t_1, \ldots, t_n]]$. Each $f \in R$ has a unique representation

$$f = \sum a_{i_1 \ldots i_n} t_1^{i_1} \cdots t_n^{i_n}$$

where the formal sum is over all $(i_1, \ldots, i_n) \in \mathbb{N}^n$ and the coefficients $a_{i_1 \ldots i_n}$ lie in A. For such f we define $\operatorname{ord} f \in \mathbb{N} \cup \{\infty\}$ by

$$\operatorname{ord} f = \min\{i_1 + \cdots + i_n : a_{i_1 \ldots i_n} \ne 0\} \quad \text{if } f \ne 0,$$

and $\operatorname{ord} 0 = \infty$. This order function satisfies:

- $\operatorname{ord} 1 = 0$,
- $\operatorname{ord}(f+g) \ge \min\{\operatorname{ord}(f), \operatorname{ord}(g)\}$,
- $\operatorname{ord}(fg) \ge \operatorname{ord}(f) + \operatorname{ord}(g)$.

It follows that $|f| := 2^{-\operatorname{ord} f}$ defines an ultranorm on R.

Exercise. Show that R is complete with respect to this norm, and has the polynomial ring $A[t_1, \ldots, t_n]$ as a dense subring.

2.5. Remark. Let the ring R be complete with respect to the norm $|\ |$, and let $x \in R$ satisfy $|x| < 1$. Then $\sum_{i=0}^{\infty} x^i := \lim_{N\to\infty} \sum_{i=0}^{N} x^i$ exists in R, and

$$(1-x)\sum_{i=0}^{\infty} x^i = 1.$$

In the next two lemmas and subsequent exercise, R is a ring complete with respect to the ultranorm $|\ |$, and $|x| \le 1$ for all $x \in R$.

2.6. Lemma. *The set $\mathfrak{N} = \{x \in R : |x| < 1\}$ is an ideal. If $a \in R$, then*

$$a \in U(R) \iff \bar{a} \in U(\overline{R}), \quad \text{where } \overline{R} := R/\mathfrak{N},\ \bar{a} := a + \mathfrak{N}.$$

Proof. The direction $\Rightarrow$ is obvious. Conversely, let $a \in R$ be such that $\bar{a} \in U(\overline{R})$. Take $b \in R$ such that $ab = 1 - x$ with $x \in \mathfrak{N}$. Then $1 - x$ is a unit in R by the above remark. Hence $a \in U(R)$ and $a^{-1} = b\sum_{i=0}^{\infty} x^i$. □

2.7. Hensel's Lemma. *Let $f(X) \in R[X]$, and let $\alpha \in R$ be such that*

$$|f(\alpha)| < 1, \qquad f'(\alpha) \in U(R).$$

Then there is a unique $a \in R$ such that $f(a) = 0$ and $|a - \alpha| < 1$.

Proof. We shall obtain a as the limit of a sequence $\{a_n\}$ in R. Put $a_0 := \alpha$ and $\varepsilon := |f(\alpha)| < 1$. Suppose $a_n \in R$ is such that

$$|f(a_n)| \le \varepsilon^{2^n}, \qquad |a_n - \alpha| \le \varepsilon.$$

(Clearly this is true for $n = 0$.) Note that $a_n \equiv \alpha \mod \mathfrak{N}$, so $f'(a_n)$ is a unit because $f'(\alpha)$ is. Now, put

$$a_{n+1} := a_n + h, \quad \text{where} \quad h = -f'(a_n)^{-1} f(a_n).$$

Then:

$$\begin{aligned} f(a_{n+1}) &= f(a_n) + f'(a_n)h + \text{multiple of } h^2 \\ &= 0 + \text{multiple of } f(a_n)^2, \end{aligned}$$

hence

$$|f(a_{n+1})| \le |f(a_n)|^2 \le (\varepsilon^{2^n})^2 = \varepsilon^{2^{n+1}}.$$

Also,

$$|a_{n+1} - \alpha| \le \max\{|a_{n+1} - a_n|, |a_n - \alpha|\} \le \varepsilon,$$

so the induction step is complete. We have

$$|a_{n+1} - a_n| \ = \ |h| \ \le \ |f(a_n)| \ \le \ \varepsilon^{2^n},$$

so $\{a_n\}$ is a Cauchy sequence. Let $a \in R$ be its limit. Then

$$f(a) = f(\lim a_n) = \lim f(a_n) = 0.$$

The condition $|a_n - \alpha| \leq \varepsilon$ for all n insures that $|a - \alpha| \leq \varepsilon < 1$. The uniqueness of a follows exactly as in the proof of Lemma 2.1. □

Exercise. Let $f_1, \ldots, f_N \in R[X]$ where $X = (X_1, \ldots, X_N)$ is a tuple of distinct indeterminates. Suppose $\alpha \in R^N$ is a "near zero" of $f_1, \ldots, f_N$, that is,

$$|f_i(\alpha)| < 1 \text{ for } i = 1, \ldots, N, \text{ and } \det\left(\frac{\partial f_i}{\partial x_j}(\alpha)\right)_{i,j} \text{ is a unit in } R.$$

Then there is a unique $a \in R^N$ such that $f_1(a) = \cdots = f_N(a) = 0$, and $a \equiv \alpha \bmod \mathfrak{N}$ componentwise.

Hint. Put $f = (f_1, \ldots, f_N) \in R[X]^N$. Check that in $R[X]^N$ we have an identity

$$f(\alpha + X) = f(\alpha) + f'(\alpha)X + \text{terms of degree} \geq 2 \text{ in } X,$$

where $f'(\alpha)$ is the matrix $\left(\frac{\partial f_i}{\partial X_j}(\alpha)\right)_{i,j}$, and in the matrix product $f'(\alpha)X$ we view X as an $N \times 1$ matrix. Verify that the proof of Hensel's Lemma goes through.

2.3 Completion

Let $(R, |\ |)$ be a normed ring, that is, R is a ring, and $|\ |$ is a norm on R. As a metric space, R has a completion $\widehat{R}$, and the ring operations $+, -, \cdot : R^2 \to R$ extend uniquely to continuous operations $+, -, \cdot : \widehat{R}^2 \to \widehat{R}$. With these extended operations $\widehat{R}$ is again a ring. The norm $|\ | : R \to \mathbb{R}$ also extends uniquely to a continuous function $\widehat{|\ |} : \widehat{R} \to \mathbb{R}$, and $\widehat{|\ |}$ is a norm on the ring $\widehat{R}$ whose corresponding metric is the metric of the complete metric space $\widehat{R}$. We have now a complete normed ring $(\widehat{R}, \widehat{|\ |})$ in which R is a dense subring. If $(R', |\ |')$ is a second complete normed ring extending the normed ring $(R, |\ |)$ such that R is dense in R', then there is a unique normed ring isomorphism $(\widehat{R}, \widehat{|\ |}) \cong (R', |\ |')$ that is the identity on R. Thus we have the right to call $(\widehat{R}, \widehat{|\ |})$ *the* completion of the normed ring $(R, |\ |)$; to keep notations simple we usually write $|\ |$ for the norm $\widehat{|\ |}$ on $\widehat{R}$.

If $|xy| = |x||y|$ for all $x, y \in R$, then we call $|\ |$ an *absolute value*, and in that case R is a domain, and $|\ |$ extends uniquely to an absolute value on the fraction field. If K is a field with absolute value $|\ |$, then the map $x \mapsto x^{-1}$ on $K^\times$ is continuous, and the completion $\widehat{K}$ of K with respect to $|\ |$ is a field, and the extended norm is again an absolute value. In this case, for any subring $R \subseteq K$, the closure of R in $\widehat{K}$ is a subring, and is thus the completion of R with respect to the restricted norm.

Suppose that $R = A[[t_1, \ldots, t_n]]$ with A a domain. Then its norm given by $|f| = 2^{-\mathrm{ord}(f)}$ is an absolute value. Note that R is complete with respect to this

norm. If $A = \boldsymbol{k}$ is a field, then the ring $R = \boldsymbol{k}[[t]]$ is a valuation ring, and its fraction field K is also complete with respect to the extended absolute value. In this fraction field we have $R = \{f \in K : |f| \leq 1\}$. One can identify K in this case with the field of Laurent series $\boldsymbol{k}((t))$.

The field of p-adic numbers. Let p be a prime number. For $a \in \mathbb{Z}$ we define $v_p(a) \in \mathbb{N} \cup \{\infty\}$ as follows: if $a \neq 0$, then $v_p(a)$ is the natural number such that $a = p^{v_p(a)}b$ where $b \in \mathbb{Z}$ and $p \nmid b$, and $v_p(0) = \infty$. It is clear that then for all $a, b \in \mathbb{Z}$:

1. $v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$,
2. $v_p(ab) = v_p(a) + v_p(b)$,
3. $v_p(1) = 0$.

This yields an absolute value $|\ |_p$ on $\mathbb{Z}$ by setting

$$|a|_p = p^{-v_p(a)}.$$

(The reason we defined $|a|_p$ in this way with base p, instead of setting $|a|_p = 2^{-v_p(a)}$ with base 2, is to have $|a| \prod_p |a|_p = 1$ for all nonzero $a \in \mathbb{Z}$, where now the product is over all prime numbers p. Taking logarithms this identity becomes $\log|a| - \sum_p v_p(a) \log p = 0$, which mimicks the identity $\deg f - \sum_{P \in \mathbb{C}} v_P(f) = 0$ for non-zero $f \in \mathbb{C}[X]$. Here $v_P(f)$ is the *order of vanishing* of f at the point P; a precise definition is given later. This strenghtens the analogy between the ring $\mathbb{Z}$ and the polynomial ring $\mathbb{C}[X]$. This analogy can be pushed much further and is very productive in number theory.)

The absolute value $|\ |_p$ extends uniquely to an absolute value on $\mathbb{Q}$, which we call the *p-adic absolute value*. The completion of $\mathbb{Q}$ with respect to the p-adic absolute value is denoted by $\mathbb{Q}_p$, and called *the field of p-adic numbers*. The closure of $\mathbb{Z}$ in $\mathbb{Q}_p$ is denoted by $\mathbb{Z}_p$. By previous remarks $\mathbb{Z}_p$ is a subring of $\mathbb{Q}_p$, and is the completion of $\mathbb{Z}$ with respect to its p-adic norm. We call $\mathbb{Z}_p$ *the ring of p-adic integers*. Thus we have the following diagram where all maps are inclusions:

$$\begin{array}{ccc} \mathbb{Z}_p & \longrightarrow & \mathbb{Q}_p \\ \uparrow & & \uparrow \\ \mathbb{Z} & \longrightarrow & \mathbb{Q} \end{array}$$

Since $|a|_p \leq 1$ for $a \in \mathbb{Z}$, this remains true for $a \in \mathbb{Z}_p$. Here are some of the most basic facts about p-adic numbers:

2.8. Proposition. *Given any sequence (a_n) of integers, $\lim_{n\to\infty} \sum_{i=0}^{n} a_i p^i$ exists in $\mathbb{Z}_p$, and for $a = \sum_{n=0}^{\infty} a_n p^n$ we have the equivalences*

$$p|a_0 \iff a \in p\mathbb{Z}_p \iff |a|_p < 1 \iff a \notin U(\mathbb{Z}_p).$$

Moreover:

(i) the map $(a_n) \mapsto \sum_{n=0}^{\infty} a_n p^n : \{0, 1, \ldots, p-1\}^{\mathbb{N}} \to \mathbb{Z}_p$ *is a bijection;*

(ii) $\mathbb{Z}_p$ *is a henselian local ring with maximal ideal* $p\mathbb{Z}_p$*;*

(iii) for each integer $k > 0$ *the ring morphism* $\mathbb{Z} \to \mathbb{Z}_p/p^k\mathbb{Z}_p$ *is surjective with kernel* $p^k\mathbb{Z}$*, and thus induces a ring isomorphism*

$$\mathbb{Z}/p^k\mathbb{Z} \;\to\; \mathbb{Z}_p/p^k\mathbb{Z}_p.$$

For $k = 1$ *this isomorphism identifies* $\mathbb{F}_p$ *with the residue field of* $\mathbb{Z}_p$*.*

(iv) each nonzero $x \in \mathbb{Q}_p$ *is of the form* $x = p^k u$ *with unique integer exponent* k *and* $u \in U(\mathbb{Z}_p)$*.*

(v) $\mathbb{Z}_p \;=\; \{x \in \mathbb{Q}_p : |x|_p \leq 1\} \;=\; \{x \in \mathbb{Q}_p : |x|_p < p\}$*.*

(vi) $\mathbb{Z}_p$ *is open and closed in* $\mathbb{Q}_p$*, and is compact.*

Proof. Let (a_n) be a sequence in $\mathbb{Z}$. By Lemma 2.4 the series $\sum_{n=0}^{\infty} a_n p^n$ converges, since $|a_n p^n|_p \leq p^{-n} \to 0$ as $n \to \infty$. Put $a := \sum_{n=0}^{\infty} a_n p^n$. If $p|a_0$, then $a_0 = pb$ with $b \in \mathbb{Z}$, so

$$a = a_0 + p\sum_{n=0}^{\infty} a_{n+1}p^n = p(b + \sum_{n=0}^{\infty} a_{n+1}p^n) \in p\mathbb{Z}_p.$$

The implications $a \in p\mathbb{Z}_p \Rightarrow |a|_p < 1$, and $|a|_p < 1 \Rightarrow a \notin U(\mathbb{Z}_p)$ follow from $|p|_p < 1$ and the fact that $|x|_p \leq 1$ for all $x \in \mathbb{Z}_p$. We obtain the implication $a \notin U(\mathbb{Z}_p) \Rightarrow p|a_0$ by proving its contrapositive: Suppose that $p \nmid a_0$. Take $b \in \mathbb{Z}$ with $a_0 b = 1 + pk$, $k \in \mathbb{Z}$. Then

$$ab = 1 + p\sum_{n=0}^{\infty} c_n p^n, \qquad c_0 := k + a_1 b,\ c_n = a_{n+1}b \text{ for } n > 0.$$

Since $|p\sum_{n=0}^{\infty} c_n p^n|_p \leq p^{-1} < 1$, it follows from Remark 2.5 that $ab \in U(\mathbb{Z}_p)$, hence $a \in U(\mathbb{Z}_p)$.

As to (i), to prove injectivity, let (a_n) and (b_n) be two distinct sequences in $\{0, 1, \ldots, p-1\}$, and $a = \sum_{n=0}^{\infty} a_n p^n$, $b = \sum_{n=0}^{\infty} b_n p^n$. Let m be the least n such that $a_n \neq b_n$. Then $a - b = p^m(\sum_{i=0}^{\infty}(a_{m+i} - b_{m+i})p^i) \neq 0$, since $p \nmid (a_m - b_m)$. For surjectivity, let A be the image of the map in (i). We claim that, given any $k \in \mathbb{Z}$ and real $\epsilon > 0$ there is $a \in A$ such that $|k - a|_p < \epsilon$. To see this, take n such that $p^{-n} \leq \epsilon$, and take $a_0, \ldots, a_{n-1} \in \{0, 1, \ldots, p-1\}$ such that $k \equiv a_0 + a_1 p + \cdots + a_{n-1}p^{n-1} \mod p^n$, so $a = a_0 + a_1 p + \cdots + a_{n-1}p^{n-1} + p^n b$ with $b \in \mathbb{Z}$, hence $|a - (a_0 + a_1 p + \cdots + a_{n-1}p^{n-1})|_p \leq p^{-n} < \epsilon$. This proves our claim, which says that $\mathbb{Z}$ is contained in the closure of A. It remains to show that A is closed in $\mathbb{Z}_p$. We equip the finite set $\{0, 1, \ldots, p-1\}$ with the discrete topology, and give $\{0, 1, \ldots, p-1\}^{\mathbb{N}}$ the corresponding product topology, making this set of sequences a compact hausdorff space (by Tychonov). It is easily checked that the map in (i) is continuous, so A is compact, hence A is closed in $\mathbb{Z}_p$.

Item (ii): By (i) and what we proved before (i), the set of nonunits in $\mathbb{Z}_p$ is the ideal $\{x \in \mathbb{Z}_p : |x|_p < 1\} = p\mathbb{Z}_p$. Hence $\mathbb{Z}_p$ is a local ring with maximal ideal $p\mathbb{Z}_p$. Since $\mathbb{Z}_p$ is complete with respect to $|\ |_p$, it is henselian by Hensel's Lemma.

Item (iii): Let k be a positive integer and $a \in \mathbb{Z}_p$. By (i) we have $a = a_0 + a_1 p + \cdots + a_{k-1}p^{k-1} + p^k b$ with $a_0, \ldots, a_{p-1} \in \{0, \ldots, p-1\}$ and $b \in \mathbb{Z}_p$, so $a + p^k\mathbb{Z}_p = (a_0 + a_1 p + \cdots + a_{k-1}p^{k-1}) + p^k\mathbb{Z}_p$. This gives surjectivity of the map in (iv). Suppose $\ell \in \mathbb{Z}$ lies in the kernel of this map, that is, $\ell = p^k b$ with $b \in \mathbb{Z}_p$. To show that $\ell \in p^k\mathbb{Z}$ we can replace ℓ by $\ell + p^k q$ where $q \in \mathbb{Z}$, and thus we can assume that $\ell = b_0 + b_1 p + \cdots + b_{k-1}p^{k-1}$ where the "base p-digits" b_i lie in $\{0, \ldots, p-1\}$. So $p^k b = b_0 + b_1 p + \cdots + b_{k-1}p^{k-1}$, and by the injectivity in (i) this yields $b_0 = \cdots = b_{k-1} = 0$.

Item (iv): By the above, each nonzero $a \in \mathbb{Z}_p$ has the form $p^n u$ with $u \in U(\mathbb{Z}_p)$, and we note that this determines n by $|a|_p = p^{-n}$. Using this fact, the set $K := \{a/p^m : a \in \mathbb{Z}_p, m \in \mathbb{N}\}$ is easily seen to be a subfield of $\mathbb{Q}_p$. Note that each non-zero $x \in K$ has the form $p^k u$ with $k \in \mathbb{Z}$ and $u \in U(\mathbb{Z}_p)$, and that then $|x|_p = p^{-k}$, so k and u are uniquely determined by x. It follows that if $x \in K$ and $|x|_p \leq 1$, then $x \in \mathbb{Z}_p$. It remains to show that $K = \mathbb{Q}_p$, and since $\mathbb{Q}_p$ is the closure of $\mathbb{Q}$, this will follow by showing that K is closed in $\mathbb{Q}_p$. Let (a_n) be a sequence in K converging to $a \in \mathbb{Q}_p$. Then the sequence $(|a_n|_p)$ is bounded, so we can take $k \in \mathbb{N}$ such that $|a_n|_p \leq p^k$ for all n, hence $|p^k a_n|_p \leq 1$ for all n, and thus $p^k a_n \in \mathbb{Z}_p$ for all n. Since $(p^k a_n)$ is a Cauchy sequence, it converges to an element $b \in \mathbb{Z}_p$, hence (a_n) converges to $b/p^k \in K$, that is, $a = b/p^k \in K$.

Item (v): The proof of (iv) shows $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$, and also that the p-adic norm of any $x \in \mathbb{Q}_p^\times$ is of the form p^k with $k \in \mathbb{Z}$. So if $x \in \mathbb{Q}_p$ and $|x|_p < p$, then $|x|_p \leq 1$.

Item (vi): that $\mathbb{Z}_p$ is open and closed in $\mathbb{Q}_p$ is immediate from (v), and that $\mathbb{Z}_p$ is compact follows from (i) and its proof: the map in (i) is a continuous bijection from the compact hausdorff space $\{0, 1, \ldots, p-1\}^{\mathbb{N}}$ onto $\mathbb{Z}_p$, so this map is even a homeomorphism. □

Note that the familiar base p representation of a natural number is extended in (i) to all p-adic integers: the natural numbers are exactly the p-adic integers whose base p representation $\sum a_n p^n$ as in (i) has $a_n = 0$ for all sufficiently large n. In connection with (vi), note that every $a \in \mathbb{Q}_p$ has a compact open neighborhood $a + \mathbb{Z}_p$.

Exercises. Find the base p representation of -1 as in (i). Prove:

1. $\mathbb{Z}_p$ is a valuation ring;
2. the $p^n\mathbb{Z}_p$ are exactly the nonzero ideals of $\mathbb{Z}_p$;
3. $\mathbb{Z}_p \cap \mathbb{Q} = \mathbb{Z}_{p\mathbb{Z}}$.

2.4 Lifting the residue field

Suppose R is a local ring with a subfield E, that is, E is a subring that happens to be a field. Then E is mapped isomorphically onto a subfield $\bar{E}$ of the residue field $\boldsymbol{k}$ by the residue map $x \mapsto \bar{x}$. (Why?) In case $\bar{E} = \boldsymbol{k}$ we call E a *lift* of $\boldsymbol{k}$. (Example: if $R = \mathbb{C}[[t]]$, then the subfield $\mathbb{C}$ is such a lift. Non-example: let p be a prime number; then $\mathbb{Z}/p^2\mathbb{Z}$ is a local ring but has no subfield.)

Suppose $\bar{E} \neq \boldsymbol{k}$. It would be nice if we could extend E to a lift of $\boldsymbol{k}$. In what follows we indicate how to do this. Let $y \in \boldsymbol{k} \setminus \bar{E}$ and take $x \in R$ such that $\bar{x} = y$.

Case 1. y is transcendental over $\bar{E}$. For $f(X) \in E[X] \setminus \{0\}$, we have $\bar{f}(X) \in \bar{E}[X] \setminus \{0\}$, hence $\overline{f(x)} = \bar{f}(y) \neq 0$, so $f(x) \in U(R)$. In particular, the subring $E[x]$ of R is mapped isomorphically onto the subring $\bar{E}[y]$ of $\boldsymbol{k}$ by the residue map. Thus $E[x]$ is a domain with fraction field $E(x)$ inside R, and $E(x)$ is mapped isomorphically onto the subfield $\bar{E}(y)$ of $\boldsymbol{k}$.

In this case we found a subfield $E(x)$ of R that strictly contains E.

Case 2. y is algebraic over E. Take the monic polynomial $f(X) \in E[X]$ such that its image $\bar{f}(X) \in \bar{E}[X]$ is the minimum polynomial of y over $\bar{E}$. Note that $f(X) \in E[X]$ is irreducible, since $\bar{f}(X) \in \bar{E}[X]$ is. We have a surjective ring morphism

$$a \mapsto \bar{a} : E[x] \to \bar{E}[y],$$

where $E[x]$ is a subring of R and $\bar{E}[y]$ is a subfield of $\boldsymbol{k}$. If we happened to be so lucky that $f(x) = 0$, then this map would be injective (why?), and we would have extended E to a strictly larger subfield $E[x]$ of R. In general $f(x) \neq 0$, but if we can find an $\epsilon \in \mathfrak{m}$ such that $f(x + \epsilon) = 0$, then we can replace in the above argument x by $x + \epsilon$, and $E[x + \epsilon]$ would be a subfield of R that strictly contains E.

To find such an ϵ we assume at this point that R *is henselian and* $\operatorname{char} \boldsymbol{k} = 0$. We have $\overline{f(x)} = \bar{f}(y) = 0$, that is, $f(x) \in \mathfrak{m}$. Since $\operatorname{char} \boldsymbol{k} = 0$, the irreducible polynomial $\bar{f}(X) \in \bar{E}[X]$ is separable, so $\bar{f}'(y) \neq 0$, that is, $f'(x) \notin \mathfrak{m}$. The henselian assumption on R now yields an $\epsilon \in \mathfrak{m}$ such that $f(x + \epsilon) = 0$, as desired.

This discussion leads to the following important result.

2.9. Theorem. *Let R be a henselian local ring with* $\operatorname{char} \boldsymbol{k} = 0$. *Then the residue field $\boldsymbol{k}$ can be lifted.*

Proof. The unique ring morphism $\mathbb{Z} \to R$ is injective, and as usual we identify $\mathbb{Z}$ with its image in R via this morphism. Each non-zero integer in R is a unit since its residue class is, so $\mathbb{Z}$ has a fraction field in R. Thus we have found a subfield of R. By Zorn's lemma there is a maximal subfield of R; by the earlier discussion, a maximal subfield of R is a lift of $\boldsymbol{k}$. □

In some cases this lift allows us to completely describe a local ring R in terms of its residue field. Here is such a case:

2.10 Proposition. *Let R be a local ring, with $t \in R$ and n such that:*

$$\operatorname{char} \boldsymbol{k} = 0, \qquad \mathfrak{m} = tR, \qquad t^n \neq 0, \qquad t^{n+1} = 0. \tag{1}$$

Then we have a ring isomorphism $R \cong \boldsymbol{k}[T]/(T^{n+1})$.

A first step in proving this proposition is to show that a local ring R as in the proposition is henselian. This will follow from the next elementary result.

2.11. Lemma. *Let R be a local ring and let $t \in R$ be such that $\mathfrak{m} = tR$. Let $A \subseteq R$ be a set of representatives modulo $\mathfrak{m}$, that is, A maps bijectively onto $\boldsymbol{k}$ via the residue map. Then we can expand in powers of t with coeffficients in A:*

(1) For any n, each $r \in R$ is of the form

$$r = a_0 + a_1 t + \cdots + a_n t^n + s t^{n+1}$$

with $a_0, \ldots, a_n \in A$ and $s \in R$.

(2) If $t^n \neq 0$, then $t^m \notin t^{m+1}R$ for $m \leq n$, and the tuple $(a_0, \ldots, a_n)$ in (1) is uniquely determined by n, r.

(3) If $t^n \neq 0$ and $t^{n+1} = 0$, then the map

$$(a_0, \ldots, a_n) \mapsto a_0 + a_1 t + \cdots + a_n t^n : A^{n+1} \to R$$

is a bijection.

Proof of Lemma. Let $r \in R$. We establish (1) by induction on n. We have $r \equiv a_0 \mod \mathfrak{m}$ with $a_0 \in A$, that is, $r = a_0 + st$ with $s \in R$. This proves the case $n = 0$. Suppose $r = a_0 + a_1 t + \cdots + a_n t^n + s t^{n+1}$ as in (1). Since $s = a_{n+1} + ut$ with $a_{n+1} \in A$ and $u \in R$, this gives

$$r = a_0 + a_1 t + \cdots + a_n t^n + a_{n+1} t^{n+1} + u t^{n+2}.$$

For (2), suppose $t^n \neq 0$, and $t^m = t^{m+1} r$ with $r \in R$. Then $t^m(1 - tr) = 0$, hence $t^m = 0$ since $1 - tr$ is a unit. This forces $m > n$. Next suppose

$$a_0 + a_1 t + \cdots + a_n t^n \equiv b_0 + b_1 t + \cdots + b_n t^n \mod t^{n+1},$$

where $a_i, b_i \in A$. Suppose $a_i \neq b_i$ for some $i \leq n$, and let m be the least i with this property. After subtracting the first m terms from each side we get $a_m t^m \equiv b_m t^m \mod t^{m+1}$, hence $(a_m - b_m) t^m \in t^{m+1} R$. But $a_m \not\equiv b_m \mod \mathfrak{m}$, so $a_m - b_m \in U(R)$, and thus $t^m \in t^{m+1} R$, a contradiction. Item (3) follows immediately from (1) and (2). □

Proof of Proposition 2.10. Let R, t and n be as in the hypothesis of the proposition. By (2) of the lemma above we have a strictly descending sequence of ideals

$$R = t^0 R \supset tR \supset \cdots \supset t^n R \supset t^{n+1} R = 0.$$

With this we can define an ultranorm $|\ |$ on R,

$$|r| = \begin{cases} 2^{-m} & \text{if } r \neq 0,\ m = \max\{i : r \in t^i R\} \\ 0 & \text{if } r = 0 \end{cases} .$$

Note that $|r| \leq 1$ for all $r \in R$, and $|r| < 1$ if and only if $r \in \mathfrak{m}$. Since the norm takes only finitely many values, R is complete in this norm. Thus by Hensel's Lemma R is henselian. By Theorem 2.9 there is a ring embedding $j : \boldsymbol{k} \to R$ such that $\bar{j}x = x$ for all $x \in \boldsymbol{k}$, so $A := j(\boldsymbol{k})$ is a set of representatives modulo $\mathfrak{m}$. We extend j to a ring morphism $j_t : \boldsymbol{k}[T] \to R$ by sending T to t. By (1) of the above lemma the map j_t is surjective, and by (2) we have $\ker j_t = (T^{n+1})$. Thus j_t induces a ring isomorphism $\boldsymbol{k}[T]/(T^{n+1}) \cong R$. □

Exercises. Prove the following:

1. Let $R := \boldsymbol{k}[T]/(T^{n+1})$, and let t be the image of T under the canonical map $\boldsymbol{k}[T] \to R$. Then R is a henselian local ring with maximal ideal tR.
2. Let p be a prime number, and $R := \mathbb{Z}/(p^{n+1})$ and let t be the image of p under the canonical map $\mathbb{Z} \to R$. Then R is a henselian local ring with maximal ideal tR.

2.5 The Ax-Kochen Principle

At this point we shall bring a little logic into the picture. In what follows L_t is the language of rings augmented by a new constant symbol t, that is $L_t = L \cup \{t\}$. Here is an easy consequence of Proposition 2.10:

2.12. Corollary. *For each sentence σ in the language L_t there is a sentence σ_n in L such that for any R, n and t as in Proposition 2.10,*

$$(R, t) \models \sigma \iff \boldsymbol{k} \models \sigma_n.$$

Note the resemblance between this result and 1.2 in the introduction. This corollary yields a "baby" Ax-Kochen principle, but for that we need one more lemma:

2.13. Lemma. *For each L-sentence τ there is an L-sentence τ^* such that, for any local ring R,*

$$R \models \tau^* \iff \boldsymbol{k} \models \tau.$$

This follows from the fact that the ideal $\mathfrak{m}$ is definable in R as the set of all non-units. Call a sentence τ^* as in this lemma a *lift* of τ.

The Ax-Kochen Principle says roughly that as the prime number p goes to infinity, the rings $\mathbb{Z}_p$ and $\mathbb{F}_p[[T]]$ are more and more alike. The simple version of this result below says the same about the rings $\mathbb{Z}/(p^n)$ and $\mathbb{F}_p[T]/(T^n)$ for any fixed $n > 0$. For example, for $n = 2$, the integers

$$a_0 + a_1 p, \qquad (a_0, a_1 \in \{0, 1, \ldots, p-1\})$$

are in bijection with their images in $\mathbb{Z}/(p^2)$, and the polynomials

$$b_0 + b_1 T \in \mathbb{F}_p[T], \quad (b_0, b_1 \in \mathbb{F}_p)$$

are in bijection with their images in $\mathbb{F}_p[T]/(T^2)$. These two rings clearly resemble each other: both are henselian local rings with maximal ideal generated by an element whose square is 0, and both have exactly p^2 elements. But they are very different in one respect: $\mathbb{Z}/(p^2)$ has no subfield, but $\mathbb{F}_p[T]/(T^2)$ has (the image of) $\mathbb{F}_p$ as subfield. The ring $\mathbb{Z}/(p^2)$ is an arithmetic object, while $\mathbb{F}_p[T]/(T^2)$ has more a geometric flavour.

2.14. Baby Ax-Kochen Principle. *Let σ be any sentence of L_t, and let $n > 0$. Then*

$$\big(\mathbb{Z}/(p^n), p_n\big) \models \sigma \iff \big(\mathbb{F}_p[T]/(T^n), T_n\big) \models \sigma$$

for all but finitely many primes p, where p_n and T_n are the image of p and T in $\mathbb{Z}/(p^n)$ and $\mathbb{F}_p[T]/(T^n)$, respectively.

Before we start the proof, we define for a prime number p the L-sentence ch_p to be $\forall x(p{\cdot}x \neq 1)$, where $p{\cdot}x$ denotes the term $x+\cdots+x$ where the logical variable x occurs exactly p times. So for any ring R we have: $R \models \mathrm{ch}_p \iff p{\cdot}1 \notin U(R)$, and thus for any local ring R we have $R \models \mathrm{ch}_p \iff \mathrm{char}\, \boldsymbol{k} = p$.

Proof. Let Σ_n be a set of axioms in the language L_t whose models are exactly the pairs (R, t) such that R is a local ring with $\mathrm{char}\, \boldsymbol{k} = 0$, $\mathfrak{m} = tR$, $t^{n-1} \neq 0$, and $t^n = 0$. By the previous corollary we can take an L-sentence σ_{n-1} such that for every model (R, t) of Σ_n we have

$$(R, t) \models \sigma \iff \boldsymbol{k} \models \sigma_{n-1}.$$

Let σ^*_{n-1} be a lift of σ_{n-1} as in the lemma. Then for every model (R, t) of Σ_n we have

$$(R, t) \models \sigma \iff R \models \sigma^*_{n-1}.$$

Thus by the completeness theorem there is a formal proof of $\sigma \leftrightarrow \sigma^*_{n-1}$ from Σ_n. We can assume that Σ_n is the union of a finite set with an infinite set $\{\neg\mathrm{ch}_2, \neg\mathrm{ch}_3, \neg\mathrm{ch}_5, \ldots, \}$. Fix a formal proof of $\sigma \leftrightarrow \sigma^*_{n-1}$ from Σ_n, and take the natural number N so large that for $p > N$ the axiom $\neg\mathrm{ch}_p$ is not used in this proof. Then for $p > N$, the structures $\big(\mathbb{Z}/(p^n), p_n\big)$ and $\big(\mathbb{F}_p[T]/(T^n), T_n\big)$ satisfy all axioms of Σ_n used in this proof, hence

$$\begin{aligned}
\big(\mathbb{Z}/(p^n), p_n\big) \models \sigma \quad &\iff \quad \mathbb{Z}/(p^n) \models \sigma^*_{n-1} \\
&\iff \quad \mathbb{F}_p \models \sigma_{n-1} \quad \text{by lemma 2.13} \\
&\iff \quad \mathbb{F}_p[T]/(T^n) \models \sigma^*_{n-1} \\
&\iff \quad \big(\mathbb{F}_p[T]/(T^n), T_n\big) \models \sigma
\end{aligned}$$

□

2.15. Remark. The proof as given shows that the equivalence holds for all $p > N(\sigma, n)$, where $(\sigma, n) \mapsto N(\sigma, n)$ is a computable function with values in $\mathbb{N}$.

Another (less constructive) argument to obtain this result is to show that for each non-principal ultrafilter $\mathcal{F}$ on the set of primes,

$$\prod_{\mathcal{F}} \big(\mathbb{Z}/(p^n), p_n\big) \;\cong\; \prod_{\mathcal{F}} \big(\mathbb{F}_p[T]/(T^n), T_n\big) \qquad \text{(as } L_t\text{-structures)}.$$

The existence of the isomorphism follows from proposition 2.10: both sides are local rings whose maximal ideal is generated by a single element (the interpretation of t) whose $(n-1)^{\text{th}}$ power is not zero, but whose n^{th} power is 0, and both sides have residue field isomorphic to $\prod_{\mathcal{F}} \mathbb{F}_p$, which has characteristic 0.

To formulate other applications of the lifting theorem, we introduce some terminology: Let R be a ring, and $X = (X_1, \dots, X_n)$ a tuple of distinct indeterminates. Given any polynomial $f(X) \in \mathbb{Z}[X]$, let the polynomial $f^R(X) \in R[X]$ be obtained from f by replacing each of its coefficients by its image under the ring morphism $\mathbb{Z} \to R$, and for $a \in R^n$, put $f(a) := f^R(a) \in R$. Given polynomials $f_1, \dots, f_k \in \mathbb{Z}[X]$ a *solution of the system* $f_1(X) = \cdots = f_k(X) = 0$ *in* R is an n-tuple $a \in R^n$ such that $f_1(a) = \cdots = f_k(a) = 0$. If R is a local ring, then a *lift* of a tuple $(x_1, \dots, x_n) \in \boldsymbol{k}^n$ is a tuple $(a_1, \dots, a_n) \in R^n$ such that $\bar{a_i} = x_i$ for $i = 1, \dots, n$.

The next lemma is an immediate consequence of the lifting theorem. In the rest of this section $X = (X_1, \dots, X_n)$ is a tuple of distinct indeterminates with $n > 0$.

2.16. Lemma. *Let R be a henselian local ring with* $\operatorname{char} \boldsymbol{k} = 0$*, and $f_1, \dots, f_k \in \mathbb{Z}[X]$. Then any solution of $f_1(X) = \cdots = f_k(X) = 0$ in $\boldsymbol{k}$ can be lifted to a solution in R.* □

The following corollary answered a question of S. Lang from the 1950's.

2.17. Corollary (Greenleaf-Ax-Kochen). *Let $f_1, \dots, f_k \in \mathbb{Z}[X]$. Then for all but finitely many primes p, every solution of*

$$f_1(X) = \cdots = f_k(X) = 0$$

in $\mathbb{F}_p$ can be lifted to a solution in $\mathbb{Z}_p$.

Proof. Since $f_1, \dots, f_k$ are given by L-terms, we can construct an L-sentence σ_f that expresses in any local ring the liftability of solutions in the residue field, that is, for for every local ring R:

$$\begin{aligned} R \models \sigma_f \iff & \text{for all } x \in R^n \text{ with } f_1(x), \dots, f_k(x) \in \mathfrak{m} \text{ there is } y \in R^n \text{ such} \\ & \text{that } f_1(y) = \cdots = f_k(y) = 0 \text{ and } y_i - x_i \in \mathfrak{m} \text{ for } i = 1, \dots, n. \end{aligned}$$

Let HLR be a set of axioms in the language L whose models are exactly the henselian local rings, and put $\text{HLR}(0) := \text{HLR} \cup \{\neg \text{ch}_2, \neg \text{ch}_3, \neg \text{ch}_5, \dots\}$. So

the models of HLR(0) are exactly the henselian local rings with residue field of characteristic 0. By the lemma we have $\mathrm{HLR}(0) \models \sigma_f$, so by compactness there is $N \in \mathbb{N}$ such that

$$\mathrm{HLR} \cup \{\neg \mathrm{ch}_p : p \leq N\} \models \sigma_f.$$

Now observe that $\mathbb{Z}_p$ is a model of the lefthandside if $p > N$. □

2.18. Theorem (Chevalley-Warning). *Let $q = p^e$, $e \in \mathbb{N}^{>0}$, and let $f_1, \ldots, f_k \in \mathbb{F}_q[X] \setminus \{0\}$ be such that $\sum \deg f_i < n$. Then*

$$\big|\{x \in \mathbb{F}_q^n : f_1(x) = \cdots = f_k(x) = 0\}\big| \equiv 0 \mod p;$$

in particular, if $f_1, \ldots, f_k$ have constant term 0, then there is a nonzero $x \in \mathbb{F}_q^n$ such that $f_1(x) = \cdots = f_k(x) = 0$.

See Serre's *Course of Arithmetic* for a proof of the Chevalley-Warning theorem. In combination with the Greenleaf-Ax-Kochen theorem it yields:

2.19. Corollary. *Let $f_1, \ldots, f_k \in \mathbb{Z}[X] \setminus \{0\}$ all have constant term 0, and suppose that $\sum \deg f_i < n$. Then for all sufficiently large primes p there exists a nonzero $x \in \mathbb{Z}_p^n$ such that $f_1(x) = \cdots = f_k(x) = 0$.*

Later in the course we shall prove:

2.20. Ax-Kochen Principle. *Let σ be any L-sentence. Then*

$$\mathbb{Z}_p \models \sigma \iff \mathbb{F}_p[[T]] \models \sigma$$

for all but finitely many primes p.

Here is an application that at the time (mid 1960's) created a stir:

2.21. *Given any positive integer d there is $N(d) \in \mathbb{N}$ such that for all prime numbers $p > N(d)$: if $f(X_1, \ldots, X_n) \in \mathbb{Z}_p[X_1, \ldots, X_n]$ is homogeneous of degree d and $n > d^2$, then there exists a nonzero $x \in \mathbb{Z}_p^n$ with $f(x) = 0$. (It is enough to consider the case $n = d^2 + 1$.)*

This follows by applying the Ax-Kochen Principle to a theorem of Tsen and Lang from the 1950's which says that if $f(X_1, \ldots, X_n) \in R[X_1, \ldots, X_n]$ is homogeneous of degree d and $n > d^2$, with $R = \mathbb{F}_p[[T]]$ and p any prime number, then there exists a nonzero $x \in R^n$ with $f(x) = 0$. (This is related to the Chevalley-Warning theorem.)

Here is some more history: it was known from the 19th century that a quadratic form (= homogeneous polynomial of degree 2) over a p-adic field in 5 variables always has a nontrivial zero in that field. Emil Artin had conjectured that this remained true for forms of degree d in d^2+1 variables. This conjecture was proved for $d = 3$ in the 1950s. Ax and Kochen proved the above asymptotic form of Artin's conjecture, and around the same time Terjanian gave a counterexample for $d = 4$.

More on completion. We still need to explain the term *complete local ring* that was used in motivating Hensel's Lemma. Let R be a ring and $I \subseteq R$ a proper ideal. (Here *proper* means that $I \neq R$.) Consider the decreasing sequence of ideals:

$$R = I^0 \supseteq I^1 \supseteq I^2 \supseteq \cdots .$$

Recall that I^n is the set of R-linear combinations of products $a_1 \cdots a_n$ with each $a_i \in I$. Suppose $\bigcap_n I^n = 0$. (This is always true if R is local and noetherian.) Define $\mathrm{ord}_I : R \to \mathbb{N} \cup \{\infty\}$ by:

$$\mathrm{ord}_I(r) = \begin{cases} \max\{n : r \in I^n\} & \text{if } r \neq 0 \\ \infty & \text{if } r = 0 \end{cases} .$$

Note that then for all $r, s \in R$:

- $\mathrm{ord}_I(r+s) \geq \min\{\mathrm{ord}_I(r), \mathrm{ord}_I(s)\}$,
- $\mathrm{ord}_I(rs) \geq \mathrm{ord}_I(r) + \mathrm{ord}_I(s)$,
- $\mathrm{ord}_I > 0 \iff r \in I$.

This defines an ultranorm by $|r| = 2^{-\mathrm{ord}_I(r)}$; note that for all $r \in R$:

$$|r| \leq 1, \qquad |r| < 1 \iff r \in I.$$

A ring R with proper ideal I is said to be *I-adically complete* if $\bigcap_n I^n = 0$ and R is complete with respect to this norm.

2.22. Lemma. *Let R be a ring with maximal ideal $\mathfrak{m}$ which is $\mathfrak{m}$-adically complete. Then R is a local ring (and thus henselian, by Hensel's lemma).*

Proof. Since $\mathfrak{m} = \{x \in R : |x| < 1\}$, Lemma 2.6 yields $R \setminus \mathfrak{m} = U(R)$. □

We define a *complete local ring* to be a local ring R that is $\mathfrak{m}$-adically complete.

Assume the proper ideal I in the ring R is finitely generated and $\bigcap_n I^n = 0$. Let $\widehat{R}$ be the completion of R with respect to the I-adic norm. Then the closure of I in $\widehat{R}$ is $I\widehat{R}$, also denoted by $\widehat{I}$. More generally, the closure of I^n in $\widehat{R}$ is $I^n\widehat{R}$, which equals $(\widehat{I})^n$. Furthermore, the natural map

$$R/I^n \to \widehat{R}/(\widehat{I})^n$$

is a ring isomorphism. We leave the proofs of these claims as an exercise.

Consider now the ring $\mathbb{Z}$, with ideal $I = p\mathbb{Z}$, where p is a prime number. Although the p-adic norm is defined with base p instead of 2, this yields the same topology on $\mathbb{Z}$ as the I-adic norm. As rings we can identify $\mathbb{Z}_p$ with the I-adic completion $\widehat{\mathbb{Z}}$ such that the p-adic norm is a fixed power of the I-adic norm: $|x|_p = |x|^{\log_2 p}$ for $x \in \mathbb{Z}_p$.

3 Valuation theory

We begin this section with developing basic valuation theory, and end it with a quantifier elimination for algebraically closed valued fields.

A *valuation* on an (additively written) abelian group A is a map

$$v : A \setminus \{0\} \to \Gamma$$

into a linearly ordered set Γ, such that $v(-x) = vx$ for nonzero $x \in A$ and $v(x+y) \geq \min\{vx, vy\}$ for $x, y \in A$ such that $x, y, x+y \neq 0$.

By convention we extend v to all of A by setting $v0 = \infty$, where ∞ is not in Γ. We extend $<$ to a linear order on $\Gamma_\infty = \Gamma \cup \{\infty\}$ by specifying $\gamma < \infty$ for all $\gamma \in \Gamma$. Then $v(-x) = vx$ and $v(x+y) \geq \min\{vx, vy\}$ for all $x, y \in A$ without exception. For future use, note that if $x, y \in A$ and $vx < vy$, then $v(x+y) = vx$. (Use that $vx = v(x+y-y) \geq \min\{v(x+y), vy\}$.) More generally, if $x_1, \ldots, x_n \in A$, $n \geq 1$, and $v(x_1) < v(x_2), \ldots, v(x_n)$, then $v(x_1 + \cdots + x_n) = v(x_1)$. Another elementary fact that is often used is that

$$\{(x, y) \in A \times A : v(x-y) > vx\}$$

is an equivalence relation on $A \setminus \{0\}$. (The reader should check this.)

Our real interest is in valuations on *fields*, and then Γ is not just a linearly ordered set but has also a compatible group structure:

An *ordered abelian group* is an abelian (additively written) group Γ equipped with a translation invariant linear order $<$. Such Γ is called *archimedean* if, for any $a, b > 0$, there is $n \in \mathbb{N}$ such that $na > b$. (Examples: The additive groups of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ with the usual ordering are archimedean ordered abelian groups.) Note that ordered abelian groups are torsion-free.

The following result has historic roots in Eudoxos, Euclid, and Archimedes, but its present formulation is due to O. Hölder and became only possible after Dedekind's foundation of the real number system in the 19th century. It says that archimedean ordered abelian groups can be embedded into the ordered additive group of real numbers.

3.1. Lemma. *Let Γ be an archimedean ordered abelian group, and $\gamma \in \Gamma^{>0}$. Then there is a unique embedding $i : \Gamma \to \mathbb{R}$ of ordered groups such that $i\gamma = 1$. If there is no $\beta \in \Gamma$ with $0 < \beta < \gamma$, then $i\Gamma = \mathbb{Z}$.*

Proof. If Γ has γ as least positive element, then $\Gamma = \mathbb{Z}\gamma$, and the embedding is given by $i(k\gamma) = k$ for $k \in \mathbb{Z}$. If Γ has no least positive element, the embedding is given by $i\beta := \sup\{\frac{k}{n} : k \in \mathbb{Z}, n > 0, n\beta < k\gamma\}$ for $\beta \in \Gamma$. The reader should fill in the details. □

3.2 Definition. A *valuation* on a domain A is a function $v : A \setminus \{0\} \to \Gamma$, where Γ is an ordered abelian group, such that for all $x, y \in A \setminus \{0\}$:

(V1) $v(x+y) \geq \min\{vx, vy\}$, provided $x + y \neq 0$,

(V2) $v(xy) = vx + vy$,

Given a domain A we have a bijective correspondence between the set of ultrametric absolute values on A and the set of valuations $v : A \setminus \{0\} \to \mathbb{R}$, with the ultrametric absolute value $|\ |$ on A corresponding to the valuation $v : A \setminus \{0\} \to \mathbb{R}$ given by $v(a) := -\log|a|$.

Let $v : A \setminus \{0\} \to \Gamma$ be a valuation on the domain A. Note that then $v1 = v(-1) = 0$, since v restricted to $U(A)$ is a group morphism. Hence $vx = v(-x)$ for all $x \in A \setminus \{0\}$, so v is a valuation on the additive group as defined earlier. We extend v uniquely to a valuation $v : K^\times \to \Gamma$ on the fraction field K of A, by

$$v(x/y) = vx - vy, \qquad x, y \in A \setminus \{0\}.$$

Thus $v(K^\times)$ is a subgroup of Γ. By convention we extend v to all of K by setting $v0 = \infty$, where $\Gamma_\infty = \Gamma \cup \{\infty\}$ is linearly ordered as before, and where we extend $+$ to a binary operation on Γ_∞ by $\gamma + \infty = \infty + \gamma = \infty$ for all $\gamma \in \Gamma_\infty$. Then (V1) and (V2) hold for all $x, y \in K$ without the proviso in (V1).

When we refer to a valuation $v : K^\times \to \Gamma$ on a field K, we shall assume from now on that $v(K^\times) = \Gamma$, unless specified otherwise. We call $\Gamma = v(K^\times)$ the *value group of the valuation*.

Motivating Example. Let $K = \mathbb{C}(t)$. Each point $a \in \mathbb{C}$ gives rise to a valuation $v_a : K^\times \to \mathbb{Z}$ by:

$$v_a(f(t)) = k \quad \text{if} \quad f(t) = (t-a)^k \frac{g(t)}{h(t)},$$

where $g, h \in \mathbb{C}[t]$ are such that $g(a), h(a) \neq 0$. Note that if $k > 0$, then $f(a) = 0$ and k is the *order of vanishing* of f at a; if $k = 0$, then $f(a) \in \mathbb{C}^\times$; and if $k < 0$, then f has a pole at a of order $-k$. Geometrically it is natural to consider $f \in K^\times$ as defining a meromorphic function on the Riemann sphere $\mathbb{C}_\infty := \mathbb{C} \cup \{\infty\}$, and to assign also to the point ∞ on this sphere a valuation $v_\infty : K^\times \to \mathbb{Z}$,

$$v_\infty(f(t)) = \deg h(t) - \deg g(t) \quad \text{if} \quad f(t) = \frac{g(t)}{h(t)},\ g, h \in \mathbb{C}[t].$$

These valuations are related by the fundamental identity

$$\sum_{a \in \mathbb{C}_\infty} v_a(f) = 0, \qquad f \in K^\times.$$

(This identity clearly holds for $f \in \mathbb{C}[t] \setminus \{0\}$, and the general case then follows easily.) This family of valuations is an important tool to understand the field $K = \mathbb{C}(t)$; the same role is played for other so-called *global* fields by a family of valuations satisfying a similar identity. In this course, however, we focus on fields with a single valuation, that is, we study *local* aspects of fields.

With this example in mind, given a valued field (K, v), we think of K as a field of (meromorphic) functions on some space in which v is associated with a

certain point of the space, where $vf > 0$ indicates that the "function" f vanishes at that point, vf measuring the order of vanishing. Likewise, $vf < 0$ means that f has a pole at that point (and $v(f^{-1})$ is the order of vanishing of f^{-1}). Indeed, we shall regard v itself as an abstract point at which the elements of K can be evaluated. This will become clear in the discussion after the next definition.

3.3 Definition. Let $v : K^\times \to \Gamma$ be a valuation on a field.

1. $\mathcal{O}_v := \{x \in K : vx \geq 0\}$, a subring of K.
2. $\mathfrak{m}_v := \{x \in K : vx > 0\}$, an ideal in $\mathcal{O}_v$.
3. $\boldsymbol{k}_v := \mathcal{O}_v/\mathfrak{m}_v$.

Note that $vx = 0 \iff v(x^{-1}) = 0$, for $x \in K^\times$, so $U(\mathcal{O}_v) = \mathcal{O}_v \setminus \mathfrak{m}_v$. Therefore $\mathcal{O}_v$ is a local ring with maximal ideal $\mathfrak{m}_v$, and $\boldsymbol{k}_v$ is the residue field.

When thinking of K as a field of functions as above, $\mathcal{O}_v$ would be the set of functions which have no pole at (the point corresponding to) v, and $\mathfrak{m}_v$ would be the set of functions that vanish at v. The residue map $\mathcal{O}_v \to \boldsymbol{k}_v$ is then to be thought of as evaluation at v. We extend the residue map to a map $K \to \boldsymbol{k}_v \cup \{\infty\}$ by sending all elements of $K \setminus \mathcal{O}_v$ to ∞.

Note that we have the following disjoint union in K,

$$K = \underbrace{\mathfrak{m}_v \ \dot\cup \ U(\mathcal{O}_v)}_{\mathcal{O}_v} \ \dot\cup \ (\mathfrak{m}_v \setminus \{0\})^{-1}.$$

For each $x \in K^\times$, either $x \in \mathcal{O}_v$ or $x^{-1} \in \mathcal{O}_v$, so $\mathcal{O}_v$ is a valuation ring in K.

We have, therefore, two maps:

$$\begin{array}{ccc} K & \xrightarrow{\ v\ } & \Gamma \cup \{\infty\} \\ \big\downarrow & & \\ \boldsymbol{k}_v \cup \{\infty\} & & \end{array}$$

The *raison d' être* of valuation theory is in analyzing K in terms of the (usually) simpler objects Γ and $\boldsymbol{k}_v$ via these two maps.

Terminology. We call v *trivial* if $\Gamma = \{0\}$, *discrete* if $\Gamma \cong \mathbb{Z}$ as ordered groups, and of *rank 1* if $\Gamma \neq 0$ and Γ is archimedean.

If v is discrete, say $\Gamma = \mathbb{Z}$, take $t \in K$ with $vt = 1$. Then $\mathfrak{m}_v = t\mathcal{O}_v$, and each $a \in K^\times$ can be written uniquely as $a = ut^k$ with $u \in \mathcal{O}_v^\times$ and $k \in \mathbb{Z}$. (Simply take $k = v(a)$, and $u = a/t^k$.) The only non-trivial ideals of $\mathcal{O}_v$ are those of the form $t^n\mathcal{O}_v$. In particular $\mathcal{O}_v$ is a principal ideal domain.

Examples.

1. Let $K = \mathbb{C}(t)$, $v = v_0 : K^\times \to \mathbb{Z}$. Then $vt = 1$ and

$$\mathcal{O}_v = \left\{ \frac{f}{g} : f, g \in \mathbb{C}[t], g(0) \neq 0 \right\} = \mathbb{C}[t]_{t\mathbb{C}[t]}.$$

We have a surjective ring morphism

$$\mathcal{O}_v \to \mathbb{C} \ : \ \frac{f(t)}{g(t)} \mapsto \frac{f(0)}{g(0)}, \quad (f, g \in \mathbb{C}[t], g(0) \neq 0)$$

which has kernel $\mathfrak{m}_v$, and thus induces a field isomorphism $\boldsymbol{k}_v = \mathcal{O}_v/\mathfrak{m}_v \cong \mathbb{C}$. It is traditional to identify $\boldsymbol{k}_v$ with $\mathbb{C}$ via this isomorphism.

2. Let $K = \mathbb{Q}_p$. Here we have the *p-adic valuation* $v = v_p : K^\times \to \mathbb{Z}$ defined by $vx = k$ if $x = p^k u$, $u \in U(\mathbb{Z}_p)$, which is related to the p-adic absolute value by $|x|_p = p^{-vx}$. We have $\mathcal{O}_v = \mathbb{Z}_p$, $v(p) = 1$, $\mathfrak{m}_v = p\mathbb{Z}_p$, and $\boldsymbol{k}_v = \mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$.

For each ordered abelian group Γ and field $\boldsymbol{k}$, there is a field $K = \boldsymbol{k}((t^\Gamma))$ with valuation v having Γ as the value group and $\boldsymbol{k}$ as the residue field. To construct $\boldsymbol{k}((t^\Gamma))$ we need some basic facts on well-ordered subsets of Γ.

Recall that a linearly ordered set A is said to be *well-ordered* if each nonempty subset of A has a least element, equivalently, there is no strictly decreasing sequence (α_n) in A.

Lemma. *Let $A, B \subseteq \Gamma$ be well-ordered (by the ordering of Γ). Then $A \cup B$ is well-ordered, the set $A + B := \{\alpha + \beta : \alpha \in A, \ \beta \in B\}$ is well-ordered, and for each $\gamma \in \Gamma$ there are only finitely many $(\alpha, \beta) \in A \times B$ such that $\alpha + \beta = \gamma$.*

Lemma. *Let $A \subseteq \Gamma^{>0}$ be well-ordered. Then*

$$[A] := \{\alpha_1 + \cdots + \alpha_n : \alpha_1, \ldots, \alpha_n \in A\}$$

is also well-ordered, and for each $\gamma \in [A]$ there are only finitely many tuples $(n, \alpha_1, \ldots, \alpha_n)$ with $\alpha_1, \ldots, \alpha_n \in A$ such that $\gamma = \alpha_1 + \cdots + \alpha_n$.

We now define $K = \boldsymbol{k}((t^\Gamma))$ to be the set of all formal series $f(t) = \sum_{\gamma \in \Gamma} a_\gamma t^\gamma$, with coefficients $a_\gamma \in \boldsymbol{k}$, such that the support,

$$\operatorname{supp}(f) = \{\gamma \in \Gamma : a_\gamma \neq 0\},$$

is a well-ordered subset of Γ. Using the first lemma on well-ordered subsets of Γ we can define binary operations of addition and multiplication on the set $\boldsymbol{k}((t^\Gamma))$ as follows:

$$\begin{aligned} \sum a_\gamma t^\gamma + \sum b_\gamma t^\gamma &= \sum (a_\gamma + b_\gamma) t^\gamma \\ \Big(\sum a_\gamma t^\gamma\Big)\Big(\sum b_\gamma t^\gamma\Big) &= \sum_\gamma \Big(\sum_{\alpha+\beta=\gamma} a_\alpha b_\beta \Big) t^\gamma. \end{aligned}$$

Note that K is a ring, even a domain, with $\boldsymbol{k}$ as a subfield via the identification $a \mapsto at^0$. To show K is a field we shall use the second lemma.

Define $v : K \setminus \{0\} \to \Gamma$ by

$$v\Big(\sum a_\gamma t^\gamma\Big) = \min\{\gamma : a_\gamma \neq 0\}.$$

Then v is a valuation on K, and if $v(f) > 0$, then by the second lemma $\sum_{n=0}^{\infty} f^n$ makes sense as an element of K: for any $\gamma \in \Gamma$ there are only finitely many n such that the coefficient of t^γ in f^n is not zero. Note that then

$$(1-f)\sum_{n=0}^{\infty} f^n = 1.$$

It now follows in the usual way that K is a field: write an arbitrary $g \in K \setminus \{0\}$ as $g = ct^\gamma(1-f)$, with $c \in k^\times$ and $v(f) > 0$. Then $g^{-1} = c^{-1}t^{-\gamma}\sum_n f^n$.

The valuation ring is

$$\mathcal{O}_v = \{f \in K : \mathrm{supp}(f) \subseteq \Gamma^{\geq 0}\}.$$

For $f = \sum a_\gamma t^\gamma$ in K, call a_0 the constant term of f. The map sending f to its constant term sends $\mathcal{O}_v$ onto $\boldsymbol{k}$, and this is a ring homomorphism. Its kernel is

$$\mathfrak{m}_v = \{f \in K : \mathrm{supp}(f) \subseteq \Gamma^{>0}\},$$

so this induces an isomorphism $\mathcal{O}_v/\mathfrak{m}_v \to \boldsymbol{k}$.

For $\Gamma = \mathbb{Z}$, the field $\boldsymbol{k}((t^{\mathbb{Z}}))$ is the usual field of Laurent series, i.e. $\boldsymbol{k}((t))$, with valuation ring $\boldsymbol{k}[\![t]\!]$. An early study of the fields $\boldsymbol{k}((t^\Gamma))$ is due to H. Hahn (of "Hahn–Banach" fame and Gödel's thesis advisor), so these valued fields are often referred to as *Hahn fields*.

Topology induced by a valuation. An *ultrametric space* is a set X with a map $v : X^2 \to \Gamma_\infty$, where Γ_∞ is a linearly ordered set with largest element ∞, such that, for all $x, y, z \in X$ and $\gamma \in \Gamma_\infty$:

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

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

(iii) $v(x,y), v(y,z) \geq \gamma \implies v(x,z) \geq \gamma$.

Example. An abelian group A with valuation v is an ultrametric space with respect to $v(x,y) := v(x-y)$.

Let X be an ultrametric space as above. For a point $a \in X$ and $\gamma \in \Gamma_\infty$, we define two kinds of disks:

$$\begin{aligned} D_a(\gamma) &= \{x \in X : v(x,a) > \gamma\}, \quad \text{an open disk} \\ \bar{D}_a(\gamma) &= \{x \in X : v(x,a) \geq \gamma\}, \quad \text{a closed disk.} \end{aligned}$$

We refer to D_a as the *open disk centered at a with valuation radius γ*, and to $\bar{D}_a(\gamma)$ as the *closed disk centered at a with valuation radius γ*. The reader should verify that $D_a(\gamma) = D_b(\gamma)$ for each $b \in D_a$, and $\bar{D}_a(\gamma) = \bar{D}_b(\gamma)$ for each $b \in \bar{D}_a$, in stark contrast to disks in the euclidean plane which have a unique center. It follows easily that if D, E are disks (of any kind) with non-empty intersection, then $D \subseteq E$ or $E \subseteq D$. The open disks form a basis for a topology

on X, the *v-topology.* It is easy to see that all disks are both open and closed in the v-topology, and that X with the v-topology is a hausdorff space. A field K with valuation v is a topological field with respect to the v-topology, that is, the field operations $+, -, \cdot : K^2 \to K$, and $x \mapsto x^{-1} : K^\times \to K^\times$ are continuous. Note that then $\mathcal{O}_v$ is the closed disk centered at 0 with valuation radius 0, and that the open disks with valuation radius 0 contained in $\mathcal{O}_v$ are exactly the cosets $a + \mathfrak{m}_v$ with $a \in \mathcal{O}$. In particular, $\mathcal{O}_v$ contains exactly $|\boldsymbol{k}_v|$ open disks of valuation radius 0. Indeed, any closed disk of valuation radius $\gamma \in v(K^\times)$ contains exactly $|\boldsymbol{k}_v|$ open disks of valuation radius γ: by a translation one can assume the closed disk contains 0, and then multiplication by an $a \in K$ with $va = -\gamma$ makes the closed disk equal to $\mathcal{O}_v$.

The next result is due to Krull. The short proof below was found by Gravett.

3.4. Proposition. *Let $v : K^\times \to \Gamma$ be a valuation on the field K, and $\boldsymbol{k} := \boldsymbol{k}_v$. Then the cardinality of K is bounded in terms of the cardinalities of $\boldsymbol{k}$ and Γ: $|K| \leq |\boldsymbol{k}|^{|\Gamma|}$.*

Proof. Let $\gamma \in \Gamma$, and define equivalence relations on K by

$$x \gamma y \iff v(x-y) > \gamma, \qquad x \bar{\gamma} y \iff v(x-y) \geq \gamma.$$

Thus the γ-classes are the open disks of valuation radius γ, and the $\bar{\gamma}$-classes are the closed disks of valuation radius γ. Each γ-class D is contained in a unique $\bar{\gamma}$-class $\bar{D}$, and each $\bar{\gamma}$-class contains exactly $|\boldsymbol{k}|$-many γ-classes. Let $\mathcal{D}_\gamma$ be the set of all γ-classes. Then we have a map $f_\gamma : \mathcal{D}_\gamma \to \boldsymbol{k}$ such that for all $D, E \in \mathcal{D}_\gamma$, if $\bar{D} = \bar{E}$ and $f_\gamma(D) = f_\gamma(E)$, then $D = E$.

We now associate to each $x \in K$ the function $\gamma \mapsto x(\gamma) : \Gamma \to \boldsymbol{k}$ by $x(\gamma) = f_\gamma(D)$ where $D \in \mathcal{D}_\gamma$ contains x. Then the map $K \to \boldsymbol{k}^\Gamma$ that sends each $x \in K$ to the function $\gamma \mapsto x(\gamma)$ is injective: if $x, y \in K$ and $x \neq y$, then for $\gamma := v(x-y)$ we have $x(\gamma) \neq y(\gamma)$ since x and y are in the same closed disk of valuation radius γ but in different open disks of valuation radius γ. □

Correspondence between valuation rings and valuations. A *valuation ring of* a field K is a subring A of K such that for each $x \in K^\times$, either $x \in A$ or $x^{-1} \in A$. Note that then A is indeed a valuation ring, with K as field of fractions.

Let A be a valuation ring of the field K. Recall that we have the disjoint union

$$K = \mathfrak{m}_A \cup U(A) \cup (\mathfrak{m}_A \setminus \{0\})^{-1}.$$

Consider the (abelian) quotient group $\Gamma_A = K^\times / U(A)$, written additively. The binary relation $\geq$ on Γ_A defined by

$$xU(A) \geq yU(A) \iff x/y \in A, \qquad (x, y \in K^\times)$$

makes Γ_A into an ordered abelian group, and the natural map

$$v_A : K^\times \to \Gamma_A, \quad v_A x = xU(A)$$

is a valuation. (Check this!) Note that $\mathcal{O}_{v_A} = A$.

Every valuation $v : K^\times \to \Gamma$ with valuation ring $\mathcal{O}_v = A$ is *equivalent* to v_A as follows: there is a unique isomorphism of ordered abelian groups $i : \Gamma_A \to \Gamma$ such that $i \circ v_A = v$. More generally, two valuations $v_1 : K^\times \to \Gamma_1$ and $v_2 : K^\times \to \Gamma_2$ are said to be *equivalent* if there is an isomorphism of ordered abelian groups $i : \Gamma_1 \to \Gamma_2$ such that $i \circ v_1 = v_2$; note that such an i is then uniquely determined. The reader should check that two valuations v_1 and v_2 on a field are equivalent iff they have the same valuation ring.

A valuation ring A is said to be *discrete* if the valuation v_A on its fraction field K is discrete. In that case there is a unique valuation $v : K^\times \to \mathbb{Z}$ such that $\mathcal{O}_v = A$; this v is called the *normalized valuation* of A. (For example, the value group of a discrete valuation v on a field could be $\frac{1}{2}\mathbb{Z}$, and then $2v$ would be the corresponding normalized valuation.) We also write *DVR* instead of *discrete valuation ring*. Note that $\mathbb{Z}_p$ and $\boldsymbol{k}[[t]]$ are DVR's.

3.5 Definition. A *valued field* is a pair (K, A), where K is a field and A is a valuation ring of K.

If (K, A) is a valued field and E a subfield of K, then $A \cap E$ is a valuation ring of E. Note: $(E, A \cap E) \subseteq (K, A)$ (where "$\subseteq$" means "is a substructure of").

Exercises. Let (K, A) be an algebraically closed valued field. Show that the residue field $\boldsymbol{k}_A$ is algebraically closed and the value group Γ_A is divisible.

Let (K, A) be a valued field, and $L \supseteq K$ a field extension. Then a valuation ring B of L *lies over* A (or *dominates* A) if $A = B \cap K$, equivalently, $(K, A) \subseteq (L, B)$. Note that then $\mathfrak{m}_A = \mathfrak{m}_B \cap K$, so we have an induced embedding of residue fields, $A/\mathfrak{m}_A \to B/\mathfrak{m}_B$, by means of which $\boldsymbol{k}_A = A/\mathfrak{m}_A$ is identified with a subfield of $\boldsymbol{k}_B = B/\mathfrak{m}_B$. Also $U(B) \cap K = U(A)$, so we have an induced embedding $v_A(x) \mapsto v_B(x) : \Gamma_A \to \Gamma_B$ $(x \in K^\times)$, of ordered abelian groups, by means of which Γ_A is identified with an ordered subgroup of Γ_B.

3.1 Valuation rings and integral closure

We begin with recalling some terminology and basic facts concerning rings and ideals. (See for example S. Lang's book "Algebra" for more details.)

Let $A \subseteq B$ be rings. For an ideal I of A we let

$$IB := \{a_1 b_1 + \cdots + a_n b_n : a_1, \ldots, a_n \in I, b_1, \ldots, b_n \in B\}$$

be the ideal of B generated by I. If $\mathfrak{p}$ and $\mathfrak{q}$ are prime ideals of A and B respectively, we say that $\mathfrak{q}$ *lies over* $\mathfrak{p}$ if $\mathfrak{q} \cap A = \mathfrak{p}$. In that case we have a ring embedding $a + \mathfrak{p} \mapsto a + \mathfrak{q} : A/\mathfrak{p} \to B/\mathfrak{q}$.

We call an element $b \in B$ *integral* over A if b is a zero of a monic polynomial over A, that is,

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

for suitable $n > 0$ and $a_1, \ldots, a_n \in A$. (Then $A[b] = A + Ab + \cdots + Ab^{n-1}$, so $A[b]$ is a finitely generated A-module. The converse is also true: if $b \in B$ and

$A[b]$ is a finitely generated A-module, then b is integral over A.) The elements of B that are integral over A form a subring of B, called the *integral closure* of A in B. We call A *integrally closed in* B if each $b \in B$ that is integral over A lies already in A.

Given rings $A \subseteq B \subseteq C$, the ring C is integral over A iff C is integral over B and B is integral over A.

Exercise. Let $A \subseteq B$ be domains, and suppose B is integral over A. Show: A is a field iff B is a field.

As before, let $A \subseteq B$ be rings, and suppose B is integral over A. Let $\mathfrak{p}$ be a prime ideal of A. Then there is a prime ideal $\mathfrak{q}$ of B that lies over $\mathfrak{p}$. Moreover, for each such $\mathfrak{q}$, the ideal $\mathfrak{p}$ is maximal iff $\mathfrak{q}$ is maximal. (Explanation: For such $\mathfrak{q}$ we have a natural ring embedding $A/\mathfrak{p} \to B/\mathfrak{q}$, and after identifying $A/\mathfrak{p}$ with its image in $B/\mathfrak{q}$, this last domain is integral over the domain $A/\mathfrak{p}$. Hence by the exercise above, $A/\mathfrak{p}$ is a field iff $B/\mathfrak{q}$ is a field.)

We say that a domain A is *integrally closed* if it is integrally closed in its field of fractions.

Given a domain A with fraction field K, and a prime ideal $\mathfrak{p}$ of A we let

$$A_{\mathfrak{p}} := \left\{ \frac{x}{y} \in K : x, y \in A, y \notin \mathfrak{p} \right\}$$

be the localization of A with respect to $\mathfrak{p}$. It is easy to check that $A_{\mathfrak{p}}$ is a local domain with maximal ideal $\mathfrak{p}A_{\mathfrak{p}}$, and that this maximal ideal lies over $\mathfrak{p}$.

3.6. Proposition. *Valuation rings are integrally closed.*

Proof. Suppose A is a valuation ring of the field K, and let $v = v_A$ be the canonical valuation. To show A is integrally closed, let $x \in K^\times$ be such that $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ with $n > 0$ and all $a_i \in A$. If $x \notin A$, then $vx < 0$, hence

$$v(x^n) = nv(x) < iv(x) + v(a_i) = v(a_i x^i), \quad i = 0, \ldots, n-1,$$

hence $v(x^n + \cdots + a_0) = v(x^n) < 0$. But $v(x^n + \cdots + a_0) = \infty$, a contradiction. □

3.7. Corollary. *Let (K, A) be an algebraically closed valued field. Then A is henselian.*

Proof. Consider a polynomial $f(Y) = Y^n + Y^{n-1} + a_2 Y^{n-2} + \cdots + a_n$ with $n \geq 2$ and $a_2, \ldots, a_n \in A$. By Lemma 2.2 it is enough to show that f has a zero in $U(A)$. By the proposition above, $f = \prod_{i=1}^{n}(Y - \alpha_i)$ with all $\alpha_i \in A$. Now $\sum_i \alpha_i = -1$, so at least one α_i must be outside $\mathfrak{m}$, and thus be in $U(A)$. □

3.8 Definition. Given local rings A, B, we say B *dominates* A (or that B *lies over* A) if $A \subseteq B$ and $\mathfrak{m}_A \subseteq \mathfrak{m}_B$ (hence $\mathfrak{m}_B \cap A = \mathfrak{m}_A$).

One should check that this agrees with our definition of domination for valuation rings in the previous subsection.

We now state the main results to be proved in this subsection.

3.9 Proposition. *Let A be a local subring of the field K. Consider the class of all local subrings of K that dominate A, partially ordered by domination. Any maximal element of this class is a valuation ring of K.*

In particular, given any local subring A of a field K, there is a valuation ring of K lying above A.

3.10 Proposition. *Let A be a local subring of a field K. The integral closure of A in K is the intersection of all valuation rings of K that dominate A.*

3.11 Proposition. *Let A be a local domain integrally closed in $K = \mathrm{Frac}(A)$, and let L be a normal field extension of K. Let B be the integral closure of A in L. Then, given any maximal ideals $\mathfrak{n}$ and $\mathfrak{n}'$ of B there exists $\sigma \in \mathrm{Aut}(L|K)$ such that $\sigma(\mathfrak{n}) = \mathfrak{n}'$. (Note: all maximal ideals in B lie over $\mathfrak{m}_A$.)*

3.12 Proposition. *Let A be a valuation ring of the field K, let $L \supseteq K$ be an algebraic field extension, and let B be the integral closure of A in L. Then every valuation ring of L dominating A is of the form $B_\mathfrak{n}$ for some maximal ideal $\mathfrak{n} \subseteq B$.*

3.13. Corollary. *With the same assumption as in the proposition, we have a bijection $\mathfrak{n} \mapsto B_\mathfrak{n}$ from the set of maximal ideals in B onto the set of valuation rings in L dominating A. If in addition L is a normal field extension of K, then for any valuation rings V, V' of L dominating A there exists $\sigma \in \mathrm{Aut}(L|K)$ such that $\sigma(V) = V'$.*

Proof. We first show that, given any maximal ideal $\mathfrak{n}$ of B, the localization $B_\mathfrak{n}$ is a valuation ring of L dominating A. Note that $\mathfrak{n}$ lies over $\mathfrak{m}_A$, hence $B_\mathfrak{n}$ dominates A. Since L is the fraction field of B, there are no local subrings of L that dominate $B_\mathfrak{n}$. Thus by proposition 3.9, $B_\mathfrak{n}$ is a valuation ring of L.

The surjectivity of $\mathfrak{n} \mapsto B_\mathfrak{n}$ now follows from Proposition 3.12. Injectivity is left to the reader. The second assertion of the corollary follows from this correspondence and Proposition 3.11. □

3.14. Corollary. *Let A be a valuation ring of K, let $\widetilde{K}$ be an algebraic closure of K and $\widetilde{A}$ a valuation ring of $\widetilde{K}$ lying over A. Then any valued field embedding $(K, A) \to (F, C)$, where F is algebraically closed, extends to an embedding $(\widetilde{K}, \widetilde{A}) \to (F, C)$.*

Proof. Let $j : \widetilde{K} \to F$ be a field embedding that extends the field embedding $K \to F$. Then $j^{-1}(C)$ is a valuation ring of $\widetilde{K}$ lying over A. Hence there is $\sigma \in \mathrm{Aut}(\widetilde{K}|K)$ such that $j^{-1}(C) = \sigma\widetilde{A}$. Then $j\sigma$ is a valued field embedding of $(\widetilde{K}, \widetilde{A})$ into (F, C). □

It remains to prove 3.9–3.12. For the first two we use the next lemma:

3.15. Lemma. *Let A be a local subring of the field K, and suppose $x \in K^\times$ is such that $1 \in \mathfrak{m}A[x^{-1}] + x^{-1}A[x^{-1}]$. Then x is integral over A.*

Proof. We have $1 = a_n x^{-n} + \cdots + a_1 x^{-1} + a_0$ with $a_1, \ldots, a_n \in A$ and $a_0 \in \mathfrak{m}$. Multiplying both sides by x^n yields:

$$x^n(1 - a_0) + (\text{terms of lower degree in } x) = 0.$$

Since $1 - a_0$ is a unit in A, it follows that x is integral over A. □

Proof of 3.9. Let V be a maximal element in the class of local subrings of K that dominate A, and let $x \in K^\times$. Put $\mathfrak{m} := \mathfrak{m}_V$.

Consider first the case that x is integral over V. Then $V[x]$ is integral over V, so we can take a maximal ideal $\mathfrak{n}$ of $V[x]$ that lies over $\mathfrak{m}$, and then $V[x]_\mathfrak{n}$ is a local subring of K dominating V. By V's maximality this gives $x \in V$.

Next, suppose x is not integral over V. Then by the above lemma we have $1 \notin \mathfrak{m}V[x^{-1}] + x^{-1}V[x^{-1}]$, so we have a maximal ideal $\mathfrak{n}$ of $V[x^{-1}]$ such that $\mathfrak{n} \supseteq \mathfrak{m}$, and thus $\mathfrak{n} \cap V = \mathfrak{m}$. The local subring $V[x^{-1}]_\mathfrak{n}$ of K dominates V, so the maximality of V yields $x^{-1} \in V$. □

Proof of 3.10. Any $x \in K$ integral over A lies in every valuation ring of K containing A as a subring. Next, suppose $x \in K^\times$ is not integral over A. By the lemma above, $\mathfrak{m}A[x^{-1}] + x^{-1}A[x^{-1}]$ is a proper ideal of $A[x^{-1}]$. So we can take a maximal ideal $\mathfrak{n} \supseteq \mathfrak{m}$ of $A[x^{-1}]$ that contains x^{-1}. This yields a local subring $A[x^{-1}]_\mathfrak{n}$ of K that dominates A. Let V be a maximal element of the class of local subrings of K that dominate $A[x^{-1}]_\mathfrak{n}$. Then V is a valuation ring (by Proposition 3.9), V dominates A, and $x^{-1} \in \mathfrak{m}_V$, so $x \notin V$. □

In the next proof we use the Chinese Remainder Theorem: *Let A be an abelian (additive) group with subgroups $B_1, \ldots, B_n$ ($n > 0$) such that $B_i + B_j = A$ for all i, j with $1 \le i < j \le n$, and let $a_1, \ldots, a_n \in A$. Then there exists $x \in A$ such that $x - a_i \in B_i$ for $i = 1, \ldots, n$.*

Proof of 3.11. The general case follows from the case $[L : K] < \infty$ (how?), so we assume $[L : K] < \infty$ below.

Let $\mathfrak{n}, \mathfrak{n}'$ be two maximal ideals in B, lying over $\mathfrak{m}$, and assume towards a contradiction that $\sigma\mathfrak{n} \neq \mathfrak{n}'$ for all $\sigma \in G := \mathrm{Aut}(L|K)$. Thus the two sets of maximal ideals of B,

$$\{\sigma\mathfrak{n} : \sigma \in G\}, \qquad \{\sigma\mathfrak{n}' : \sigma \in G\}$$

are disjoint; since $[L : K] < \infty$, these two sets are also finite. By the Chinese Remainder Theorem there is $x \in B$ such that

$$x \equiv 0 \mod \sigma\mathfrak{n}, \qquad x \equiv 1 \mod \sigma\mathfrak{n}'$$

for all $\sigma \in G$. Hence $\sigma x \in \mathfrak{n} \setminus \mathfrak{n}'$ for all $\sigma \in G$. Recall that

$$\mathrm{N}_K^L(x) := (\prod_{\sigma \in G} \sigma x)^\ell$$

lies in K, where $\ell = 1$ if $\mathrm{char}\, K = 0$, and $\ell = p^e$ for some $e \in \mathbb{N}$ if $\mathrm{char}\, K = p > 0$. Each σx is integral over A, so $\mathrm{N}_K^L(x) \in A$. Also $\mathrm{N}_K^L(x) \in \mathfrak{n} \setminus \mathfrak{n}'$ because $\mathfrak{n}$ and $\mathfrak{n}'$ are prime ideals, hence $\mathrm{N}_K^L(x) \in A \cap \mathfrak{n} = \mathfrak{m} \subseteq \mathfrak{n}'$, a contradiction. □

Proof of 3.12. Let V be a valuation ring of L lying over A. Valuation rings are integrally closed, so $B \subseteq V$. We claim that $V = B_{\mathfrak{n}}$ where $\mathfrak{n} := \mathfrak{m}_V \cap B$. Clearly $B \setminus \mathfrak{n} \subseteq V \setminus \mathfrak{m}_V$, hence $B_{\mathfrak{n}} \subseteq V$. For the other inclusion, let $x \in V$, $x \neq 0$. We have a relation $a_n x^n + \cdots + a_0 = 0$, where $a_0, \ldots, a_n \in A$ and $a_n \neq 0$. Take $s \in \{0, \ldots, n\}$ maximal such that $v_A(a_s) = \min_i v_A(a_i)$. Put $b_i := a_i/a_s$. Dividing by $a_s x^s$ yields

$$\underbrace{(b_n x^{n-s} + \cdots + b_{s+1}x + 1)}_{y} + x^{-1}\underbrace{(b_{s-1} + \cdots + b_0/x^{s-1})}_{z} = 0.$$

So $y = -(z/x)$, and thus $-xy = z$. Since $b_i \in \mathfrak{m}_A$ for $s < i \leq n$, we have $y \in U(V)$, and hence $y \notin \mathfrak{n}$. Thus to get $x \in B_{\mathfrak{n}}$ it suffices to show that $y, z \in B$. This will follow if we show that y, z lie in every valuation ring of L dominating A. If such a ring contains x, it also contains y, hence contains $z = -yx$. If such a ring contains x^{-1}, it contains z, hence also $y = -zx^{-1}$. □

3.16 Proposition. *Let A be a local ring, $f(X) \in A[X]$ a monic polynomial of degree $d > 0$, and $A[x] := A[X]/(f)$ with $x := X + (f)$. Let $\overline{f}(X) \in \boldsymbol{k}[X]$ factor in $\boldsymbol{k}[X]$ as*

$$\overline{f} = \prod_{i=1}^{n} \overline{f_i}^{e_i}$$

where each $e_i > 0$, each $f_i \in A[X]$ is monic, and $\overline{f_1}, \ldots, \overline{f_n}$ are irreducible in $\boldsymbol{k}[X]$ and distinct. Put $\mathfrak{m}_i := (\mathfrak{m}, f_i(x))A[x]$. Then $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ are exactly the distinct maximal ideals of $A[x]$, and $A[x]/\mathfrak{m}_i \cong \boldsymbol{k}[X]/(\overline{f_i})$ (as rings) for each i.

Proof. For each i, consider the canonical morphisms,

$$A[x] = A[X]/(f) \xrightarrow{\pi} \boldsymbol{k}[X]/(\overline{f}) \xrightarrow{\pi_i} \boldsymbol{k}[X]/(\overline{f_i}).$$

Note that $\ker \pi = \mathfrak{m}A[x]$, and $\ker \pi_i = \overline{f_i} + (\overline{f})$. Therefore

$$\ker(\pi_i \pi_{\mathfrak{m}}) = (\mathfrak{m}, f_i(x)) = \mathfrak{m}_i,$$

since $f_i(x)$ is the preimage of $\overline{f_i} + (\overline{f})$ in $A[x]$. Because $\boldsymbol{k}[X]/\overline{f_i}$ is a field, $(\mathfrak{m}, f_i(x))$ is maximal in $A[x]$. Note that $\overline{f_i} \neq \overline{f_j}$ implies $\overline{f_i} \neq 0$ under $\pi_j \pi_{\mathfrak{m}}$, since $\overline{f_i} \not\equiv 0 \mod \overline{f_j}$. Thus $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ are distinct. It remains to show that the $\mathfrak{m}_i$'s are the only maximal ideals in $A[x]$. First note that the ring $A[x]$ is integral over A, so each maximal ideal in $A[x]$ lies over $\mathfrak{m}$. The polynomial $\prod f_i^{e_i} - f$ is in $\mathfrak{m}[X]$, and $f(x) = 0$, so $\prod f(x)^{e_i} \in \mathfrak{m}A[x]$. Thus each maximal ideal of $A[x]$ contains $\prod f_i(x)^{e_i}$, hence contains some $f_i(x)$, and thus is one of the $\mathfrak{m}_i$'s. □

3.2 Quantifier elimination

We shall prove quantifier elimination for algebraically closed *valued* fields using Corollary 3.14. We also need to know some ways to extend a valuation on a field K to $K(x)$ where x is transcendental over K. This is related to the next result, which is a fundamental inequality for valued field extensions. Given a

field extension $K \subseteq L$ we let $[L : K]$ be its *degree*, that is, the dimension of L as a vector space over K; to keep things simple we set $[L : K] = \infty$ if this dimension is infinite. Likewise, given an extension $\Gamma \subseteq \Gamma'$ of abelian groups we let $[\Gamma' : \Gamma]$ be its index, which by convention is ∞ if Γ'/Γ is infinite.

3.17 Proposition. *Let $(K, A) \subseteq (L, B)$ be valued fields, with corresponding inclusions $\boldsymbol{k}_A \subseteq \boldsymbol{k}_B$ and $\Gamma_A \subseteq \Gamma_B$ between their residue fields and value groups. Then:*

$$[L : K] \geq [\boldsymbol{k}_B : \boldsymbol{k}_A] \cdot [\Gamma_B : \Gamma_A].$$

Proof. Let $b_1, \dots, b_p \in B$ be such that $\overline{b}_1, \dots, \overline{b}_p$ are linearly independent over $\boldsymbol{k}_A$, $p \geq 1$. Likewise, let $c_1, \dots, c_q \in L^\times$ be such that $vc_1, \dots, vc_q$ lie in distinct cosets of Γ_A, $q \geq 1$. It is enough to show that then $[L : K] \geq pq$; this will follow from the K-linear independence of the family $(b_i c_j)$, which in turn follows from the identity:

$$v(\sum a_{ij} b_i c_j) = \min_{i,j} v(a_{ij} b_i c_j) = \min_{i,j}\{v(a_{ij}) + v(c_j)\} \qquad (\text{all } a_{ij} \in K) \qquad (2)$$

First we show that $v(a_1 b_1 + \cdots + a_p b_p) = \min_i v(a_i)$, where $a_1, \dots, a_p \in K$. We can assume that some $a_i \neq 0$, and then dividing by an a_i of minimum valuation, we can reduce to the case that all a_i are in A and $v(a_i) = 0$ for some i. We must show that then $v(a_1 b_1 + \cdots + a_p b_p) = 0$. We have:

$$\overline{a_1 b_1 + \cdots + a_p b_p} = \overline{a_1}\,\overline{b_1} + \cdots + \overline{a_p}\,\overline{b_p} \neq 0,$$

since $\overline{b_1}, \dots, \overline{b_p}$ are linearly independent over $\boldsymbol{k}_A$ and $\overline{a_i} \neq 0$ for some i. This proves what we want. Next, to prove (2) we can assume that for each j there is i such that $a_{ij} \neq 0$. Then for any j,

$$\begin{aligned} v\big(\sum_i a_{ij} b_i c_j\big) &= v\big((\sum_i a_{ij} b_i) c_j\big) \\ &= v(\sum_i a_{ij} b_i) + vc_j \\ &= \min_i v(a_{ij}) + vc_j \\ &\in \Gamma_A + vc_j. \end{aligned}$$

For $j_1 \neq j_2$ we have $\Gamma_A + vc_{j_1} \neq \Gamma_A + vc_{j_2}$, so

$$v\big(\sum_i a_{ij_1} b_i c_{j_1}\big) \neq v\big(\sum_i a_{ij_2} b_i c_{j_2}\big),$$

hence,

$$\begin{aligned} v(\sum a_{ij} b_i c_j) &= \min_j\{\min_i v(a_{ij}) + vc_j\} \\ &= \min_{i,j}\{v(a_{ij}) + vc_j\} \end{aligned}$$

□

For algebraic extensions this yields:

3.18. Corollary. *If $[L : K] = n$, then $[\boldsymbol{k}_B : \boldsymbol{k}_A] \leq n$ (so $\boldsymbol{k}_B$ is algebraic over $\boldsymbol{k}_A$), and $[\Gamma_B : \Gamma_A] \leq n$ (so $m\Gamma_B \subseteq \Gamma_A$ for some $m \in \{1, \ldots, n\}$.*

If L is an algebraic closure of K, then $\boldsymbol{k}_B$ is an algebraic closure of $\boldsymbol{k}_A$, and Γ_B is a divisible hull of Γ_A.

For simple transcendental extensions it is the *proof* of the fundamental inequality that really matters, as the next two lemmas will show.

3.19. Lemma. *Let (K, A) be a valued field, and let $L = K(x)$ be a field extension with x transcendental over K. There is a unique valuation ring B of L lying over A, such that $x \in B$, and $\bar{x}$ is transcendental over $\boldsymbol{k}_A$. Moreover, this B satisfies $\boldsymbol{k}_B = \boldsymbol{k}_A(\bar{x})$ and $\Gamma_B = \Gamma_A$.*

Proof. Let B be a valuation ring as in the lemma. Then $\bar{1}, \bar{x}, \bar{x}^2, \ldots$ are linearly independent over $\boldsymbol{k}_A$, so by the proof of Proposition 3.17,

$$v_B(f_0 + f_1 x + \cdots + f_n x^n) = \min_i v_A(f_i) \qquad (f_i \in K).$$

Thus v_B is uniquely determined by v_A on $K[x]$, hence on L. In particular, there is at most one B as in the lemma.

(Existence.) Define $v : K[x] \setminus \{0\} \to \Gamma_A$ by:

$$v(f_0 + f_1 x + \cdots + f_n x^n) = \min_i v_A(f_i) \qquad (f_i \in K).$$

Claim. v is a valuation on $K[x]$ (hence extends to a valuation on L).

It is clear that (V1) is satisfied. We need to check (V2). Let $f, g \in K[x] \setminus \{0\}$, so $f = \sum_i f_i x^i$, $g = \sum_j g_j x^j$ $(f_i, g_j \in K)$. Take i_0 minimal such that $v(f_{i_0}) = \min_i v(f_i)$, and take j_0 minimal such that $v(g_{j_0}) = \min_j v(g_j)$. Then

$$fg = \sum_n \Big(\sum_{i+j=n} f_i g_j \Big) x^n,$$

and for each n

$$v\Big(\sum_{i+j=n} f_i g_j \Big) \geq \min_{i+j=n} \{v(f_i) + v(g_j)\} \geq v(f) + v(g).$$

Now consider

$$\sum_{i+j=i_0+j_0} f_i g_j = f_{i_0} g_{j_0} + \underbrace{\text{terms } f_i g_j \text{ with } i < i_0 \text{ or } j < j_0}_{\text{each has valuation} > v(f_{i_0}) + v(g_{j_0})}$$

Therefore:

$$v\Big(\sum_{i+j=i_0+j_0} f_i g_j \Big) = v(f_{i_0}) + v(g_{j_0}) = v(f) + v(g).$$

This finishes the proof of the claim. Put $B := \mathcal{O}_v$. We still need to check:

Claim. $x \in B$, and $\bar{x}$ is transcendental over $\boldsymbol{k}_A$.

To see this, note that $v(x) = 0$, so $x \in B$. Let $a_1, \ldots, a_n \in A$ be such that $\bar{a_1}, \ldots, \bar{a_n}$ are not all zero. Then $v(x^n + a_1 x^{n-1} + \cdots a_n) = 0$, hence

$$\bar{x}^n + \bar{a_1}\bar{x}^{n-1} + \cdots + \bar{a_n} \neq 0.$$

This proves that $\bar{x}$ is transcendental over $\boldsymbol{k}_A$.

Claim. $\boldsymbol{k}_B = \boldsymbol{k}_A(\bar{x})$.

Let $b \in B$ be such that $v(b) = 0$. Write $b = \frac{f(x)}{g(x)}$, with $f, g \in K[x] \setminus \{0\}$, so $vf = vg$. Dividing all coefficients of f and g by a coefficient of g of minimal valuation, we may assume $vg = 0$, so $vf = 0$. Then $\bar{f}(\bar{x}) \neq 0$, $\bar{g}(\bar{x}) \neq 0$. Hence $bg(x) = f(x)$ yields $\bar{b}\bar{g}(\bar{x}) = \bar{f}(\bar{x})$, so

$$\bar{b} = \frac{\bar{f}(\bar{x})}{\bar{g}(\bar{x})} \in \boldsymbol{k}_A(\bar{x}),$$

as desired.

Finally, it is clear from the above that $\Gamma_B = \Gamma_A$. □

3.20. Lemma. *Let $v : K^\times \to \Gamma$ be a valuation on a field K, and let $L = K(x)$ be a field extension with x transcendental over K. Let δ, in some ordered abelian group extending Γ, satisfy $n\delta \notin \Gamma$ for all $n > 0$. Then v extends uniquely to a valuation $w : L^\times \to \Gamma + \mathbb{Z}\delta$ such that $w(x) = \delta$. Moreover, $\boldsymbol{k}_v = \boldsymbol{k}_w$.*

3.21. Remark. If Γ is a *divisible* ordered abelian group, δ is in some ordered abelian group extension, and $\delta \notin \Gamma$, then $n\delta \notin \Gamma$ for all $n > 0$.

Proof. Let w be as in the lemma. Then

$$w(1) = 0,\ w(x) = \delta,\ w(x^2) = 2\delta,\ \ldots$$

lie in different cosets of Γ, so by the proof of Proposition 3.17,

$$w(f_0 + f_1 x + \cdots + f_n x^n) = \min_i \{v(f_i) + i\delta\} \qquad (\text{all } f_i \in K). \tag{3}$$

Thus w is completely determined by v.

(Existence.) Define $w : K[x] \setminus \{0\} \to \Gamma + \mathbb{Z}\delta$ by (3). Again it is clear that (V1) is satisfied. To verify (V2) we mimic the proof of the previous lemma: take i_0 minimal such that $w(f_{i_0}) = \min_i\{v(f_i) + i\delta\}$, and choose j_0 minimal such that $w(g_{j_0}) = \min_j\{v(g_j) + j\delta\}$. Put $n_0 := i_0 + j_0$. First note that

$$w((\sum_{i+j=n} f_i g_j)x^n) \geq \min_{i+j=n}\{v(f_i) + v(g_j) + n\delta\} \geq w(f) + w(g).$$

Next,

$$\sum_{n \leq n_0} (\sum_{i+j=n} f_i g_j)x^n = f_{i_0} g_{j_0} x^{n_0} + \underbrace{\text{terms } f_i g_j x^n \text{ with } i < i_0 \text{ or } j < j_0}_{\text{valuation} > v(f_{i_0}) + v(g_{j_0}) + n_0\delta}.$$

Therefore:

$$w((\sum_{i+j=n_0} f_i g_j)x^n) = v(f_{i_0}) + v(g_{j_0}) + n_0\delta = w(f) + w(g).$$

So w is a valuation on $K[x]$, hence yields a valuation on L extending v and satisfying $w(x) = \delta$.

It is an instructive exercise to prove $\boldsymbol{k}_v = \boldsymbol{k}_w$. □

3.22. Let (K, A) be an algebraically closed valued field with $A \neq K$, and consider it as a structure for the language of rings with a unary relation symbol U (interpreted as the set A). Then the binary relation "$v_A(x) \leq v_A(y)$" on K is definable in (K, A) by the formula $\exists z\big(U(z) \wedge xz = y\big)$. However, one can show that this relation is not qf-definable in (K, A), even if we allow names for the elements of K to be used. Thus QE for algebraically closed valued fields needs a different language. It turns out that the binary relation above is the only *obstruction* to QE in the language above.

3.23 Definition. A *valuation divisibility* on a domain R is a binary relation $|$ on R such that for all $x, y, z \in R$

(i) not $0 \mid 1$;

(ii) $x \mid y$ and $y \mid z \implies x \mid z$;

(iii) $x \mid y$ and $x \mid z \implies x \mid y + z$;

(iv) $x \mid y \iff xz \mid yz$ for $z \neq 0$;

(v) $x \mid y$ or $y \mid x$.

3.24. Lemma. *Valuation divisibilities and valuations are related as follows:*

(i) Each valuation ring A of a field K gives rise to a valuation divisiblity $|_A$ on K by

$$x \mid_A y \iff v_A(x) \leq v_A(y) \ (\iff ax = y \text{ for some } a \in A).$$

(ii) Given a field K, the map

$$A \mapsto |_A : \{ \text{valuation rings of } K \} \longrightarrow \{ \text{valuation divisibilities on } K \}$$

is a bijection.

(iii) For each valuation divisibility $|$ on a domain R there is a unique valuation divisiblity $|'$ on $K = \mathrm{Frac}(R)$ such that $(R, |) \subseteq (K, |')$; it is given by

$$\frac{a_1}{b} \mid' \frac{a_2}{b} \iff a_1 \mid a_2 \qquad (a_1, a_2, b \in R, b \neq 0).$$

(iv) The valuation divisibilities on $\mathbb{Z}$ are exactly the $|_p$ (p a prime number) and $|_t$, where $|_t$ is the trivial valuation divisibility:

$$a \,|_p\, b \iff v_p(a) \leq v_p(b),$$

$$a \,|_t\, b \text{ for all } a, b \text{ with } a \neq 0.$$

3.25 Definition. Let $L_{\text{val}} := \{\, 0, 1, +, -, \cdot, |\,\}$ be the language of rings with a binary relation symbol $|$, and let ACF_{val} be the theory in this language whose models are the structures $(K, |\ )$ such that $K \models ACF$, and $|$ is a *non-trivial* valuation divisibility on K. (Here a valuation divisibility on a field K is said to be *trivial* if the corresponding valuation ring is K, equivalently, the associated valuation is trivial.)

We shall obtain quantifier elimination (QE) for ACF_{val} using

QE-Test: Given a theory T, the following are equivalent:

1. T has QE;
2. given any models $\mathcal{M}, \mathcal{N}$ of T where $\mathcal{N}$ is $|\mathcal{M}|^+$-saturated, and given any embedding $i : \mathcal{A} \to \mathcal{N}$ of a proper substructure $\mathcal{A}$ of $\mathcal{M}$ into $\mathcal{N}$, we can extend i to an embedding $j : \mathcal{A}' \to \mathcal{N}$ of some substructure $\mathcal{A}'$ of $\mathcal{M}$ that properly extends $\mathcal{A}$.

Thus the algebraic counterpart of T having QE is that isomorphisms between substructures of models of T can be extended.

Any substructure of a model of ACF_{val} is clearly a domain with a valuation divisibility on it. Conversely, every domain with a valuation divisibility on it is a substructure of a model of ACF_{val}: first extend the domain with its valuation divisibility to its fraction field; then extend further to the algebraic closure of the fraction field; in case a valuation is trivial, adjoin a transcendental to make it non-trivial.

Let $(R, |)$ be a domain with valuation divisibility $|$ on R, and let

$$i : (R, |) \to (F, |_F)$$

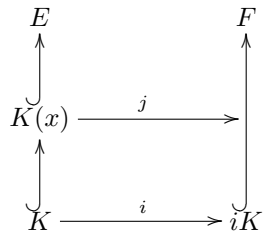
be an embedding into an algebraically closed field F with valuation divisibility $|_F$ on F. By item (iii) of the lemma above, and using its notation, we can extend i uniquely to an embedding $i' : (K, |') \to (F, |_F\ )$. Let $\widetilde{K}$ be an algebraic closure of K, and $\widetilde{|}$ a valuation divisibility on $\widetilde{K}$ such that $(K, |') \subseteq (\widetilde{K}, \widetilde{|}\ )$. Then by corollary 3.14 we can extend i' to an embedding $\widetilde{i} : (\widetilde{K}, \widetilde{|}\ ) \to (F, |_F)$.

3.26. Theorem. *ACF_{val} has QE.*

Proof. By the remarks preceding the theorem, and the QE-test it suffices to prove the following:

Let (E, A), (F, B) be non-trivially valued algebraically closed fields such that (F, B) is $|E|^+$-saturated. Let K be a proper algebraically closed subfield of E,

and $i : (K, A \cap K) \longrightarrow (F, B)$ a valued field embedding. Then there is $x \in E \setminus K$ such that i extends to a valued field embedding $j : (K(x), A \cap K(x)) \longrightarrow (F, B)$.



To find such x and j we shall distinguish three cases. To simplify notation, denote both v_A and v_B by v, and let $\overline{z}$ be the residue class of z in $\boldsymbol{k}_A$ for $z \in A$, and also the residue class of z in $\boldsymbol{k}_B$ for $z \in B$.

Case 1: $\boldsymbol{k}_{A\cap K} \neq \boldsymbol{k}_A$. Then we take $x \in A$ such that $\overline{x} \notin \boldsymbol{k}_{A\cap K}$. Since $\boldsymbol{k}_{A\cap K}$ is algebraically closed, $\overline{x}$ is transcendental over $\boldsymbol{k}_{A\cap K}$. Also $x \notin K$, so x is transcendental over K. By the saturation assumption on (F, B) we can find $y \in B$ such that $\overline{y} \notin \boldsymbol{k}_{B\cap iK}$. So $\overline{y}$ is transcendental over $\boldsymbol{k}_{B\cap iK}$ and y is transcendental over iK. Extend i to a field isomorphism $j : K(x) \longrightarrow (iK)(y)$ by $j(x) = y$. By the uniqueness part of lemma 3.19, j is also an isomorphism

$$\big(K(x), A \cap K(x)\big) \xrightarrow{\sim} \big((iK)(y), B \cap (iK)(y)\big) \subseteq (F, B).$$

Case 2: $v(K^\times) \neq v(E^\times)$. Take any $\gamma \in v(E^\times) \setminus v(K^\times)$. Note that $v(K^\times)$ and $v(iK^\times)$ are divisible. Since (F, B) is κ^+-saturated where $\kappa = |K|$, so is $v(F^\times)$ as an ordered abelian group. Also $v(F^\times) \neq \{0\}$. It follows that we can take $\delta \in v(F^\times) \setminus v(iK^\times)$ such that for all $a \in K^\times$,

$$\gamma < v(a) \iff \delta < v(ia).$$

Thus the isomorphism of ordered abelian groups

$$va \mapsto v(ia) : v(K^\times) \longrightarrow v(iK^\times), \qquad (a \in K^\times)$$

extends to an isomorphism of ordered abelian groups

$$va + k\gamma \mapsto v(ia) + k\delta : v(K^\times) + \mathbb{Z}\gamma \longrightarrow v(iK^\times) + \mathbb{Z}\delta.$$

Take $x \in E^\times$ and $y \in F^\times$ such that $vx = \gamma$, and $vy = \delta$. Since $x \notin K$, x is transcendental over K; likewise, y is transcendental over iK. By the uniqueness part of lemma 3.20, the field isomorphism $j : K(x) \longrightarrow (iK)(y)$ extending i and sending x to y is even a valued field isomorphism

$$\big(K(x), A \cap K(x)\big) \xrightarrow{\sim} \big((iK)(y), B \cap (iK)(y)\big) \subseteq (F, B).$$

Case 3: $\boldsymbol{k}_{A\cap K} = \boldsymbol{k}_A$ and $v(K^\times) = v(E^\times) =: \Gamma$. Take any $x \in E \setminus K$. The valuation $v|_{K(x)} : K(x) \to \Gamma_\infty$ is completely determined by $v|_K : K \to \Gamma_\infty$

and by the map $a \mapsto v(x-a) : K \longrightarrow \Gamma$, since each $f \in K[x] \setminus \{0\}$ factors as $f = c\prod_i (x-a_i)$ with $c, a_i \in K$, so $vf = vc + \sum_i v(x-a_i)$. To simplify notation, let us identify $(K, A \cap K)$ with $(iK, B \cap iK)$ via i (so both now have value group Γ). It is enough to find $y \in F \setminus iK$ such that $v(y-a) = v(x-a)$ for all $a \in K$, because for such y the field isomorphism $j : K(x) \longrightarrow (iK)(y)$ extending i and sending x to y is even a valued field isomorphism

$$(K(x), A \cap K(x)) \xrightarrow{\sim} ((iK)(y), B \cap (iK)(y)) \subseteq (F, B).$$

Such an element y exists by saturation and the following general lemma. □

3.27. Lemma. *Let $(K, A) \subseteq (L, B)$ be a valued field extension such that $\boldsymbol{k}_A = \boldsymbol{k}_B$, and let $v = v_B$. Let $a_1, \ldots, a_n \in K$, $n \geq 1$, and let $x \in L \setminus K$ be such that $v(x-a_i) \in v(K^\times)$ for $i = 1, \ldots, n$. Then there exists $a \in K$ such that $v(x-a_i) = v(a-a_i)$ for $i = 1, \ldots, n$.*

Proof. Any $a \in K$ such that $v(a-x) > v(a-a_i)$ for $i = 1, \ldots, n$ has the desired property. We may assume $v(x-a_1) \geq v(x-a_i)$ for $i = 2, \ldots, n$. Since $v(x-a_1) \in v(K^\times)$ we can take $b \in K$ such that $v(x-a_1) = vb$. So $v(\frac{x-a_1}{b}) = 0$, and since $\boldsymbol{k}_A = \boldsymbol{k}_B$, $\frac{x-a_1}{b} = c + \varepsilon$ with $c \in K$, $v(c) = 0$, $v(\varepsilon) > 0$. Then $a = a_1 + bc$ works because $x - a = b\varepsilon$ and $v(b\varepsilon) > v(x-a_i)$. □

3.3 The complete extensions of $ACF_{\mathbf{val}}$

For a valued field (K, A) with residue field $\boldsymbol{k} = \boldsymbol{k}_A$ the pair $\big(\mathrm{char}(K), \mathrm{char}(\boldsymbol{k})\big)$ can take the following values:

$(0,0)$: "equicharacteristic 0"; an example is $\boldsymbol{k}((t^\Gamma))$ with $\mathrm{char}(\boldsymbol{k}) = 0$ and the usual valuation.

$(0,p)$, p a prime number: "mixed characteristic p"; an example is $\mathbb{Q}_p$ with the p-adic valuation, whose residue field is $\mathbb{F}_p$.

(p,p), p a prime number: "equicharacteristic p"; an example is $\boldsymbol{k}((t^\Gamma))$ with $\mathrm{char}(\boldsymbol{k}) = p$ and the usual valuation.

It is easy to check that $(p,0)$ with p prime, and (p,q) with p, q distinct primes, are impossible as values of $\big(\mathrm{char}(K), \mathrm{char}(\boldsymbol{k})\big)$. Let us call $\big(\mathrm{char}(K), \mathrm{char}(\boldsymbol{k})\big)$ the *characteristic* of the valued field (K, A).

Let (a,b) be a possible characteristic of a valued field, and let $ACF_{\mathrm{val}}(a,b)$ be obtained from ACF_{val} by adding axioms specifying that the characteristic of the underlying field is a and that the characteristic of the residue field is b.

3.28. Corollary. *$ACF_{val}(a,b)$ is complete.*

Proof. Construing valued fields as fields with a valuation divisibility, those of characteristic $(0,0)$ all have (an isomorphic copy of) $(\mathbb{Z}, |_{\mathrm{t}})$ as substructure, those of charcteristic $(0,p)$ have $(\mathbb{Z}, |_p)$ and those of characteristic (p,p) have $(\mathbb{F}_p, |_{\mathrm{t}})$ as substructure, where $|_{\mathrm{t}}$ is the trivial valuation divisibility on $\mathbb{F}_p$. To see this, use the classification of valuation divisibilities on $\mathbb{Z}$, and the fact that finite fields only admit the trivial valuation divisibility. □

Let (K, A) be a non-trivially valued algebraically closed field. The above suggests some natural model-theoretic questions.

1. Find natural models for the completions of ACF_{val}.
2. What is the shape of the subsets of K definable in (K, A)?
3. What structure does (K, A) induce on $\boldsymbol{k}_A$ and Γ_A?
4. What is the definable closure (in (K, A)) of a subfield of K?
5. Does ACF_{val} or some natural expansion of it by definable sorts admit elimination of imaginaries?

Later we shall prove the following answers to some of these questions:

1. For any algebraically closed field $\boldsymbol{k}$ and any divisible ordered abelian group Γ, the power series field $\boldsymbol{k}((t^\Gamma))$ is also algebraically closed, in particular, $\mathbb{C}((t^{\mathbb{Q}}))$ with its usual valuation divisibility is a model of $ACF_{\text{val}}(0, 0)$, and $\widetilde{\mathbb{F}_p}((t^{\mathbb{Q}}))$ with its usual valuation divisibility is a model of $ACF_{\text{val}}(p, p)$. (Here p is a prime number and $\widetilde{\mathbb{F}_p}$ is the algebraic closure of $\mathbb{F}_p$.)
2. Each definable subset of K is a disjoint union of finitely many swiss cheeses, where a *swiss cheese* is a set $D \setminus (E_1 \cup \cdots \cup E_n)$ with D either a disc in K or $D = K$, and $E_1, \ldots, E_n$ discs in K.
3. ToDo: reference
4. ToDo: ref to homework for case char 0
5. ToDo: reference

Exercise on Puiseux series fields. Let $\boldsymbol{k}$ be a field, and define the field of *Puiseux series* over $\boldsymbol{k}$ to be the subfield of $\boldsymbol{k}((t^{\mathbb{Q}}))$ given by

$$P(\boldsymbol{k}) := \bigcup_{d=1}^{\infty} \boldsymbol{k}((t^{\frac{1}{d}\mathbb{Z}})).$$

Note that $P(\boldsymbol{k})$ contains the field $\boldsymbol{k}((t))$ of Laurent series over $\boldsymbol{k}$ as a subfield. Show that if d is a positive integer and $\alpha = t^{\frac{1}{d}} \in P(\boldsymbol{k})$, then

$$\boldsymbol{k}((t^{\frac{1}{d}\mathbb{Z}})) = \boldsymbol{k}((t)) + \boldsymbol{k}((t))\alpha + \cdots + \boldsymbol{k}((t))\alpha^{d-1}.$$

Use this to show that $\boldsymbol{k}((t^{\frac{1}{d}\mathbb{Z}}))$ is an algebraic extension of $\boldsymbol{k}((t))$ of degree d. (Thus $P(\boldsymbol{k})$ is an algebraic extension of $\boldsymbol{k}((t))$.)

Show that the closure of $P(\boldsymbol{k})$ in $\boldsymbol{k}((t^{\mathbb{Q}}))$ (with respect to the valuation topology) is the subfield

$$\left\{ f \in \boldsymbol{k}((t^{\mathbb{Q}})) \mid \operatorname{supp} f \cap (-\infty, n) \text{ is finite for each } n \right\}$$

of $\boldsymbol{k}((t^{\mathbb{Q}}))$. In particular, $P(\boldsymbol{k})$ is not dense in $\boldsymbol{k}((t^{\mathbb{Q}}))$, although it has the same residue field $\boldsymbol{k}$ and the same value group $\mathbb{Q}$ as $\boldsymbol{k}((t^{\mathbb{Q}}))$.

Comment on exercise: It will be shown later that if $\boldsymbol{k}$ is algebraically closed of characteristic 0, then $P(\boldsymbol{k})$ is algebraically closed, and thus an algebraic closure of $\boldsymbol{k}((t))$. On the other hand, if $\boldsymbol{k}$ is algebraically closed of characteristic $p \neq 0$, then $P(\boldsymbol{k})$ is not algebraically closed, since the equation $x^p - x - t^{-1} = 0$ over $P(\boldsymbol{k})$ has a root

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

in $\boldsymbol{k}((t^{\mathbb{Q}}))$ that does not lie in $P(\boldsymbol{k})$.

4 Immediate Extensions

Consider a valued field extension $(K, v, \Gamma) \subseteq (K', v', \Gamma')$. We identify $\boldsymbol{k}_v$ with a subfield of $\boldsymbol{k}_{v'}$ in the usual way. This extension is said to be *immediate* if $\boldsymbol{k}_v = \boldsymbol{k}_{v'}$ and $\Gamma = \Gamma'$. The basic facts on immediate extensions, due to Ostrowski, Krull, Kaplansky (first half of the 20th century), have their own intrinsic interest, and are also crucial in the later work by Ax–Kochen and Ersov.

These facts are related to the notion of *pseudoconvergence*. To explain this, consider for example the valued field $P(\boldsymbol{k})$ of Puiseux series over a field $\boldsymbol{k}$ and its immediate valued field extension $\boldsymbol{k}((t^{\mathbb{Q}}))$ (with valuation v). The series

$$a = 1 + t^{1/2} + t^{2/3} + t^{3/4} + \cdots = \sum_n t^{n/(n+1)}$$

in $\boldsymbol{k}((t^{\mathbb{Q}}))$ does not lie in $P(\boldsymbol{k})$. While a is approximated in a certain sense by the sequence $\{a_n\}$ in $P(\boldsymbol{k})$, where $a_n := \sum_{i=0}^{n} t^{i/(i+1)}$, a is not the limit of this sequence in the valuation topology of $\boldsymbol{k}((t^{\mathbb{Q}}))$: $v(a - a_n) \not\to \infty$ as $n \to \infty$, in fact, $v(a - a_n) < 1$ for all n. On the other hand, $v(a - a_n)$ is strictly increasing as a function of n, and this suggests a notion of (pseudo)limit that turns out to be useful.

In this section (K, v, Γ) *is a valued field, and* $\mathcal{O} := \mathcal{O}_v, \mathfrak{m} := \mathfrak{m}_v, \boldsymbol{k} := \boldsymbol{k}_v$.

4.1 Pseudoconvergence

A *well-indexed sequence in* K is a sequence $\{a_\rho\}$ in K whose terms a_ρ are indexed by the elements ρ of an infinite well-ordered set without a last element. Let $\{a_\rho\}$ be a *well-indexed sequence in* K, and $a \in K$. Then $\{a_\rho\}$ is said to *pseudoconverge to* a (notation: $a_\rho \rightsquigarrow a$), if $\{v(a - a_\rho)\}$ is eventually strictly increasing, that is, for some index ρ_0 we have $v(a - a_\sigma) > v(a - a_\rho)$ whenever $\sigma > \rho > \rho_0$. We also say in that case that a *is a pseudolimit of* $\{a_\rho\}$. Note that if $a_\rho \rightsquigarrow a$, then $a_\rho + b \rightsquigarrow a + b$ for each $b \in K$, and $a_\rho b \rightsquigarrow ab$ for each $b \in K^\times$. We also have the equivalence

$$a_\rho \rightsquigarrow 0 \iff \{v(a_\rho)\} \text{ is eventually strictly increasing.}$$

4.1. Lemma. *Let $\{a_\rho\}$ be a well-indexed sequence in K such that $a_\rho \rightsquigarrow a$ where $a \in K$. With $\gamma_\rho := v(a - a_\rho)$, we have:*

(i) either $va > va_\rho$ eventually, or $va_\rho = va$ eventually.

(ii) $\{va_\rho\}$ is either eventually strictly increasing, or eventually constant.

(iii) For each $b \in K$: $a_\rho \rightsquigarrow b \iff v(a-b) > \gamma_\rho$ eventually.

Proof. Let ρ_0 be as in the definition of "$a_\rho \rightsquigarrow a$". Suppose $va \leq va_\rho$ for a certain $\rho > \rho_0$. Then we claim that $va = va_\sigma$ for all $\sigma > \rho$. This is because for $\sigma > \rho$ we have $v(a - a_\sigma) > v(a - a_\rho) \geq va$, so $va = va_\sigma$. This proves (i). Now (ii) follows from (i) by noting that if $va > va_\rho$ eventually, then $v(a - a_\rho) = va_\rho$ eventually, so $\{va_\rho\}$ is eventually strictly increasing. We leave (iii) to the reader. □

If $\{a_\rho\}$ is a well-indexed sequence in K and $a \in K'$ where (K', v', Γ') is a valued field extension of (K, v, Γ), then "$a_\rho \rightsquigarrow a$" is of course to be interpreted in this valued field extension, that is, by considering the sequence $\{a_\rho\}$ in K as a sequence in K'.

4.2. Lemma. *Suppose (K', v', Γ) is an immediate valued field extension of (K, v, Γ), and let $a' \in K' \setminus K$. Then there is well-indexed sequence $\{a_\rho\}$ in K such that $a_\rho \rightsquigarrow a'$ and $\{a_\rho\}$ has no pseudolimit in K.*

Proof. We claim that the subset $\{v'(a'-x) : x \in K\}$ of Γ has no largest element. To see this, let $x \in K$; we shall find $y \in K$ such that $v'(a' - y) > v'(a' - x)$. Take $b \in K$ such that $v'(a' - x) = vb$. Then $v'(\frac{a'-x}{b}) = 0$, so $\frac{a'-x}{b} = c + \epsilon$ with $c \in K$, $vc = 0$, and $v'\epsilon > 0$. Then $a' - x = bc + b\epsilon$, and thus $y = x + bc$ has the desired property. It follows that we can take a well-indexed sequence $\{a_\rho\}$ in K such that the sequence $\{v'(a' - a_\rho)\}$ is strictly increasing and cofinal in $\{v'(a' - x) : x \in K\}$. Thus $a_\rho \rightsquigarrow a'$. If $a_\rho \rightsquigarrow a \in K$, then $v'(a' - a) > v(a' - a_\rho)$ for all ρ by Lemma 4.1, part(iii), hence $v'(a' - a) > v(a' - x)$ for all $x \in K$, a contradiction. □

An illustration of this lemma comes from the beginning of this section: we have the immediate valued field extension $P(\boldsymbol{k}) \subseteq \boldsymbol{k}((t^{\mathbb{Q}}))$, the sequence $\{a_n\}$ in $P(\boldsymbol{k})$ has no pseudolimit in $P(\boldsymbol{k})$ but pseudoconverges to $a \in \boldsymbol{k}((t^{\mathbb{Q}}))$. Note also that the pseudolimits of $\{a_n\}$ in $\boldsymbol{k}((t^{\mathbb{Q}}))$ are exactly the series $a + b$ with $vb \geq 1$, by part (iii) of Lemma 4.1.

To capture within (K, v, Γ) that a well-indexed sequence $\{a_\rho\}$ in K has a pseudolimit in some valued field extension we make the following definition. A *pseudo-cauchy sequence in K* (more precisely, in (K, v, Γ)) is a well-indexed sequence $\{a_\rho\}$ in K such that for some index ρ_0 we have

$$\tau > \sigma > \rho > \rho_0 \implies v(a_\tau - a_\sigma) > v(a_\sigma - a_\rho).$$

We also write "pc-sequence" for "pseudo-cauchy sequence".

4.3. Lemma. *Let $\{a_\rho\}$ be a well-indexed sequence in K. Then $\{a_\rho\}$ is a pc-sequence in K if and only if $\{a_\rho\}$ has a pseudolimit in some valued field extension of (K, v, Γ). In that case, $\{a_\rho\}$ has even a pseudolimit in some elementary extension of (K, v, Γ).*

Proof. Suppose $\{a_\rho\}$ is a pc-sequence in K, and let ρ_0 be as in the definition of "pseudo-cauchy sequence". We consider the partial type in the variable x consisting of the formulas

$$v(x - a_\sigma) > v(x - a_\rho), \qquad (\sigma > \rho > \rho_0).$$

Every finite subset of this partial type is realized by some a_τ. By compactness we can realize this partial type by a suitable $a \in K'$ for some elementary extension (K', v', Γ') of (K, v, Γ), and then $a_\rho \rightsquigarrow a$.

For the converse, suppose $a_\rho \rightsquigarrow a$ where $a \in K'$ and (K', v', Γ') is a valued field extension of (K, v, Γ). Let ρ_0 be as in the definition of pseudolimit, and let $\sigma > \rho > \rho_0$. Then $a_\sigma - a_\rho = (a_\sigma - a) - (a_\rho - a)$, so $v(a_\sigma - a_\rho) = v(a - a_\rho)$. So if in addition $\tau > \sigma$, then $v(a_\tau - a_\sigma) = v(a - a_\sigma) > v(a - a_\rho) = v(a_\sigma - a_\rho)$. □

This Lemma, and part (ii) of Lemma 4.1 yield:

4.4. Corollary. *If $\{a_\rho\}$ is a pc-sequence in K, then $\{va_\rho\}$ is either eventually strictly increasing, or eventually constant.*

We are going to show that polynomials behave well on pc-sequences, and in this connection it is useful to fix some notation. For a polynomial $f(x) \in K[x]$ of degree $\leq n$ we have a unique Taylor expansion for $f(x + y)$ in the ring $K[x, y]$ of polynomials over K in the distinct indeterminates x, y:

$$f(x + y) = \sum_{i=0}^{n} f_{(i)}(x) \cdot y^i,$$

where each $f_{(i)}(x) \in K[x]$. For convenience we also set $f_{(i)} = 0$ for $i > n$, so $f_{(0)} = f$ and $f_{(1)} = f'$. (If $\mathrm{char}(K) = 0$, then $f_{(i)}(x) = f^{(i)}(x)/i!$ where $f^{(i)}$ is the usual i^{th} formal derivative of f.) It is convenient to record here the following identity, although is is needed only much later in this section:

4.5. Lemma. $f_{(i)(j)} = \binom{i+j}{i} f_{(i+j)}, \qquad (i, j \in \mathbb{N}).$

We also need an elementary fact on ordered abelian groups whose proof we leave to the reader as an easy exercise.

4.6. Lemma *For each i in a finite nonempty set I, let $\beta_i \in \Gamma$, and $n_i \in \mathbb{N}^{>0}$, and let $\lambda_i : \Gamma \to \Gamma$ be the linear function given by $\lambda_i(\gamma) = \beta_i + n_i\gamma$. Assume that $n_i \neq n_j$ for distinct $i, j \in I$. Let $\rho \mapsto \gamma_\rho$ be a strictly increasing function from an infinite linearly ordered set without largest element into Γ. Then there is an $i_0 \in I$ such that if $i \in I$ and $i \neq i_0$, then $\lambda_{i_0}(\gamma_\rho) < \lambda_i(\gamma_\rho)$, eventually.*

We can now prove an important continuity property of polynomials:

4.7. Proposition. *Let $\{a_\rho\}$ be a well-indexed sequence in K such that $a_\rho \rightsquigarrow a$, where $a \in K$, and let $f(x) \in K[x]$ be a nonconstant polynomial (that is, $f \notin K$). Then $f(a_\rho) \rightsquigarrow f(a)$.*

Proof. Let f be of degree $\leq n$, so we have the identity

$$f(x+y) = f(x) + f_{(1)}(x)y + \cdots + f_{(n)}(x)y^n$$

in the polynomial ring $K[x,y]$. Substituting a for x and $a_\rho - a$ for y yields

$$f(a_\rho) - f(a) = f_{(1)}(a)(a_\rho - a) + \cdots + f_{(n)}(a)(a_\rho - a)^n = \sum_{i=1}^{n} f_{(i)}(a)(a_\rho - a)^i.$$

Since $f(x) = f(a) + \sum_{i=1}^{n} f_{(i)}(a)(x-a)^i$ and f is not constant, there exists $i \in \{1,\dots,n\}$ such that $f_{(i)}(a) \neq 0$. Now $v\big(f_{(i)}(a)(a_\rho - a)^i\big) = \beta_i + i\gamma_\rho$ where $\beta_i := v\big(f_{(i)}(a)\big)$ and $\gamma_\rho := v(a_\rho - a)$. Since $\{\gamma_\rho\}$ is eventually strictly increasing, there is by the previous lemma an $i_0 \in \{1,\dots,n\}$ such that for every $i \in \{1,\dots,n\}$ with $i \neq i_0$ we have

$$\beta_{i_0} + i_0\gamma_\rho < \beta_i + i\gamma_\rho, \quad \text{eventually.}$$

Then $v\big(f(a_\rho) - f(a)\big) = \beta_{i_0} + i_0\gamma_\rho$ eventually, in particular, $\{v\big(f(a_\rho) - f(a)\big)\}$ is eventually strictly increasing, that is, $f(a_\rho) \rightsquigarrow f(a)$. □

4.8. Corollary. *Suppose $\{a_\rho\}$ is a pc-sequence in K, and $f(x) \in K[x]$ is nonconstant. Then $\{f(a_\rho)\}$ is a pc-sequence.*

Proof. By Lemma 4.3 we have $a_\rho \rightsquigarrow a$ with a in a valued field extension. Then $f(a_\rho) \rightsquigarrow f(a)$ in this extension, and thus $\{f(a_\rho)\}$ is a pc-sequence. □

Let $\{a_\rho\}$ be a pc-sequence in K, and let $f(x) \in K[x]$ be nonconstant. Then by the two corollaries above there are two possibilities: either

$$\{v\big(f(a_\rho)\big)\} \text{ is eventually strictly increasing,} \quad (\text{equivalently, } f(a_\rho) \rightsquigarrow 0),$$

or

$$\{v\big(f(a_\rho)\big)\} \text{ is eventually constant,} \quad (\text{equivalently, } f(a_\rho) \not\rightsquigarrow 0).$$

We say that $\{a_\rho\}$ is of *algebraic type over K* if the first possibility is realized for some nonconstant $f \in K[x]$, and then such an f of least degree is called a *minimal polynomial of $\{a_\rho\}$ over K*.

We say that $\{a_\rho\}$ is of *transcendental type over K* if the second possibility is realized for all nonconstant $f \in K[x]$. (Note that then $\{v\big(f(a_\rho)\big)\}$ is eventually constant for any $f \in K[x]$, whether constant or not.) A pc-sequence in K of transcendental type determines an essentially unique immediate extension:

4.9. Theorem *Let $\{a_\rho\}$ be a pc-sequence in K of transcendental type over K. Then $\{a_\rho\}$ has no pseudolimit in K. The valuation v on K extends uniquely to a valuation $v : K(x)^\times \to \Gamma$ (x transcendental over K) such that*

$$vf \;=\; \text{eventual value of } v(f(a_\rho))$$

for each $f \in K[x]$. With this valuation $K(x)$ is an immediate valued field extension of (K, v, Γ) in which $a_\rho \rightsquigarrow x$.

Conversely, if $a_\rho \rightsquigarrow a$ in a valued field extension of (K, v, Γ), then there is a valued field isomorphism $K(x) \to K(a)$ over K that sends x to a.

Proof. If $a_\rho \rightsquigarrow a$ with $a \in K$, then the polynomial $x - a$ witnesses that $\{a_\rho\}$ is of algebraic type over K. So $\{a_\rho\}$ has no pseudolimit in K.

It is clear that by defining vf for $f \in K[x]$ as in the above display, we have a valuation on $K[x]$, and thus on $K(x)$. The value group of this valuation is still Γ, and one checks easily that $a_\rho \rightsquigarrow x$. To verify that the residue field of $K(x)$ is the residue field of K we first note that because the value groups are equal, each $a \in K(x)$ with $va = 0$ has the form $a = f/g$ where $f, g \in K[x]$ with $vf = vg = 0$. So it is enough to consider a nonconstant $f \in K[x]$ with $vf = 0$, and find $b \in K$ with $v(f - b) > 0$. We have $0 = vf = v\big(f(a_\rho)\big)$ eventually, and $\{v\big(f - f(a_\rho)\big)\}$ is eventually strictly increasing, so $v\big(f - f(a_\rho)\big) > 0$, eventually. Thus $b = f(a_\rho)$ for big enough ρ will do the job.

Finally, suppose $a_\rho \rightsquigarrow a$ with a in a valued field extension whose valuation we also indicate by v for simplicity. For nonconstant $f \in K[x]$ we have $f(a_\rho) \rightsquigarrow f(a)$, and thus $v\big(f(a)\big) = v\big(f(a_\rho)\big)$ eventually; in particular, $f(a) \neq 0$ and $v(f(a)) = vf \in \Gamma$. Thus a is transcendental over K and the field isomorphism $K(x) \to K(a)$ over K that sends x to a is even a valued field isomorphism. $\square$

Here is the analogue for pc-sequences of *algebraic* type over K:

4.10. Theorem *Let $\{a_\rho\}$ be a pc-sequence in K of algebraic type over K, without pseudolimit in K, and let $\mu(x)$ be a minimal polynomial of $\{a_\rho\}$ over K. Then μ is irreducible in $K[x]$ and $\deg \mu \geq 2$. Let a be a zero of μ in an extension field of K. Then v extends uniquely to a valuation $v : K(a)^\times \to \Gamma$ such that*

$$v\big(f(a)\big) \;=\; \text{eventual value of } v\big(f(a_\rho)\big)$$

for each nonzero polynomial $f \in K[x]$ of degree $< \deg \mu$. With this valuation $K(a)$ is an immediate valued field extension of (K, v, Γ), and $a_\rho \rightsquigarrow a$.

Conversely, if $\mu(b) = 0$ and $a_\rho \rightsquigarrow b$ in a valued field extension of (K, v, Γ), then there is a valued field isomorphism $K(a) \to K(b)$ over K sending a to b.

Proof. Much of the proof duplicates the proof for the case of transcendental type. A difference is in how we obtain the multiplicative law for $v : K(a)^\times \to \Gamma$ as defined above. Let $s, t \in K(a)^\times$, and write $s = f(a), t = g(a)$ with nonzero $f, g \in K[x]$ of degree $< \deg \mu$. Then $fg = q\mu + r$ with $q, r \in K[x]$ and $\deg r < \deg \mu$, so $st = r(a)$, and thus eventually

$$v(s) = v\big(f(a_\rho)\big), \quad v(t) = v\big(g(a_\rho)\big), \quad v(st) = v\big(r(a_\rho)\big).$$

Also $v(s)+v(t)=v\big(f(a_\rho)g(a_\rho)\big)=v\big(q(a_\rho)\mu(a_\rho)+r(a_\rho)\big)$, eventually. Since $\{v\big(q(a_\rho)\mu(a_\rho)\big)\}$ is either eventually strictly increasing, or eventually ∞, this forces $v(s)+v(t)=v\big(r(a_\rho)\big)$, eventually, so $v(s)+v(t)=v(st)$. □

The minimal polynomial $\mu(x)$ in this theorem, even if we assume it to be monic, is in general highly non-unique. (For example, adding to its constant term an $\varepsilon\in K$ such that eventually $v\varepsilon > v(\mu a-\mu a_\rho)$, does not change its status as minimal polynomial of $\{a_\rho\}$.) That is why we have to specify a particular minimal polynomial in this theorem to achieve the uniqueness up to isomorphism of $K(a)$.

4.2 Maximal Valued Fields

A *maximal valued field* is by definition a valued field that has no immediate proper valued field extension. If $\boldsymbol{k}$ is algebraically closed and Γ is divisible, then by Corollary 3.18 the algebraic closure of K equipped with a valuation that extends v is necessarily an immediate extension of (K,v,Γ). Therefore:

4.11. Corollary. *If (K,v,Γ) is maximal valued, $\boldsymbol{k}$ is algebraically closed and Γ is divisible, then K is algebraically closed.*

Theorems 4.9 and 4.10 in combination with Lemma 4.2 yield:

4.12. Corollary. *(K,v,Γ) is maximal valued if and only if each pc-sequence in K has a pseudolimit in K.*

We use this equivalence to get the next result.

4.13. Corollary. *The Hahn field $\boldsymbol{k}((t^\Gamma))$ is maximal valued. If $\boldsymbol{k}$ is algebraically closed and Γ is divisible, then $\boldsymbol{k}((t^\Gamma))$ is algebraically closed.*

Proof. The first assertion implies the second one, so it is enough to consider an arbitrary pc-sequence $\{a_\rho\}$ in $\boldsymbol{k}((t^\Gamma))$ and show that it has a pseudolimit in $\boldsymbol{k}((t^\Gamma))$. Take an index ρ_0 such that

$$\tau>\sigma>\rho>\rho_0 \implies v(a_\tau-a_\sigma)>v(a_\sigma-a_\rho).$$

Below we restrict ρ to be $>\rho_0$. Note that we have $\gamma_\rho\in\Gamma$ with $v(a_\sigma-a_\rho)=\gamma_\rho$ for all $\sigma>\rho$, and that $\{\gamma_\rho\}$ is strictly increasing. We split up a_ρ as follows:

$$a_\rho=\sum_{\gamma<\gamma_\rho}c_{\gamma\rho}t^\gamma+\sum_{\gamma\geq\gamma_\rho}c_{\gamma\rho}t^\gamma,\qquad (\text{all } c_{\gamma\rho}\in\boldsymbol{k}).$$

Then $c_{\gamma\rho}=c_{\gamma\sigma}$ for $\gamma<\gamma_\rho$ and $\sigma>\rho$. For any $\gamma\in\Gamma$, either $\gamma<\gamma_\rho$ for *some* ρ, or $\gamma>\gamma_\rho$ for *all* ρ. Thus we can define the series $a:=\sum_\gamma c_\gamma t^\gamma\in\boldsymbol{k}((t^\Gamma))$ by setting $c_\gamma:=c_{\gamma\rho}$ whenever $\gamma<\gamma_\rho$, and $c_\gamma:=0$ if $\gamma>\gamma_\rho$ for all ρ. Then $a_\rho\rightsquigarrow a$, as is easily verified. □

Under certain conditions on residue field and value group, a maximal valued field is isomorphic to a Hahn field, see Corollary 4.31. First a consequence of Krull's cardinality bound $|K|\leq|\boldsymbol{k}|^{|\Gamma|}$ (Proposition 3.4) and Zorn:

4.14. Corollary. (K, v, Γ) *has an immediate maximal valued field extension.*

This raises of course the question whether such an extension is unique up to isomorphism. In the equicharacteristic 0 case the answer is yes (Corollary 4.28), but first we take care of a loose end in Theorem 4.10:

4.15. Lemma. *Let a in an immediate valued field extension of (K, v, Γ) be algebraic over K, and $a \notin K$. Then there is a pc-sequence $\{a_\rho\}$ in K of algebraic type over K that has no pseudolimit in K, such that $a_\rho \rightsquigarrow a$.*

Proof. By Lemma 4.2 we have a pc-sequence $\{a_\rho\}$ in K without pseudolimit in K, such that $a_\rho \rightsquigarrow a$. Let $f(x)$ be the minimum polynomial of a over K. Then by the Taylor identity preceding Lemma 4.5 we have

$$fa_\rho = fa_\rho - fa = (a_\rho - a) \cdot ga_\rho, \quad g(x) \in K(a)[x].$$

Thus $v(fa_\rho) = v(a_\rho - a) + v(ga_\rho)$. Since $\{v(a_\rho - a)\}$ is eventually strictly increasing and $\{v(ga_\rho)\}$ is eventually strictly increasing or eventually constant, $\{v(fa_\rho)\}$ is eventually strictly increasing, so $\{a_\rho\}$ is of algebraic type over K. □

A valued field is *algebraically maximal* if it has no immediate proper algebraic valued field extension. (Thus *maximal* $\Longrightarrow$ *algebraically maximal*.) Obviously, every algebraically closed valued field is algebraically maximal.

Theorem 4.10 and Lemma 4.15 yield:

4.16. Corollary. (K, v, Γ) *is algebraically maximal if and only if each pc-sequence in K of algebraic type over K has a pseudolimit in K.*

Just from the definition of *algebraically maximal* (and Zorn) it follows that (K, v, Γ) has an immediate valued field extension that is algebraically maximal and algebraic over K. A natural question is whether such an extension is determined up to isomorphism over (K, v, Γ). The answer is *yes* in equicharacteristic 0 and in some other cases, see Theorem 4.27 and its consequences.

First we show that algebraic maximality implies henselianity. A valued field is said to be *henselian* if its valuation ring is henselian.

4.17. Lemma. *Let $f \in \mathcal{O}[x]$ and $a \in \mathcal{O}$ be such that $v(fa) > 0$, $v(f'a) = 0$, and f has no zero in $a + \mathfrak{m}$. Then there is a pc-sequence $\{a_\rho\}$ in K such that $f(a_\rho) \rightsquigarrow 0$, and $\{a_\rho\}$ has no pseudolimit in K.*

Proof. We build such a sequence by the Newton approximation at the beginning of subsection 2.2, starting with $a_0 = a$. Indeed, this method yields $b \in \mathcal{O}$ such that $v(b-a) = v(fa) > 0$ and $v(fb) \geq 2v(fa) > 0$. In particular, $a \equiv b \mod \mathfrak{m}$, hence $f'a \equiv f'b \mod \mathfrak{m}$, so $v(f'b) = 0$. We now take $a_1 = b$, and continue with b as new input. More precisely, let λ be an ordinal > 0 and $\{a_\rho\}$ a sequence in $a + \mathfrak{m}$ indexed by the ordinals $\rho < \lambda$ such that $a_0 = a$, and $v(a_\sigma - a_\rho) = v(fa_\rho)$ and $v(fa_\sigma) \geq 2v(fa_\rho)$ whenever $\lambda > \sigma > \rho$. (For $\lambda = 2$ we have such a sequence with $a_0 = a$ and $a_1 = b$.) If $\lambda = \mu + 1$ is a successor ordinal, then we construct the next term $a_\lambda \in a + \mathfrak{m}$ by Newton approximation so that $v(a_\lambda - a_\mu) = v(fa_\mu)$ and $v(fa_\lambda) \geq 2v(fa_\mu)$.

Suppose now that λ is a limit ordinal. Then $\{a_\rho\}$ is clearly a pc-sequence and $f(a_\rho) \rightsquigarrow 0$. If $\{a_\rho\}$ has no pseudolimit in K, then we are done. If $\{a_\rho\}$ has a pseudolimit in K, let a_λ be such a pseudolimit. Then $fa_\rho \rightsquigarrow fa_\lambda$; since $\{v(fa_\rho)\}$ is strictly increasing, this yields $v(fa_\lambda) \geq v(fa_{\rho+1}) \geq 2v(fa_\rho)$ for each index $\rho < \lambda$. It is also clear that $v(a_\lambda - a_\rho) = v(a_{\rho+1} - a_\rho) = v(fa_\rho)$ for each $\rho < \lambda$, in particular, $a_\lambda \in a + \mathfrak{m}$. Thus we have extended our sequence by one more term. This building process must come to an end. □

In combination with Theorem 4.10 the previous lemma yields:

4.18. Corollary. *Each algebraically maximal valued field is henselian (and thus each maximal valued field is henselian).*

For example, the Puiseux series field $P(\boldsymbol{k})$ is henselian, since it is the directed union of its maximal valued subfields $\boldsymbol{k}((t^{\frac{1}{d}\mathbb{Z}}))$ $(d = 1, 2, 3, \dots)$.
In the equicharacteristic 0 case, *algebraically maximal* is equivalent to *henselian*; see Corollary 4.22. For (K, v, Γ) to be henselian is a condition on polynomials over its valuation ring $\mathcal{O}$. It is convenient to have an equivalent condition for polynomials over K. Let $f(x) \in K[x]$ be of degree $\leq n$, and let $a \in K$, so

$$f(a + x) = \sum_{i=0}^{n} f_{(i)}(a)x^i = fa + f'(a)x + \sum_{i=2}^{n} f_{(i)}(a)x^i.$$

4.19 Definition. We say f, a is in *hensel configuration* if $f'a \neq 0$, and either $fa = 0$ or there is $\gamma \in \Gamma$ such that

$$v(fa) = v(f'a) + \gamma < v\big(f_{(i)}a\big) + i \cdot \gamma$$

for $2 \leq i \leq n$. (This γ is unique: $\gamma = v(fa) - v(f'a)$.)

Suppose f, a is in hensel configuration and $fa \neq 0$. Take γ as in the definition, take $c \in K$ with $vc = \gamma$ and put $g(x) := f(cx)/f(a)$ and $\alpha := a/c$. Then $g(\alpha) = 1$, $v\big(g'(\alpha)\big) = 0$, and $v\big(g_{(i)}(\alpha)\big) > 0$ for $i > 1$, as is easily verified. Thus

$$h(x) := g(\alpha + x) = 1 + g'(\alpha)x + \sum_{i=2}^{n} g_{(i)}(\alpha)x^i$$

lies in $\mathcal{O}[x]$. The set $\{u \in \mathcal{O} : v\big(1 + g'(\alpha)u\big) > 0\}$ is a congruence class modulo $\mathfrak{m}$. For u in this set we have $v\big(h(u)\big) = v\big(g(\alpha + u)\big) > 0$,

$$h'(u) = g'(\alpha + u) = g'(\alpha) + \sum_{j=1}^{n-1} g_{(1)(j)}(\alpha)u^j,$$

and $v\big(g_{(1)(j)}(\alpha)\big) \geq v\big(g_{(1+j)}(\alpha)\big) > 0$ for $j > 0$, so $v\big(h'(u)\big) = 0$.

Suppose now that (K, v, Γ) is henselian; this allows us to pick u as above such that $g(\alpha + u) = 0$. By Lemma 2.1 this u is unique in the sense that there is no $u' \in \mathcal{O}$ such that $g(\alpha + u') = 0$ and $u' \neq u$. Now $b := a + cu$ satisfies $f(b) = 0$ and $v(a - b) = \gamma$. Summarizing:

4.20. Lemma. *If (K, v, Γ) is henselian and f, a is in hensel configuration, then there is a unique $b \in K$ such that $f(b) = 0$ and $v(a-b) \geq v(fa) - v(f'a)$; this b satisfies $v(a-b) = v(fa) - v(f'a)$.*

Suppose (K, v, Γ) is of mixed characteristic $(0, p)$. Then we say that (K, v, Γ) is *finitely ramified* if the set $\{\gamma \in \Gamma : 0 \leq \gamma < vp\}$ is finite. For example, $\mathbb{Q}_p$ with its p-adic valuation is finitely ramified.

4.21. Proposition. *Suppose (K, v, Γ) is of equicharacteristic 0, or finitely ramified of mixed characteristic. Let $\{a_\rho\}$ be a pc-sequence in K and let $f(x) \in K[x]$ be such that $fa_\rho \rightsquigarrow 0$ and $f_{(j)}a_\rho \not\rightsquigarrow 0$ for all $j \geq 1$. Then*

(i) f, a_ρ is in hensel configuration, eventually;

(ii) in any henselian valued field extension of (K, v, Γ) there is a unique b such that $a_\rho \rightsquigarrow b$ and $f(b) = 0$.

Proof. Let a be a pseudolimit of $\{a_\rho\}$ in some valued field extension of (K, v, Γ) whose valuation we also denote by v, and put $\gamma_\rho := v(a - a_\rho)$. The proof of Proposition 4.7 yields a unique $j_0 \geq 1$ such that for each $k \geq 1$ with $k \neq j_0$,

$$v\big(fa_\rho - fa\big) = v\big(f_{(j_0)}a\big) + j_0\gamma_\rho < v\big(f_{(k)}a\big) + k \cdot \gamma_\rho, \quad \text{eventually.}$$

Now $f(a_\rho) \rightsquigarrow 0$, so for $k \geq 1$, $k \neq j_0$:

$$v\big(fa_\rho\big) = v\big(f_{(j_0)}a\big) + j_0 \cdot \gamma_\rho < v\big(f_{(k)}a\big) + k \cdot \gamma_\rho, \quad \text{eventually.}$$

We claim that $j_0 = 1$. Let $k > 1$; our claim will then follow by deriving

$$v\big(f'a\big) + \gamma_\rho < v\big(f_{(k)}a\big) + k\gamma_\rho, \quad \text{eventually.}$$

The proof of Proposition 4.7 applied to f' instead of f also yields

$$v\big(f'a_\rho - f'a\big) \leq v\big(f_{(1)(j)}a\big) + j \cdot \gamma_\rho, \quad \text{eventually}$$

for all $j \geq 1$. Since $v\big(f'a_\rho\big) = v\big(f'a\big)$ eventually, this yields

$$v\big(f'a\big) \leq v\big(f_{(1)(j)}a\big) + j \cdot \gamma_\rho, \quad \text{eventually}$$

for all $j \geq 1$. Using $f_{(1)(j)} = (1+j)f_{(1+j)}$ (Lemma 4.5), this gives for $j \geq 1$:

$$v\big(f'a\big) \leq v(1+j) + v\big(f_{(1+j)}(a)\big) + j \cdot \gamma_\rho, \quad \text{eventually}$$

For $j = k - 1$, this yields

$$v(f'a) \leq vk + v\big(f_{(k)}(a)\big) + (k-1) \cdot \gamma_\rho, \quad \text{eventually.}$$

The assumption on (K, v, Γ) then yields:

$$v\big(f'a\big) < v\big(f_{(k)}a\big) + (k-1) \cdot \gamma_\rho, \quad \text{eventually, hence}$$

$$v\big(f'a\big) + \gamma_\rho < v(f_{(k)}a) + k \cdot \gamma_\rho, \quad \text{eventually.}$$

Thus $j_0 = 1$, as claimed. Since for each $k \geq 1$ we have $v(f_{(k)}a_\rho) = v(f_{(k)}a)$, eventually, the above equalities and inequalities also show that f, a_ρ is in hensel configuration, eventually. This proves (i).

For (ii), let (K', v', Γ') be a henselian valued field extension of (K, v, Γ). After deleting an initial segment of the sequence $\{a_\rho\}$ we can assume that $\{\gamma_\rho\}$ is strictly increasing, that $v(a_\sigma - a_\rho) = \gamma_\rho$ whenever $\sigma > \rho$, and that $f'a_\rho \neq 0$ for all ρ. Likewise, by (i) and Lemma 4.20 we can assume that for every ρ there is a unique $b_\rho \in K'$ such that $f(b_\rho) = 0$ and $v(a_\rho - b_\rho) = v(fa_\rho) - v(f'a_\rho)$. The proof of (i) shows that we can also assume that $v(fa_\rho) - v(f'a_\rho) = \gamma_\rho$ for all ρ, so $v(a_\rho - b_\rho) = \gamma_\rho$ for all ρ. The uniqueness of b_ρ shows that $b_\sigma = b_\rho$ whenever $\sigma > \rho$. Thus all b_ρ are equal to a single b, which has the desired properties. □

4.22. Corollary. *Let (K, v, Γ) be of equicharacteristic 0, or finitely ramified of mixed characteristic. Then (K, v, Γ) is henselian if and only if it is algebraically maximal.*

Proof. Assume (K, v, Γ) is henselian, and let $\{a_\rho\}$ be a pc-sequence in K of algebraic type over K. Take a monic minimal polynomial $f(x)$ of $\{a_\rho\}$ over K. Then $fa_\rho \rightsquigarrow 0$ and $f_{(j)}a_\rho \not\rightsquigarrow 0$ for each $j \geq 1$, so f, a_ρ is in hensel configuration, eventually, and thus by Lemma 4.20 we have $b \in K$ such that $f(b) = 0$. Since $f(x)$ is irreducible, this gives $f(x) = x - b$, so $a_\rho \rightsquigarrow b$. □

This leads to a partial converse to some earlier results:

4.23. Corollary. *Let (K, v, Γ) be of equicharacteristic 0. Then K is algebraically closed if and only if (K, v, Γ) is henselian, $\boldsymbol{k}$ is algebraically closed and Γ is divisible.*

Puiseux series fields $P(\boldsymbol{k})$ are henselian with value group $\mathbb{Q}$, hence:

4.24. Application. *Suppose $\boldsymbol{k}$ is algebraically closed of characteristic 0. Then the Puiseux series field $P(\boldsymbol{k})$ is algebraically closed.*

Exercise. Let $\boldsymbol{k} \subseteq \boldsymbol{k}'$ be a field extension of finite degree n, and let $b_1, \dots, b_n$ be a basis of $\boldsymbol{k}'$ over $\boldsymbol{k}$. Show that $\boldsymbol{k}'((t^\Gamma))$ is also of finite degree n over its subfield $\boldsymbol{k}((t^\Gamma))$ with basis $b_1, \dots, b_n$.

Show that if $\boldsymbol{k}$ has characteristic 0 with algebraic closure $\tilde{\boldsymbol{k}}$, then the algebraic closure of $\boldsymbol{k}((t))$ in the algebraically closed field extension $\tilde{\boldsymbol{k}}((t^{\mathbb{Q}}))$ is the union of the Puiseux series fields $P(\boldsymbol{k}')$ where $\boldsymbol{k}'$ ranges over the subfields of $\tilde{\boldsymbol{k}}$ that contain $\boldsymbol{k}$ and are of finite degree over $\boldsymbol{k}$.

4.3 Henselization

The following notion is fundamental in valuation theory and beyond.

4.25 Definition. A *henselization* of (K, v, Γ) is a henselian valued field extension $(K^{\mathrm{h}}, v^{\mathrm{h}}, \Gamma^{\mathrm{h}})$ of (K, v, Γ) such that any valued field embedding

$$(K, v, \Gamma) \to (K', v', \Gamma')$$

into a henselian valued field (K', v', Γ') extends uniquely to an embedding

$$(K^{\mathrm{h}}, v^{\mathrm{h}}, \Gamma^{\mathrm{h}}) \to (K', v', \Gamma').$$

As usual with such definitions, existence guarantees uniqueness: if (K_1, v_1, Γ_1) and (K_2, v_2, Γ_2) are henselizations of (K, v, Γ), then the unique embedding $(K_1, v_1, \Gamma_1) \to (K_2, v_2, \Gamma_2)$ over (K, v, Γ) is an isomorphism. Thus there is no harm in referring to *the* henselization of (K, v, Γ) if there is one. Of course, if (K, v, Γ) is henselian, it is its own henselization. Also, if (K, v, Γ) has a henselization and (K', v', Γ') is any henselian valued field extension of (K, v, Γ), then the *henselization of* (K, v, Γ) *in* (K', v', Γ') is by definition the henselization $(K^{\mathrm{h}}, v^{\mathrm{h}}, \Gamma^{\mathrm{h}})$ of (K, v, Γ) such that

$$(K, v, \Gamma) \subseteq (K^{\mathrm{h}}, v^{\mathrm{h}}, \Gamma^{\mathrm{h}}) \subseteq (K', v', \Gamma').$$

4.26. Corollary. *Any henselization of* (K, v, Γ) *is an immediate valued field extension of* (K, v, Γ) *and algebraic over* K*.*

Proof. We already know that (K, v, Γ) has an immediate algebraically maximal valued field extension that is algebraic over K. Any henselization of (K, v, Γ) must embed over (K, v, Γ) into such an extension. □

Each valued field has a henselization, as we show later in the more general setting of local rings. For the Ax–Kochen–Ershov story it is enough to consider the equicharacteristic 0 case and the finitely ramified mixed characteristic case. In those cases the henselization has a particularly nice characterization:

4.27. Theorem. *Let* (K, v, Γ) *be of equicharacteristic* 0*, or finitely ramified of mixed characteristic. Let* (K_1, v_1, Γ) *be an immediate henselian valued field extension of* (K, v, Γ) *such that* K_1 *is algebraic over* K*. Then* (K_1, v_1, Γ) *is a henselization of* (K, v, Γ)*.*

Proof. Call a field L with $K \subseteq L \subseteq K_1$ *nice* if each valued field embedding from (K, v, Γ) into a henselian valued field (K', v', Γ') extends uniquely to an embedding from (L, v_L, Γ) into (K', v', Γ'), where $v_L := v_1|_{L^\times}$. Consider a nice field L such that $L \neq K_1$. With Zorn in mind, it clearly suffices to show that then there is a nice field L' with $L \subseteq L' \subseteq K_1$ and $L \neq L'$.

Lemma 4.15 gives a pc-sequence $\{a_\rho\}$ in L of algebraic type over L without pseudolimit in L. Take a minimal polynomial $\mu(x)$ of $\{a_\rho\}$ over L. Then $\mu(a_\rho) \rightsquigarrow 0$ and $\mu_{(j)}(a_\rho) \not\rightsquigarrow 0$ for all $j \geq 1$. Item (ii) of Proposition 4.21 yields $a \in K_1$ such that $a_\rho \rightsquigarrow a$ and $\mu(a) = 0$. Let a valued field embedding i from (K, v, Γ) into a henselian valued field (K', v', Γ') be given, and let i_L be the unique extension of i to an embedding from (L, v_L, Γ) into (K', v', Γ'). To simplify notation, identify (L, v_L, Γ) with a valued subfield of (K', v', Γ') via i_L. Item (ii) of Proposition 4.21 also gives a unique $b \in K'$ such that $a_\rho \rightsquigarrow b$ and $\mu(b) = 0$. Now apply Theorem 4.10 to conclude that $L(a)$ is nice. □

Since (K, v, Γ) has an immediate algebraically maximal valued field extension that is algebraic over K, this theorem shows in particular:

If (K, v, Γ) is of equicharacteristic 0 or finitely ramified of mixed characteristic, then (K, v, Γ) has a henselization, and any immediate algebraically maximal valued field extension of (K, v, Γ) that is algebraic over K is isomorphic over (K, v, Γ) to this henselization by a unique isomorphism.

4.4 Uniqueness of immediate maximal extensions

The results above have some very nice consequences:

4.28. Corollary. *Let (K, v, Γ) be of equicharacteristic 0, or finitely ramified of mixed characteristic. Then any two immediate maximal valued field extensions of (K, v, Γ) are isomorphic over (K, v, Γ).*

Proof. Let (K_1, v_1, Γ) and (K_2, v_2, Γ) be immediate maximal valued field extensions of (K, v, Γ). Below, each subfield of K_i $(i = 1, 2)$, is viewed as valued field by taking as valuation the restriction of v_i to the subfield. Consider fields L_1, L_2 with $K \subseteq L_1 \subseteq K_1$ and $K \subseteq L_2 \subseteq K_2$, and suppose we have a valued field isomorphism $L_1 \cong L_2$. Note that $L_1 = K_1$ iff $L_2 = K_2$.

Suppose $L_1 \neq K_1$ and $L_2 \neq K_2$. It suffices to show that then we can extend the isomorphism $L_1 \cong L_2$ to a valued field isomorphism $L_1' \cong L_2'$ where L_1' and L_2' are fields with $L_i \subseteq L_i' \subseteq K_i$ and $L_i \neq L_i'$ for $i = 1, 2$. If L_1 is not henselian, then we can take for L_i' the henselization of L_i in K_i, by Theorem 4.27. Suppose L_1 is henselian. Take $b \in K_1 \setminus L_1$, and take a pc-sequence $\{a_\rho\}$ in L_1 such that $a_\rho \rightsquigarrow b$ and $\{a_\rho\}$ has no pseudolimit in L_1. Since L_1 is algebraically maximal by Corollary 4.22, $\{a_\rho\}$ is of transcendental type over L_1. The image of $\{a_\rho\}$ under our isomorphism $L_1 \cong L_2$ has a pseudolimit $c \in K_2$, and then Theorem 4.9 allows us to extend this isomorphism to an isomorphism $L_1(b) \cong L_2(c)$. □

The next variant is just what we need for the proof of the Ax-Kochen-Ershov theorem in the next section.

4.29. Lemma. *Let (K, v, Γ) be of equicharacteristic 0, or finitely ramified of mixed characteristic, and let (K^*, v^*, Γ) be an immediate maximal extension of (K, v, Γ). Then we can embed (K^*, v^*, Γ) over (K, v, Γ) into any $|\Gamma|^+$-saturated henselian valued field extension (K', v', Γ') of (K, v, Γ).*

Proof. Exercise. □

Are there useful conditions on $\boldsymbol{k}$ and Γ implying that if (K, v, Γ) is maximal valued, then (K, v, Γ) is isomorphic to the Hahn field $\boldsymbol{k}((t^\Gamma))$? The answer is yes, and here liftings and cross-sections come into play. (A *lifting* of the residue field of (K, v, Γ) is a field embedding $i : \boldsymbol{k} \to K$ such that $\overline{ia} = a$ for all $a \in \boldsymbol{k}$. A *cross-section* of the valuation $v : K^\times \to \Gamma$ is a group morphism $s : \Gamma \to K^\times$ such that $v(s\gamma) = \gamma$ for all $\gamma \in \Gamma$.) For example, the valuation of the Hahn field $\boldsymbol{k}((t^\Gamma))$ has the cross-section $\gamma \mapsto t^\gamma$. Also, if $\Gamma = \mathbb{Z}$ and $v(\pi) = 1$, $\pi \in K$, then $k \mapsto \pi^k : \mathbb{Z} \to K^\times$ is a cross-section; in particular $\mathbb{Q}_p$ has cross section $k \mapsto p^k$.

To see how a lifting of the residue field and a cross-section of the valuation can help in answering the question above, we first single out the valued subfield $\boldsymbol{k}(t^\Gamma)$ of $\boldsymbol{k}((t^\Gamma))$: its underlying field is the subfield of $\boldsymbol{k}((t^\Gamma))$ generated over $\boldsymbol{k}$ by the multiplicative group t^Γ. Note that $\boldsymbol{k}((t^\Gamma))$ is an immediate extension of $\boldsymbol{k}(t^\Gamma)$. Suppose now that we have both a lifting $i : \boldsymbol{k} \to K$ of the residue field of (K, v, Γ) and a cross-section $s : \Gamma \to K^\times$ of v. Jointly i and s yield a unique valued field embedding from $\boldsymbol{k}(t^\Gamma)$ into (K, v, Γ) that extends i and maps t^γ to $s\gamma$ for each $\gamma \in \Gamma$. (Exercise.) It is clear that (K, v, Γ) is an immediate extension of the image of this embedding. Making now the additional assumption that (K, v, Γ) is maximal valued and $\operatorname{char}(\boldsymbol{k}) = 0$, we conclude from Corollary 4.28 that (K, v, Γ) is isomorphic to the Hahn field $\boldsymbol{k}((t^\Gamma))$ under an isomorphism that maps ia to a for each $a \in \boldsymbol{k}$ and $s\gamma$ to t^γ for each $\gamma \in \Gamma$.

4.30. Lemma. *Suppose (K, v, Γ) is henselian, $\operatorname{char}(\boldsymbol{k}) = 0$ and the abelian groups $\boldsymbol{k}^\times$ and Γ are divisible. Then $K^\times$ is divisible, and the valuation v has a cross-section.*

Proof. Let $a \in K^\times$, and $n > 0$; we shall find $b \in K$ so that $a = b^n$. First take $d \in K$ with $n \cdot vd = va$, so $a = ud^n$ with $vu = 0$. Now the residue class $\bar{u}$ is an nth power in $\boldsymbol{k}^\times$, so $u = c^n$ with $c \in K$ by an earlier exercise. Hence $a = (cd)^n$.

The second statement follows from the first: From the divisibility of $K^\times$ it follows that $U(\mathcal{O})$ is divisible. Thus the exact sequence

$$1 \to U(\mathcal{O}) \hookrightarrow K^\times \xrightarrow{v} \Gamma \to 0$$

splits, so v has a cross-section. □

The first two assumptions in this lemma imply also that there is a lifting of the residue field of (K, v, Γ), by Theorem 2.9. Therefore:

4.31. Corollary. *Suppose (K, v, Γ) is maximal valued, $\operatorname{char}(\boldsymbol{k}) = 0$ and the abelian groups $\boldsymbol{k}^\times$ and Γ are divisible. Then (K, v, Γ) is isomorphic to the Hahn field $\boldsymbol{k}((t^\Gamma))$ via an isomorphism that induces the identity on $\boldsymbol{k}$ and on Γ.*

4.32. Corollary. *Suppose (K, v, Γ) is maximal valued, $\boldsymbol{k}$ is algebraically closed, $\operatorname{char}(\boldsymbol{k}) = 0$ and Γ is divisible. Then (K, v, Γ) is isomorphic to the Hahn field $\boldsymbol{k}((t^\Gamma))$ via an isomorphism that induces the identity on $\boldsymbol{k}$ and on Γ.*

The exercise below gives another case where a maximal valued field is isomorphic to a Hahn field.

Exercise. Show that if Γ is free as an abelian group, then v has a cross-section. Show: if (K, v, Γ) is maximal valued, $\operatorname{char}(\boldsymbol{k}) = 0$, and Γ is free as an abelian group, then (K, v, Γ) is isomorphic to the Hahn field $\boldsymbol{k}((t^\Gamma))$ via an isomorphism that induces the identity on $\boldsymbol{k}$ and on Γ.

5 The Theorem of Ax–Kochen and Ershov

We prove here the original AKE-theorem, where AKE abbreviates *Ax–Kochen and Ershov* (really two groups who proved the theorem independently, one from the USA: Ax and Kochen, the other from Russia: Ershov). In later sections we shall prove more refined versions.

5.1. AKE-Theorem. *Let (K, A) and (K', A') be two henselian valued fields with residue fields $\boldsymbol{k}$ and $\boldsymbol{k}'$, and value groups Γ and Γ' (viewed as ordered abelian groups). Suppose that char$(\boldsymbol{k}) = 0$. Then*

$$(K, A) \equiv (K', A') \iff \boldsymbol{k} \equiv \boldsymbol{k}' \text{ and } \Gamma \equiv \Gamma'.$$

The forward direction $\Rightarrow$ should be clear (and does not need the henselian or residue characteristic zero assumption). It will be convenient to prove first a variant of theorem where we have also a lifting of the residue field and a cross-section of the valuation as part of the structure. So we begin with some additional facts on cross-sections.

5.1 Existence of cross-sections in elementary extensions

In this subsection we fix a valued field (K, v, Γ). We shall write *$\times$-section* to abbreviate the word *cross-section*.

5.2 Definition. A *partial $\times$-section* of v is a group morphism $s : \Delta \longrightarrow K^\times$ from a subgroup Δ of Γ back into $K^\times$ such that $v(s\delta) = \delta$ for all $\delta \in \Delta$.

A subgroup Δ of Γ is said to be *pure in* Γ if Γ/Δ is torsion free, that is, whenever $n\gamma \in \Delta$ with $n > 0$ and $\gamma \in \Gamma$, then $\gamma \in \Delta$.

5.3. Lemma. *Let $s : \Delta \longrightarrow K^\times$ be a partial $\times$-section of v such that Δ is pure in Γ. Then there is an elementary extension (K_1, v_1, Γ_1) of (K, v, Γ) with a partial $\times$-section $s_1 : \Gamma \longrightarrow K_1^\times$ of v_1.*

Proof. Let Δ' be a subgroup of Γ that contains Δ such that Δ'/Δ is finitely generated as an abelian group. Since Δ'/Δ is torsion-free, it is free as abelian group, so we can take nonzero $\gamma_1, \dots, \gamma_k \in \Delta'$ such that

$$\Delta' = \Delta \oplus \mathbb{Z}\gamma_1 \oplus \cdots \oplus \mathbb{Z}\gamma_k \quad \text{(internal direct sum of subgroups of } \Gamma).$$

Take $a_1, \dots, a_k \in K^\times$ such that $v(a_1) = \gamma_1, \dots, v(a_k) = \gamma_k$. Extend s to a group morphism $s' : \Delta' \longrightarrow K^\times$ by $s'(\gamma_i) = a_i$, $i = 1, \dots, k$. It is easy to check that s' is a partial $\times$-section of v.

Since Δ' was arbitray, a compactness argument gives an elementary extension (K_1, v_1, Γ_1) of (K, v, Γ) with a partial $\times$-section $s_1 : \Gamma \longrightarrow K_1^\times$ of v_1. $\square$

Since $\Gamma \preccurlyeq \Gamma_1$ as ordered abelian groups, Γ is pure in Γ_1, so the purity assumption on s is inherited by s_1. Thus we can *iterate* the lemma:

5.4. Proposition. *Let $s : \Delta \longrightarrow K^\times$ be a partial $\times$-section of v such that Δ is pure in Γ. Then there is an elementary extension (K', v', Γ') of (K, v, Γ) with a $\times$-section $s' : \Gamma' \longrightarrow K'^\times$ of v' that extends s.*

Proof. Use the previous lemma to build an elementary chain

$$(K, v, \Gamma) = (K_0, v_0, \Gamma_0) \preccurlyeq (K_1, v_1, \Gamma_1) \preccurlyeq (K_2, v_2, \Gamma_2) \preccurlyeq \dots$$

with a partial $\times$-section $s_n : \Delta_n \longrightarrow K_n^\times$ of v_n for each n, such that $\Delta_0 = \Delta$, $\Delta_{n+1} = \Gamma_n$ and s_{n+1} extends s_n, for each n. Then $(K', v', \Gamma') = \bigcup_n (K_n, v_n, \Gamma_n)$ works with $s' = \bigcup_n s_n$ as $\times$-section. □

By taking $\Delta = \{0\}$ in this proposition we get:

5.5. Corollary. *(K, v, Γ) has an elementary extension with a cross-section.*

Exercise. Suppose K is algebraically closed and $s : \Delta \to K^\times$ is a partial $\times$-section of v. Show that s extends to a $\times$-section of v.

5.2 Extending the value group

We need a few more basic results on how the value group can change when we extend a valued field. Let (K, v, Γ) be a valued field, and let

$$\Gamma^{\mathrm{d}} = \{\gamma/n : \gamma \in \Gamma, n > 0\}$$

be the divisible hull of Γ.

5.6. Lemma. *Let p be a prime number, and x an element in a field extension of K such that $x^p = a \in K^\times$ but $va \notin p\Gamma$. Then $X^p - a$ is the minimum polynomial of x over K, and v extends uniquely to a valuation $w : K(x)^\times \to \Delta$ with $\Delta \subseteq \Gamma^d$ (as ordered groups). Moreover, $\boldsymbol{k}_w = \boldsymbol{k}_v$, and $[\Delta : \Gamma] = p$, with*

$$\Delta = \bigcup_{i=0}^{p-1} \Gamma + iw(x) \qquad (\textit{disjoint union}).$$

Proof. Let $w : K(x)^\times \to \Delta$ with $\Delta \subseteq \Gamma^d$ be a valuation extending v. (By earlier results we know that there is such an extension.) Since $va \notin p\Gamma$, the elements

$$w(x^0) = 0,\ w(x^1) = \frac{va}{p},\ \dots,\ w(x^{p-1}) = \frac{(p-1)va}{p}$$

of Δ are in distinct cosets of Γ, so $1, x, \dots, x^{p-1}$ are K-linearly independent, and thus $X^p - a$ is the minimum polynomial of x over K. Also, for an arbitrary nonzero element $b = b_0 + b_1 x + \cdots + b_{p-1}x^{p-1}$ of $K(x)$ ($b_0, \dots, b_{p-1} \in K$, not all zero), we have

$$w(b) = \min\{v(b_i) + \frac{iva}{p} : 0 \le i \le p-1\},$$

showing the uniqueness of w. This also proves the claims made by the lemma about Δ. Since $p = [K(x) : K] \ge [\Delta : \Gamma] \cdot [\boldsymbol{k}_w : \boldsymbol{k}_v]$, this yields $[\boldsymbol{k}_w : \boldsymbol{k}_v] = 1$, that is, $\boldsymbol{k}_w = \boldsymbol{k}_v$. □

5.7. Lemma. *Let (K', v', Γ') be a valued field extension of (K, v, Γ), let $x \in K'$, and put $v'(x - K) := \{v'(x - a) : a \in K\}$. If $v'(x - K)$ has no largest element, then $v'(x - K) \subseteq \Gamma$. If $v'(x - K)$ has a largest element $v'(x - a)$, $a \in K$, then $v'(x - K) \subseteq \Gamma \cup \{v'(x - a)\}$.*

Proof. For $b, c \in K$ we have: $v'(x-b) < v'(x-c) \implies v'(x-b) = v(b-c)$. □

5.8. Corollary. *Let (K, v, Γ) be algebraically maximal and have the valued field extension (K', v', Γ'), and let $x \in K' \setminus K$. Then one of the following holds:*

1. *x is a pseudolimit of a pc-sequence in K of transcendental type over K;*
2. *there exists $a \in K$ such that $v'(x - a) \notin \Gamma$;*
3. *there exist $a, b \in K$, $b \neq 0$, such that $v'(x - a) = vb$ and the residue class of $(x - a)/b$ does not lie in $\boldsymbol{k}$.*

Proof. Suppose $v'(x - K)$ has no largest element. As at the end of the proof of Lemma 4.2, this yields a pc-sequence in K that pseudoconverges to x but has no pseudolimit in K. By the algebraic maximality of (K, v, Γ) this pc-sequence must be of transcendental type over K.

Suppose next that $v'(x - K)$ has a largest element $v'(x - a)$, $a \in K$, and that $v'(x - a) \in \Gamma$. Then $v'(x - a) = vb$ with $b \in K$, $b \neq 0$. If the residue class of $(x - a)/b$ were in $\boldsymbol{k}$, then $(x - a)/b = u + \epsilon$ with $u \in K$, $vu = 0$, and $v'\epsilon > 0$, so $v'(x - (a + bu)) > vb = v'(x - a)$, a contradiction. Thus the residue class of $(x - a)/b$ cannot lie in $\boldsymbol{k}$. □

5.9. Corollary. *Let (K', v', Γ') be a valued field extension of (K, v, Γ), and let $x \in K'$, $x \notin K$. If $\Gamma = v(K^\times)$ is countable, so is $v'(K(x)^\times)$.*

Proof. By passing to an algebraic closure of K' and extending the valuation v' to this algebraic closure we can assume that K' is algebraically closed. Replacing K by its algebraic closure inside K' we further reduce to the case that K is algebraically closed. Suppose first that $v'(x - K) \subseteq \Gamma$. Then, given any non-zero element $f(x) \in K[x]$ we have a factorization $f(x) = c(x - a_1) \cdots (x - a_m)$ with $c, a_1, \ldots, a_m \in K$, $c \neq 0$, so

$$v'(f(x)) = vc + v'(x - a_1) + \cdots + v'(x - a_m) \in \Gamma,$$

hence $v'(K(x)^\times) \subseteq \Gamma$. Next, suppose that $a \in K$ is such that $v'(x - a) \notin \Gamma$. Then $v'(x-K) \subseteq \Gamma \cup \{v'(x-a)\}$ by Lemma 5.7, and thus by the same argument $v'(K(x)^\times) \subseteq \Gamma + \mathbb{Z} \cdot v'(x - a)$. □

5.3 AKE-theorem with lifting and cross-section

Consider 3-sorted structures

$$\mathcal{K} = (K, \Gamma, \boldsymbol{k}; v, s, \pi, i)$$

where K and $\boldsymbol{k}$ are fields, Γ is an ordered abelian group, $v : K^\times \to \Gamma$ is a valuation with $\times$-section s, and $\pi : \mathcal{O}_v \to \boldsymbol{k}$ and $i : \boldsymbol{k} \to \mathcal{O}_v$ are ring morphisms such that $\pi(ir) = r$ for all $r \in \boldsymbol{k}$.

Note that then π is surjective, so π has kernel $\mathfrak{m}_v$, and thus we have a field isomorphism $\boldsymbol{k} \cong \boldsymbol{k}_v$ of $\boldsymbol{k}$ onto the residue field such that the diagram

.....

commutes. We call K the underlying field of $\mathcal{K}$, Γ its value group, and $\boldsymbol{k}$ its residue field (even though the latter is only isomorphic to the residue field $\boldsymbol{k}_v$ of $\mathcal{O}_v$).

Such a structure $\mathcal{K}$ will be called a *cl-valued field*, with "c" recalling the cross-section s and "l" the lifting i.

5.10. Remark. *Each henselian valued field (K, A) of equicharacteristic 0 has an elementary extension (K', A') that can be expanded to a cl-valued field*

$$(K', \Gamma', \boldsymbol{k}'; v', s', \pi', i')$$

where $v' := v_{A'} : K'^\times \to \Gamma' := \Gamma_{A'}$ and $\pi' : A' \to \boldsymbol{k}' := \boldsymbol{k}_{A'}$ is the residue map.

This follows from our lifting theorem for henselian local rings with residue field of characteristic 0, and Corollary 5.5.

In the rest of this section $\mathcal{K}$ and $\mathcal{K}'$ are cl-valued fields,

$$\mathcal{K} = (K, \Gamma, \boldsymbol{k}; v, s, \pi, i), \text{ and } \mathcal{K}' = (K', \Gamma', \boldsymbol{k}'; v', s', \pi', i').$$

An *embedding* $\mathcal{K} \to \mathcal{K}'$ is a triple $(f, f_{\mathrm{val}}, f_{\mathrm{res}})$ consisting of a field embedding $f : K \to K'$, an ordered group embedding $f_{\mathrm{val}} : \Gamma \to \Gamma'$ and a field embedding $f_{\mathrm{res}} : \boldsymbol{k} \to \boldsymbol{k}'$ such that

$$f_{\mathrm{val}}(va) = v'(fa) \text{ for } a \in K^\times, \quad f(s\gamma) = s'(f_{\mathrm{val}}\gamma) \text{ for } \gamma \in \Gamma,$$
$$f_{\mathrm{res}}(\pi a) = \pi'(fa) \text{ for } a \in \mathcal{O}_v, \quad f(ir) = i'(f_{\mathrm{res}}r) \text{ for } r \in \boldsymbol{k}.$$

If $K \subseteq K'$, $\Gamma \subseteq \Gamma'$, and $\boldsymbol{k} \subseteq \boldsymbol{k}'$ (as sets), and the corresponding inclusion maps $f : K \to K'$, $f_{\mathrm{val}} : \Gamma \to \Gamma$, and $f_{\mathrm{res}} : \boldsymbol{k} \to \boldsymbol{k}'$ yield an embedding $(f, f_{\mathrm{val}}, f_{\mathrm{res}}) : \mathcal{K} \to \mathcal{K}'$, then we call $\mathcal{K}$ an *cl-valued subfield* of $\mathcal{K}'$; notation: $\mathcal{K} \subseteq \mathcal{K}'$.

Consider an embedding $(f, f_{\mathrm{val}}, f_{\mathrm{res}}) : \mathcal{K} \to \mathcal{K}'$. Then f_{val} and f_{res} are completely determined by f. If f is a bijection, then f_{val} and f_{res} are bijections, and we call $(f, f_{\mathrm{val}}, f_{\mathrm{res}})$ an *isomorphism from $\mathcal{K}$ onto $\mathcal{K}'$*; note that then $(f^{-1}, f_{\mathrm{val}}^{-1}, f_{\mathrm{res}}^{-1})$ is an isomorphism from $\mathcal{K}'$ onto $\mathcal{K}$.

In view of Remark 5.10 the AKE-theorem 5.1 is a consequence of the following stronger result.

5.11. Theorem. *Suppose $\mathcal{K}$ and $\mathcal{K}'$ are henselian of equicharacteristic 0. Then*

$$\mathcal{K} \equiv \mathcal{K}' \iff \boldsymbol{k} \equiv \boldsymbol{k}' \text{ and } \Gamma \equiv \Gamma'.$$

Proof. Since the forward direction $\Rightarrow$ is clear, we assume below that $\boldsymbol{k} \equiv \boldsymbol{k}'$ and $\Gamma \equiv \Gamma'$, and our task is to derive $\mathcal{K} \equiv \mathcal{K}'$. The case that $\Gamma = \{0\}$ is trivial, so we assume from now on that $\Gamma \neq \{0\}$ and thus $\Gamma' \neq \{0\}$.

More drastically, we shall assume the *Continuum Hypothesis* CH, in order to make our job a little easier. (Theorem 5.11 belongs to a class of mathematical statements with the property that any proof of a statement in that class from ZFC + CH can be converted in a, possibly longer, proof of the same statement from ZFC alone. See for example an exercise in the chapter on set theory in Shoenfield's *Mathematical Logic*.)

After replacing $\mathcal{K}$ and $\mathcal{K}'$ by elementarily equivalent cl-valued fields, we may (and shall) assume that $\mathcal{K}$ and $\mathcal{K}'$ are saturated of cardinality $\aleph_1$. (This is exactly where CH gets used.) In particular, Γ and Γ' are saturated of cardinality $\aleph_1$, so we have an isomorphism $f_{\mathrm{val}} : \Gamma \cong \Gamma'$ of ordered abelian groups; likewise, $\boldsymbol{k}$ and $\boldsymbol{k}'$ are saturated of cardinality $\aleph_1$, so we have an isomorphism $f_{\mathrm{res}} : \boldsymbol{k} \cong \boldsymbol{k}'$ of fields.

To obtain Theorem 5.11 it suffices to establish:

Claim. There is a field isomorphism $f : K \cong K'$ which together with f_{val}, and f_{res} yields an isomorphism $(f, f_{\mathrm{val}}, f_{\mathrm{res}}) : \mathcal{K} \cong \mathcal{K}'$.

We shall obtain such f by a back-and-forth construction. A *good subfield of* K is by definition a subfield E of K such that $i\boldsymbol{k} \subseteq E$, $s(vE^\times) \subseteq E$, and $vE^\times$ is countable. (Note that then E is the underlying field of a cl-valued subfield of $\mathcal{K}$.) Likewise, we define the notion *good subfield of* K'. A *good map* is an isomorphism $e : E \cong E'$ between good subfields E and E' of K and K', such that $e(E \cap \mathcal{O}_v) = E' \cap \mathcal{O}_{v'}$ and

$$f_{\mathrm{val}}(va) = v'(ea) \text{ for } a \in E^\times, \quad e(s\gamma) = s'(f_{\mathrm{val}}\gamma) \text{ for } \gamma \in vE^\times,$$
$$f_{\mathrm{res}}(\pi a) = \pi'(ea) \text{ for } a \in E \cap \mathcal{O}_v, \quad e(ir) = i'(f_{\mathrm{res}}r) \text{ for } r \in \boldsymbol{k}.$$

Note that $i\boldsymbol{k}$ and $i'\boldsymbol{k}'$ are good subfields of K and K' and that

$$ir \mapsto i'(f_{\mathrm{res}}r) \ : \ i\boldsymbol{k} \to i'\boldsymbol{k}' \quad (r \in \boldsymbol{k})$$

is a good map. Thus the claim above is a consequence of:

Back-and-Forth. The set of good maps has the back-and-forth property.

To prove *Back-and-Forth*, consider a good map $e : E \cong E'$. We view E and E' as valued subfields of (K, v, Γ) and (K', v', Γ') and we note that $e : E \to E'$ is a valued field isomorphism. Before addressing *Back-and-Forth* we indicate two basic ways in which e can be extended.

(1) *Adjunction of an element of* Γ *that has prime-torsion modulo* $vE^\times$. Let $\delta \in \Gamma$ be such that $\delta \notin vE^\times$ but $p\delta \in vE^\times$ where p is a prime number. Take $x = s\delta$, so $x^p = s(p\delta) \in E^\times$. Then by Lemma 5.6,

$$v(E(x)^\times) = vE^\times + \mathbb{Z}\delta = \bigcup_{i=0}^{p-1} vE^\times + i\delta \quad \text{(disjoint union)}.$$

Since $s(vE^\times + \mathbb{Z}\delta) = s(vE^\times)\cdot x^{\mathbb{Z}} \subseteq E(x)$, it follows that $E(x)$ is a good subfield of K. Put $x' := s'(f_{\mathrm{val}}\delta) \in K'$. Then $E'(x')$ is likewise a good subfield of K', and Lemma 5.6 shows we have a good map $E(x) \to E'(x')$ that extends e and maps x to x'.

(2) *Adjunction of an element of* Γ *that has no torsion modulo* $vE^\times$. Let $\gamma \in \Gamma$ be such that $n\gamma \notin vE^\times$ for all $n > 0$. Take $x = s\gamma$. By an earlier lemma x is transcendental over E and $v(E(x)^\times) = vE^\times \oplus \mathbb{Z}\gamma$. Since

$$s(vE^\times \oplus \mathbb{Z}\gamma) = s(vE^\times)\cdot x^{\mathbb{Z}} \subseteq E(x),$$

$E(x)$ is a good subfield of K. Put $x' := s'(f_{\mathrm{val}}\gamma) \in K'$. Then $E'(x')$ is likewise a good subfield of K', and the same earlier lemma shows we have a good map $E(x) \to E'(x')$ that extends e and maps x to x'.

Let Δ be any countable subgroup of Γ that contains $vE^\times$. We now show how to extend our good map e to a good map whose domain has value group Δ. Clearly Δ is the union $\bigcup_{i=0}^{\infty} \Delta_i$ of an increasing sequence

$$vE^\times = \Delta_0 \subseteq \Delta_1 \subseteq \Delta_2 \subseteq \dots$$

of subgroups Δ_i of Δ such that for each $i \in \mathbb{N}$, either $\Delta_{i+1} = \Delta_i$, or $\Delta_{i+1} = \Delta_i + \mathbb{Z}\delta_i$ with $\delta_i \in \Delta \setminus \Delta_i$ but $p\delta_i \in \Delta_i$ for some prime number p, or $\Delta_{i+1} = \Delta_i + \mathbb{Z}\delta_i$ and $n\delta_i \notin \Delta_i$ for all $n > 0$. Then by repeated application of (1) and (2) and taking a union we see that $E_\Delta := E(s\delta_i : i = 0, 1, 2, \dots)$ is a good subfield of K with $vE_\Delta^\times = \Delta$, and that e extends (uniquely) to a good map with domain E_Δ.

In addition to (1) and (2), Lemma 4.29 provides a third way to extend good maps. We now combine these three ways of extending e to establish *Back-and-Forth*. Consider an element $x \in K$. We wish to find a good map extending e that contains x in its domain. By Corollary 5.9 the group $v(E(x)^\times)$ is countable, so by the construction above we can extend e to a good map e_1 with domain E_1 such that $v(E_1^\times) = v(E(x)^\times)$. In the same way we extend e_1 to a good map e_2 with domain E_2 such that $v(E_2^\times) = v(E_1(x)^\times)$. By iterating this construction and taking a union (and renaming this union as E) we reduce to the case that $E(x)$ is an immediate extension of E. The valued field $E(x)$ has an immediate maximal extension, which by Lemma 4.29 can be taken inside (K, v, Γ); let $E_\bullet$ be the underlying field of such an a immediate maximal extension of $E(x)$ inside (K, v, Γ). Since $E_\bullet$ as valued field is also an immediate maximal extension of E, we can use Lemma 4.29 to extend e to a valued field isomorphism $e_\bullet$ from $E_\bullet$ onto a valued difference field $E'_\bullet$ inside (K', v', Γ'). Then $e_\bullet$ is a good map with x in its domain.

This takes care of the *Forth* part of *Back-and-Forth*. The *Back* part is done likewise by interchanging the role of E and E'. □

Note that Theorem 1.1 (announced in the Introduction) is a special case of Theorem 5.1, since $\boldsymbol{k}[[t]]$ is the valuation ring of the Laurent series field $\boldsymbol{k}((t))$ (where $\boldsymbol{k}$ is a field).

Elementary classifications like Theorem 5.11 often imply a seemingly stronger result to the effect that each sentence in a certain language is equivalent in a suitable theory to a sentence of a special form. We now turn our attention to this aspect. It involves the following elementary fact on boolean algebras, which is useful in a wide variety of model-theoretic situations.

5.12. Lemma. *Let B be a boolean algebra and $S(B)$ its Stone space of ultrafilters. Let Ψ be a subset of B and suppose the map $F \mapsto F \cap \Psi : S(B) \to \mathcal{P}(\Psi)$ is injective. Then Ψ generates B: every element of B is a boolean combination of elements of Ψ.*

Proof. Let B_Ψ be the boolean subalgebra of B generated by Ψ. The inclusion $B_\Psi \hookrightarrow B$ induces the *surjective* map $F \mapsto F \cap B_\Psi : S(B) \twoheadrightarrow S(B_\Psi)$. This map is also *injective*: if $F_1, F_2 \in S(B)$ and $F_1 \cap B_\Psi = F_2 \cap B_\Psi$, then $F_1 \cap \Psi = F_2 \cap \Psi$, hence $F_1 = F_2$ by the hypothesis of the lemma. The bijectivity of $F \mapsto F \cap B_\Psi : S(B) \to S(B_\Psi)$ yields $B = B_\Psi$ by the Stone representation theorem. □

Let L be the 3-sorted language of cl-valued fields with 1-sorted sublanguages L_{val} for value groups and L_{res} for residue fields. Let T be the L-theory of henselian cl-valued fields with residue field of characteristic 0. Then:

5.13. Corollary. *For each L-sentence σ there are sentences $\sigma^1_{val}, \dots, \sigma^k_{val}$ in the language L_{val} and sentences $\sigma^1_{res}, \dots, \sigma^k_{res}$ in L_{res} such that*

$$T \vdash \sigma \iff (\sigma^1_{val} \wedge \sigma^1_{res}) \vee \cdots \vee (\sigma^k_{val} \wedge \sigma^k_{res}).$$

Proof. Let B be the boolean algebra of L-sentences modulo T-equivalence. Let $\Psi \subseteq B$ be the set of T-equivalence classes of sentences of the form $\sigma_{\mathrm{val}} \wedge \sigma_{\mathrm{res}}$ where σ_{val} is an L_{val}-sentence and σ_{res} is an L_{res}-sentence. Using the familiar bijective correspondence between ultrafilters of B and complete L-theories extending T, Theorem 5.11 shows that the map $F \mapsto F \cap \Psi : S(B) \to \mathcal{P}(\Psi)$ from the Stone space $S(B)$ of B into the power set of Ψ is injective. Thus by Lemma 5.12 each element of B is a boolean combination of elements of Ψ. We leave it as an exercise to show that this yields the desired result. □

The equivalence displayed in Corollary 5.13 holds in all henselian cl-valued fields of equicharacteristic 0, and thus also in all henselian cl-valued fields with residue characteristic $p > N$ where $N \in \mathbb{N}$ depends only on σ.

When we fix the value group to be $\mathbb{Z}$, Corollary 5.13 becomes:

5.14. Corollary. *For each L-sentence σ there is a sentence σ_{res} in L_{res} such that for all henselian $\mathcal{K}$ of equicharacteristic 0 with value group $\mathbb{Z}$,*

$$\mathcal{K} \models \sigma \iff \boldsymbol{k} \models \sigma_{res}.$$

It is convenient to state some of the above also for (one-sorted) valued fields (K, A) without a cross-section or lifting as part of the structure.

5.15. Corollary. *Let σ be a sentence in the language of rings with an extra unary relation symbol. Then there are sentences $\sigma^1_{val}, \dots, \sigma^k_{val}$ in L_{val} and sentences $\sigma^1_{res}, \dots, \sigma^k_{res}$ in L_{res} such that for all henselian valued fields (K, A) of equicharacteristic 0:*

$$(K, A) \models \sigma \iff \Gamma_A \models \sigma^i_{val} \text{ and } \boldsymbol{k}_A \models \sigma^i_{res}, \text{ for some } i \in \{1, \dots, k\}.$$

It should be clear how this follows from Corollary 5.13 in view of Remark 5.10. Note also that the equivalence holds for all henselian valued fields with residue characteristic $p > N$ where N depends only on σ. Thus we have established Theorem 1.2 and the Ax-Kochen Principle 2.20.

There remain some claims in the Introduction—for example, $\widetilde{\mathbb{Q}}[[t]] \preceq \mathbb{C}[[t]]$—which belong to the circle of AKE-results, but where some extra work is needed. We also want to have equivalences like the above not just for sentences, but also for formulas (with applications to the structure of definable sets). These issues will be addressed in a later version of the notes.

6 Unramified Mixed Characteristic

We now aim for results in the mixed characteristic case that are analogous to the "equicharacteristic 0" theorems in the previous section. A key difference is that in the mixed characteristic case we don't have a lifting of the residue field. Fortunately, we do have a perfect substitute, namely the Teichmüller map.

After introducing the Teichmüller map we are naturally led to Witt vectors which allow us to construct, for each perfect field $\boldsymbol{k}$ of characteristic $p > 0$, a discrete valuation ring $W[\boldsymbol{k}]$ with residue field $\boldsymbol{k}$. This construction is functorial and has various other good properties. We shall determine the elementary theory of the ring $W[\boldsymbol{k}]$ in terms of the elementary theory of the field $\boldsymbol{k}$; this covers the elementary theories of the p-adic fields $\mathbb{Q}_p$ as a special case.

Throughout we fix a prime number p. Recall that $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is the field of p elements. For integers a and $N \geq 1$ we let $a \bmod N$ be the image of a in the residue ring $\mathbb{Z}/N\mathbb{Z}$.

6.1 The Teichmüller Map

As we have seen, we cannot lift the residue fields of (henselian) local rings like $\mathbb{Z}/p^2\mathbb{Z}$ and $\mathbb{Z}_p$ for the simple reason that these rings do not contain any subfield. Fortunately, it turns out that there is a canonical system of representatives for the residue field in these rings, but it only preserves the multiplicative structure of the residue field, not its additive structure. For $\mathbb{Z}/p^2\mathbb{Z}$ it is the map

$$\tau : \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p^2\mathbb{Z}, \quad \tau(a \bmod p) = a^p \bmod p^2, \quad a \in \mathbb{Z}.$$

To see that such a map τ exists, use the fact that for all $a, b \in \mathbb{Z}$,

$$a \equiv b \mod p \implies a^p \equiv b^p \mod p^2.$$

Because also $a \equiv a^p \mod p$ for all $a \in \mathbb{Z}$, this map τ is a system of representatives for the residue field $\mathbb{F}_p$, in the sense that for each $x \in \mathbb{F}_p$ the image of τx in $\mathbb{F}_p$ is x. Note also that $\tau(xy) = \tau(x)\tau(y)$ for all $x, y \in \mathbb{F}_p$. For the ring $\mathbb{Z}/p^3\mathbb{Z}$, the canonical system of representatives for its residue field $\mathbb{F}_p$ is given by $a \bmod p \mapsto a^{p^2} \bmod p^3$, $(a \in \mathbb{Z})$. Below we extend these observations to complete local rings with perfect residue field of characteristic p.

A field $\boldsymbol{k}$ of characteristic p is said to be *perfect* if its *Frobenius endomorphism* $x \mapsto x^p$ is an automorphism. Given any local ring A with residue field $\boldsymbol{k}$ of characteristic p, one shows easily by induction on n that for all $x, y \in A$,

$$(*) \qquad x \equiv y \mod \mathfrak{m} \implies x^{p^n} \equiv y^{p^n} \mod \mathfrak{m}^{n+1}.$$

6.1. Theorem. *Let A be a complete local ring with maximal ideal $\mathfrak{m}$ and perfect residue field $\boldsymbol{k}$ of characteristic p. Then there is a unique map $\tau : \boldsymbol{k} \to A$ such that $\overline{\tau x} = x$ and $\tau(x^p) = (\tau x)^p$ for all $x \in \boldsymbol{k}$. This (Teichmüller) map τ has the following properties:*

(i) $\tau(\boldsymbol{k}) = \{a \in A : a$ *is a* p^n*th power in* A*, for each* $n\}$*;*

(ii) $\tau(xy) = \tau(x)\tau(y)$ *for all* $x, y \in \boldsymbol{k}$*,* $\tau(0) = 0$*,* $\tau(1) = 1$*, and* $\tau(\boldsymbol{k}^\times) \subseteq U(A)$*;*

(iii) if $p \cdot 1 = 0$ *in* A*, then* τ *is a ring embedding.*

Proof. Let $x \in \boldsymbol{k}$, and choose for each n an $a_n \in A$ such that

$$x = (\overline{a_n})^{p^n}, \qquad \text{(possible since } \boldsymbol{k} \text{ is perfect).}$$

Then $a_{n+1}^p \equiv a_n \mod \mathfrak{m}$, so $a_{n+1}^{p^{n+1}} \equiv a_n^{p^n} \mod \mathfrak{m}^{n+1}$ by (*) above. Hence the sequence $\{a_n^{p^n}\}$ converges in the $\mathfrak{m}$-adic norm to an element in A. This limit does not depend on the choice of $\{a_n\}$: if $\{b_n\}$ is another choice, then $a_n \equiv b_n \mod \mathfrak{m}$, so $a_n^{p^n} \equiv b_n^{p^n} \mod \mathfrak{m}^{n+1}$ by (*) above, and thus $\{a_n^{p^n}\}$ and $\{b_n^{p^n}\}$ have the same limit. We define τx to be this limit. It is easy to check that $\overline{\tau x} = x$ and $\tau(x^p) = (\tau x)^p$ for all $x \in \boldsymbol{k}$.

To show that these two identities uniquely determine τ, consider a map $\iota : \boldsymbol{k} \to A$ such that $\overline{\iota x} = x$ and $\iota(x^p) = (\iota x)^p$ for all $x \in \boldsymbol{k}$. For $x \in \boldsymbol{k}$ and $\{a_n\}$ as above, put $b_n := \iota\overline{a_n}$, so $\iota x = b_n^{p^n}$, so $x = (\overline{b_n})^{p^n}$ (for all n), and thus

$$\tau x = \lim b_n^{p^n} = \iota x.$$

To prove (i), each element of $\tau(\boldsymbol{k})$ is a p^nth power in A for each n, since each element of $\boldsymbol{k}$ is a p^nth power in $\boldsymbol{k}$ for each n. Conversely, let $a \in A$ be a p^nth power in A for each n. Choose for each n an $a_n \in A$ such that $a = a_n^{p^n}$. Then the construction of τ above shows that for $x := \bar{a}$ we have $\tau x = a$.

This construction also yields (ii), and (iii) follows from (i) by noting that if $p \cdot 1 = 0$ in A, then $(a + b)^{p^n} = a^{p^n} + b^{p^n}$ for all $a, b \in A$ and all n. □

The reader should verify that for $A = \mathbb{Z}/p^2\mathbb{Z}$ and $A = \mathbb{Z}/p^3\mathbb{Z}$ the Teichmüller map is the one given at the beginning of this subsection.

Exercise. With the same assumptions as in the Theorem, show that $\tau(\boldsymbol{k})$ is the unique set $S \subseteq A$ such that $s^p \in S$ for each $s \in S$, and S is mapped bijectively onto $\boldsymbol{k}$ by the residue class map. Show that for $A = \mathbb{Z}_p$ one has $\tau(\mathbb{F}_p) = \{x \in \mathbb{Z}_p : x^{p-1} = 1\} \cup \{0\}$.

A *local p-ring* is a complete local ring A such that $\mathfrak{m} = pA$ and $\boldsymbol{k}$ is perfect. If in addition $p^n \neq 0$ in A for all n, then we say that A is *strict*. (Here $p := p \cdot 1 \in A$, and below we often commit the same abuse of notation by letting p denote the element $p \cdot 1$ in a ring.)

6.2. Corollary. *Let A be a local p-ring. If $p^n \neq 0$ and $p^{n+1} = 0$ in A, then there is for every $a \in A$ a unique tuple $(x_0, \ldots, x_n) \in \boldsymbol{k}^{n+1}$ such that*

$$a = \sum_{i=0}^{n} \tau(x_i) p^n.$$

If A is strict, then there is for every $a \in A$ a unique sequence $\{x_n\} \in \boldsymbol{k}^{\mathbb{N}}$ such that

$$a = \sum_{n=0}^{\infty} \tau(x_n) p^n.$$

Let A be a strict local p-ring. For $a \in A$, call $\{x_n\}$ as above the *Teichmüller vector of a*. Note that the map

$$a \mapsto \text{Teichmüller vector of } a \ : \ A \to \boldsymbol{k}^{\mathbb{N}}$$

is a bijection. Given the Teichmüller vectors of $a, b \in A$, how do we obtain the Teichmüller vectors of $a + b$ and ab? It turns out that there is a good answer to this question, but things become more transparent if we change from Teichmüller vectors to Witt vectors: Let $a \in A$; then the unique sequence $\{x_n\} \in \boldsymbol{k}^{\mathbb{N}}$ such that $a = \sum_{n=0}^{\infty} \tau(x_n^{p^{-n}}) p^n$ is called the *Witt vector of a* (and then $\{x_n^{p^{-n}}\}$ is its Teichmüller vector). Note that if $\boldsymbol{k} = \mathbb{F}_p$, then there is no difference between the Teichmüller vector and the Witt vector of a.

We also want to show that, given any perfect field $\boldsymbol{k}$, there is exactly one strict local p-ring with residue field isomorphic to $\boldsymbol{k}$, up to isomorphism. To construct such a ring from $\boldsymbol{k}$ we shall take the set $\boldsymbol{k}^{\mathbb{N}}$ of Witt vectors over $\boldsymbol{k}$ and define a suitable addition and multiplication on it making it a strict local p-ring $W[\boldsymbol{k}]$. This is done in the next subsection.

Exercises. For any ring R, let $\mu(R) := \{x \in R : x^n = 1 \text{ for some } n > 0\}$ be the group of roots of unity in R, so $\mu(R)$ is a subgroup of $U(R)$. Let A be a strict local p-ring. Show that if $p \neq 2$, then τ maps $\mu(\boldsymbol{k})$ bijectively onto $\mu(A)$.

6.2 Witt vectors

Under the familiar bijection $\mathbb{F}_p^2 \longrightarrow \mathbb{Z}/p^2\mathbb{Z}$ given by

$$(i \bmod p,\ j \bmod p) \mapsto (i + jp) \bmod p^2, \qquad i, j \in \{0, \ldots, p-1\}$$

the addition and multiplication of $\mathbb{Z}/p^2\mathbb{Z}$ do not correspond to algebraically natural operations on $\mathbb{F}_p^2$. One motivation for Witt vectors is to find a bijection $\mathbb{F}_p^2 \longrightarrow \mathbb{Z}/p^2\mathbb{Z}$ that makes the addition map of the ring $\mathbb{Z}/p^2\mathbb{Z}$,

$$+ \ : \ \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z} \ \longrightarrow \ \mathbb{Z}/p^2\mathbb{Z}$$

correspond to an explicit polynomial map

$$\mathbb{F}_p^4 = \mathbb{F}_p^2 \times \mathbb{F}_p^2 \ \longrightarrow \ \mathbb{F}_p^2,$$

and likewise with multiplication on $\mathbb{Z}/p^2\mathbb{Z}$. Corollary 6.2 applied to $A = \mathbb{Z}/p^2\mathbb{Z}$ turns out to provide just the right (Witt) bijection $\mathbb{F}_p^2 \longrightarrow \mathbb{Z}/p^2\mathbb{Z}$:

$$(a \bmod p, \ a' \bmod p) \mapsto (a^p + pa') \bmod p^2, \qquad a, a' \in \mathbb{Z}.$$

To see which binary operations on $\mathbb{F}_p^2$ correspond under this bijection to addition and multiplication on $\mathbb{Z}/p^2\mathbb{Z}$ we note that for integers a, a', b, b',

$$\begin{aligned}(a^p + pa') + (b^p + pb') &= (a+b)^p + p\big(a' + b' - \sum_{i=1}^{p-1} c(p,i)a^i b^{p-i}\big),\\ (a^p + pa') \times (b^p + pb') &= (ab)^p + p\big(a^p b' + a' b^p + pa'b'\big),\end{aligned}$$

where $c(p,i)$ is the integer $\binom{p}{i}/p$ for $i = 1, \ldots, p-1$. Thus addition on $\mathbb{Z}/p^2\mathbb{Z}$ corresponds under the Witt bijection to the binary operation on $\mathbb{F}_p^2$ given by

$$\big((x_0, x_1), (y_0, y_1)\big) \mapsto \big(x_0 + y_0, \ x_1 + y_1 - \sum_{i=1}^{p-1} c(p,i) x_0^i y_0^{p-i}\big) \ : \ \mathbb{F}_p^2 \times \mathbb{F}_p^2 \to \mathbb{F}_p^2.$$

Likewise, multiplication on $\mathbb{Z}/p^2\mathbb{Z}$ corresponds under this bijection to

$$\big((x_0, x_1), (y_0, y_1)\big) \mapsto (x_0 y_0, \ x_0^p y_1 + x_1 y_0^p + p x_1 y_1) \ : \ \mathbb{F}_p^2 \times \mathbb{F}_p^2 \to \mathbb{F}_p^2.$$

(Of course, in $\mathbb{F}_p$ we have the identity $x_0^p y_1 + x_1 y_0^p + p x_1 y_1 = x_0 y_1 + x_1 y_0$, but we prefer to state it the way we did because later we shall replace $\mathbb{F}_p$ by an arbitrary ring.) So our bijection turns the ring $\mathbb{Z}/p^2\mathbb{Z}$ into an algebraic-geometric object living in $\mathbb{F}_p$ so to say.

Next we try to extend all this to $\mathbb{Z}/p^3\mathbb{Z}$, $\mathbb{Z}/p^4\mathbb{Z}$, and so on, all the way up to $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$. Applying Corollary 6.2 to $A = \mathbb{Z}/p^3\mathbb{Z}$ yields the bijection

$$(a \bmod p, \ a' \bmod p, \ a'' \bmod p) \mapsto (a^{p^2} + pa'^p + p^2 a'') \bmod p^3, \quad a, a', a'' \in \mathbb{Z}.$$

from $\mathbb{F}_p^3$ onto $\mathbb{Z}/p^3\mathbb{Z}$. Again, under this bijection the addition and multiplication of $\mathbb{Z}/p^3\mathbb{Z}$ correspond to binary operations on $\mathbb{F}_p^3$ given by easily specifiable polynomials over $\mathbb{F}_p$.

Just as crucial is that this Witt bijection between $\mathbb{F}_p^3$ and $\mathbb{Z}/p^3\mathbb{Z}$ is compatible with the earlier one between $\mathbb{F}_p^2$ and $\mathbb{Z}/p^2\mathbb{Z}$ in the sense that we have a commuting diagram

$$\begin{array}{ccc} \mathbb{F}_p^3 & \longrightarrow & \mathbb{F}_p^2 \\ \downarrow & & \downarrow \\ \mathbb{Z}/p^3\mathbb{Z} & \longrightarrow & \mathbb{Z}/p^2\mathbb{Z} \end{array}$$

where the vertical arrows are the Witt bijections, and horizontal arrows are given by

$$\begin{aligned} (x_0, x_1, x_2) &\mapsto (x_0, x_1) && \text{(top)}, \\ a \bmod p^3 &\mapsto a \bmod p^2,\ a \in \mathbb{Z} && \text{(bottom)}. \end{aligned}$$

It is also important that these constructions are *functorial*. Indeed, for any ring R we can define the ring $W_2[R]$ as follows: its underlying set is R^2, its addition is given by

$$\big((x_0, x_1), (y_0, y_1)\big) \mapsto \Big(x_0 + y_0,\ x_1 + y_1 - \sum_{i=1}^{p-1} c(p,i) x_0^i y_0^{p-i}\Big)\ :\ R^2 \times R^2 \to R^2$$

and its multiplication by

$$\big((x_0, x_1), (y_0, y_1)\big) \mapsto (x_0 y_0,\ x_0^p y_1 + x_1 y_0^p + p x_1 y_1)\ :\ R^2 \times R^2 \to R^2.$$

The zero element of $W_2[R]$ is $(0,0)$, and its multiplicative identity is $(1,0)$. One can view some of the above as providing an explicit isomorphism from the ring $W_2[\mathbb{F}_p]$ onto the ring $\mathbb{Z}/p^2\mathbb{Z}$. Likewise, we can define a ring $W_3[R]$, and so on, but at this point we may as well go the whole distance, and define $W[R]$.

The Witt Polynomials. Fix distinct indeterminates

$$X_0, X_1, X_2, \ldots, Y_0, Y_1, Y_2, \ldots.$$

The polynomials $W_0(X_0), W_1(X_0, X_1), \ldots, W_n(X_0, \ldots, X_n), \ldots$ are elements of the polynomial ring $\mathbb{Z}[X_0, X_1, X_2, \ldots]$ defined as follows:

$$\begin{aligned} W_0 &= X_0, \\ W_1 &= X_0^p + pX_1, \\ W_2 &= X_0^{p^2} + pX_1^p + p^2 X_2, \\ &\cdots\cdots \\ W_n &= X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^n X_n = \sum_{i=0}^{n} p^i X_i^{p^{n-i}}, \\ &\cdots\cdots \end{aligned}$$

Note that $W_{n+1}(X_0,\dots,X_{n+1}) = W_n(X_0^p,\dots,X_n^p) + p^{n+1}X_{n+1}$. Let R be a ring and consider the map $\theta : R^{\mathbb{N}} \longrightarrow R^{\mathbb{N}}$ defined by

$$\theta(x_0,x_1,x_2,\dots) = \big(W_0(x_0), W_1(x_0,x_1),\dots,W_n(x_0,\dots,x_n),\dots\big).$$

Exercise. Show that $\theta(1,0,0,0,\dots) = (1,1,1,1,\dots)$. Show also:

$$\theta(-1,0,0,0,\dots) = (-1,-1,-1,-1,\dots) \text{ if } p \text{ is odd,}$$
$$\theta(-1,-1,-1,-1,\dots) = (-1,-1,-1,-1,\dots) \text{ if } p = 2.$$

Below, $x = (x_0,x_1,x_2,\dots)$ and $y = (y_0,y_1,y_2,\dots)$ range over $R^{\mathbb{N}}$.

6.3. Lemma. *Suppose $p\cdot 1 \in U(R)$. Then θ is a bijection.*

Proof. We have $\theta(x) = y$ if and only if

$$x_0 = y_0,\ px_1 = y_1 - x_0^p,\ \dots,\ p^n x_n = y_n - x_0^{p^n} - \cdots - p^{n-1}x_{n-1}^p,\dots,$$

so there is exactly one such x for each y. □

Remark. By the same argument, θ is injective if $pa \neq 0$ for all $a \in R\setminus\{0\}$.

6.4. Lemma. *Suppose $pa \neq 0$ for all nonzero $a \in R$, let m be given, and let $x_0,x_1,\dots,x_n,y_0,y_1,\dots,y_n \in R$. Then the following are equivalent*

(1) $x_i \equiv y_i \mod p^m R$ *for* $i = 0,\dots,n$;

(2) $W_i(x_0,\dots,x_i) \equiv W_i(y_0,\dots,y_i) \mod p^{m+i}R$ *for* $i = 0,\dots,n$.

Proof. That (1) implies (2) is because for all $a,b \in R$ and $i \in \mathbb{N}$,

$$a \equiv b \mod p^m R \implies a^{p^i} \equiv a^{p^i} \mod p^{m+i}R.$$

The converse follows by induction on i, using the assumption on p. □

6.5. Lemma. *Let $A := \mathbb{Z}[X_0,X_1,\dots,Y_0,Y_1,\dots]$. There are polynomials $S_0,S_1,S_2\dots,P_0,P_1,P_2,\dots \in A$ such that for all n,*

$$W_n(X_0,\dots,X_n) + W_n(Y_0,\dots,Y_n) = W_n(S_0,\dots,S_n),$$
$$W_n(X_0,\dots,X_n) \times W_n(Y_0,\dots,Y_n) = W_n(P_0,\dots,P_n).$$

These conditions determine the sequences $\{S_n\}$ and $\{P_n\}$ uniquely, and for each n we have $S_n,P_n \in \mathbb{Z}[X_0,\dots,X_n,Y_0,\dots,Y_n]$.

Proof. We make $p \in A$ a unit by working in the larger domain

$$R := \{a/p^m : a \in A, m = 0,1,2\dots\} \subseteq \mathbb{Q}[X_0,X_1,\dots,Y_0,Y_1,\dots].$$

Then the bijectivity of the map θ of Lemma 6.3 shows that there are unique sequences $\{S_n\}$ and $\{P_n\}$ in R such that the identities above hold. Note that

$S_0 = X_0 + Y_0$. Assume for a certain $n > 0$ that $S_i \in \mathbb{Z}[X_0, \dots, X_i, Y_0, \dots, Y_i]$ for $i = 0, \dots, n-1$. We have

$$\begin{aligned} W_n(S_0, \dots, S_n) &= W_{n-1}(S_0^p, \dots, S_{n-1}^p) + p^n S_n \\ &= W_n(X_0, \dots, X_n) + W_n(Y_0, \dots, Y_n) \\ &= W_{n-1}(X_0^p, \dots, X_{n-1}^p) + W_{n-1}(Y_0^p, \dots, Y_{n-1}^p) + p^n(X_n + Y_n) \\ &= W_{n-1}\big(S_0(X_0^p, Y_0^p), \dots, S_{n-1}(X_0^p, \dots, X_{n-1}^p, Y_0^p, \dots, Y_{n-1}^p)\big) \\ &\quad + p^n(X_n + Y_n). \end{aligned}$$

Also, $S_i^p \equiv S_i(X_0^p, \dots, X_i^p, Y_0^p, \dots, Y_i^p) \mod pA$ for $i = 0, \dots, n-1$, hence by Lemma 6.4 the polynomial $W_{n-1}(S_0^p, \dots, S_{n-1}^p)$ is congruent modulo $p^n A$ to

$$W_{n-1}\big(S_0(X_0^p, Y_0^p), \dots, S_{n-1}(X_0^p, \dots, X_{n-1}^p, Y_0^p, \dots, Y_{n-1}^p)\big).$$

It follows that all coefficients of S_n are in $\mathbb{Z}$. The proof for the P_n is similar, starting with $P_0 = X_0 Y_0$. □

Of course, the letters S and P were chosen to remind the reader of *sum* and *product*. The polynomials S_0, S_1, P_0, P_1 are easy to write down:

$$\begin{aligned} S_0 &= X_0 + Y_0, \quad & S_1 &= X_1 + Y_1 - \sum_{i=1}^{p-1} c(p,i) X_0^i Y_0^{p-i}, \\ P_0 &= X_0 Y_0, & P_1 &= X_0^p Y_1 + X_1 Y_0^p + p X_1 Y_1. \end{aligned}$$

It is also easy to check that the constant terms of S_n and P_n are zero.

Let $W[R]$ be the set $R^{\mathbb{N}}$ equipped with the binary operations

$$+ \ : \ W[R] \times W[R] \to W[R], \quad \cdot \ : \ W[R] \times W[R] \to W[R],$$

defined as follows:

$$\begin{aligned} x + y &:= \big(S_0(x_0, y_0), S_1(x_0, x_1, y_0, y_1), \dots, S_n(x_0, \dots, x_n, y_0, \dots, y_n), \dots\big), \\ x \cdot y &:= \big(P_0(x_0, y_0), P_1(x_0, x_1, y_0, y_1), \dots, P_n(x_0, \dots, x_n, y_0, \dots, y_n), \dots\big). \end{aligned}$$

We also define the elements $\mathbf{0}$ and $\mathbf{1}$ of $W[R]$ by $\mathbf{0} = (0, 0, 0, \dots)$ and $\mathbf{1} = (1, 0, 0, \dots)$. For any ring morphism $\phi : R \to R'$ we define

$$W[\phi] : W[R] \to W[R'], \quad W[\phi](x) = (\phi x_0, \phi x_1, \phi x_2, \dots),$$

so $W[\phi]$ is a homomorphism for the addition and multiplication operations on $W[R]$ and $W[R']$, and $W[\phi](\mathbf{0}) = \mathbf{0}$, $W[\phi](\mathbf{1}) = \mathbf{1}$.

6.6. Corollary. *With these operations, $W[R]$ is a ring with zero element $\mathbf{0}$ and multiplicative identity $\mathbf{1}$.*

Proof. By the previous lemma, the map $\theta : W[R] \to R^{\mathbb{N}}$ is a homomorphism for addition and multiplication, where these operations are defined componentwise on $R^{\mathbb{N}}$. Note also that $\theta(\mathbf{0}) = \mathbf{0}$ and $\theta(\mathbf{1}) = (1, 1, 1, \dots)$ are the zero and multiplicative identity of the ring $R^{\mathbb{N}}$. Thus by the exercise preceding Lemma 6.3 we have a subring $\theta(W[R])$ of $R^{\mathbb{N}}$. In view of the remark following Lemma 6.3, we conclude that if $pa \neq 0$ for all nonzero $a \in R$, then $W[R]$ is a ring with zero element $\mathbf{0}$ and multiplicative identity $\mathbf{1}$. In particular, $W[A]$ is a ring with zero element $\mathbf{0}$ and multiplicative identity $\mathbf{1}$ for any polynomial ring $A = \mathbb{Z}[(X_i)_{i\in I}]$ in any family of distinct indeterminates $(X_i)_{i\in I}$. The general case now follows by taking a surjective ring morphism $\phi : A \to R$ where A is such a polynomial ring, and using the surjective map $W[\phi] : W[A] \to W[R]$. □

We call $W[R]$ the *ring of Witt vectors over* R. The map θ is a ring morphism of $W[R]$ into the product ring $R^{\mathbb{N}}$. Note also that if $\phi : R \to R'$ is a ring morphism, so is $W[\phi] : W[R] \to W[R']$. Below we consider $x = (x_0, x_1, \dots)$ and $y = (y_0, y_1, \dots)$ as elements of the ring $W[R]$ rather than of the product ring $R^{\mathbb{N}}$; we also put $x^{(i)} := W_i(x_0, \dots, x_i) \in R$ for $i \in \mathbb{N}$, and $x^{(i)} := 0 \in R$ for negative $i \in \mathbb{Z}$.

Exercise. Show that if p is odd, then the additive inverse of x in $W[R]$ is given by $-x = (-x_0, -x_1, -x_2, \dots)$.

We now define two further (unary) operations on $W[R]$:

$$\begin{aligned} \mathbf{V} &: W[R] \to W[R], \quad \mathbf{V}x = (0, x_0, x_1, x_2, \dots), \\ \mathbf{F} &: W[R] \to W[R], \quad \mathbf{F}x = (x_0^p, x_1^p, x_2^p, \dots). \end{aligned}$$

The map $\mathbf{V}$ is a *shift* operation ("Verschiebung" in German). The shift map $\mathbf{V}$ can also be viewed as a unary operation on the ring $R^{\mathbb{N}}$, and as such it is an endomorphism of the additive group of $R^{\mathbb{N}}$; this is also the case for $\mathbf{V}$ as an operation on $W[R]$, but this requires an argument:

6.7. Lemma. *The following identities hold:*

$$(\mathbf{V}x)^{(n)} = px^{(n-1)}, \quad \mathbf{V}(x + y) = \mathbf{V}x + \mathbf{V}y, \quad (\mathbf{V}^m x)^{(n)} = p^m x^{(n-m)}.$$

Proof. For $n > 0$ we have

$$W_n(0, x_0 \dots, x_{n-1}) = px_0^{p^{n-1}} + \cdots + p^n x_{n-1} = pW_{n-1}(x_0, \dots, x_{n-1}),$$

which gives the first identity. In other words, $\theta(\mathbf{V}x) = p\mathbf{V}(\theta x)$. Hence

$$\begin{aligned} \theta(\mathbf{V}(x + y)) &= p\mathbf{V}(\theta(x + y)) = p\mathbf{V}(\theta x + \theta y) \\ &= p\mathbf{V}(\theta x) + p\mathbf{V}(\theta y) = \theta(\mathbf{V}x) + \theta(\mathbf{V}y) \\ &= \theta(\mathbf{V}x + \mathbf{V}y). \end{aligned}$$

Thus $\mathbf{V}(x + y) = \mathbf{V}(x) + \mathbf{V}(y)$ if R is a polynomial ring over $\mathbb{Z}$. The validity of this identity in this special case implies its validity in general since each ring is isomorphic to a quotient of a polynomial ring over $\mathbb{Z}$. The third identity follows by induction on m from the first identity. □

Next we put $[a] := (a, 0, 0, \dots) \in W[R]$ for $a \in R$.

6.8. Lemma. *The following identities hold, where $a \in R$:*

(1) $[a]^{(n)} = a^{p^n}$;

(2) $x = \sum_{i=0}^{n-1} \mathbf{V}^i[x_i] + \mathbf{V}^n(x_n, x_{n+1}, \dots)$;

(3) $[a]x = (ax_0, a^p x_1, a^{p^2} x_2, \dots)$.

Proof. Identity (1) is immediate. It easily yields identity (2) for $n = 1$, initially in the case that R is a polynomial ring over $\mathbb{Z}$, and then for any R by the usual argument. Induction gives identity (2) for all n. Identity (3) follows likewise by checking that $([a]x)^{(n)} = W_n(ax_0, \dots, a^{p^n} x_n)$. □

Remark. The decomposition in (2) is clearly unique: if $x = \sum_{i=0}^{n-1} \mathbf{V}^i[y_i] + \mathbf{V}^n z$, then $x_i = y_i$ for all $i < n$.

6.9. Lemma. *Let $y = px$ and $z = \mathbf{V}(\mathbf{F}x)$. Then $y_n \equiv z_n \mod pR$.*

Proof. We have $y^{(n)} = px^{(n)} = p\big(\mathbf{F}(x)^{(n-1)} + p^n x_n\big)$ by the recursion for the Witt polynomials. Also $p(\mathbf{F}x)^{(n-1)} = (\mathbf{V}(\mathbf{F}x)^{(n)} = z^{(n)}$ by the first identity of Lemma 6.7, so $y^{(n)} \equiv z^{(n)} \mod p^{n+1}R$. This holds for all n, so by Lemma 6.4 we have $y_n \equiv z_n \mod pR$ for all n in case R is a polynomial ring over $\mathbb{Z}$, and thus for all R by the usual argument. □

By Lemma 6.3 the ring $W[R]$ is just a disguised version of the product ring $R^{\mathbb{N}}$ if R is a field of characteristic 0. The situation is much more interesting if R is a perfect field of characteristic p, and from this point on we are just going to consider this case. So in the remainder of this subsection $\boldsymbol{k}$ denotes a perfect field of characteristic p, and $x = (x_0, x_1, x_2, \dots)$, $y = (y_0, y_1, y_2, \dots) \in W[\boldsymbol{k}]$.

Note that then $\mathbf{F} = W[\Phi]$ where $\Phi : \boldsymbol{k} \to \boldsymbol{k}$ is the Frobenius automorphism. Thus $\mathbf{F}$ is an automorphism of the ring $W[\boldsymbol{k}]$. The map $\mathbf{V}$ is related to $\mathbf{F}$ by

$$\mathbf{F} \circ \mathbf{V} = \mathbf{V} \circ \mathbf{F} = p \cdot \mathrm{Id},$$

as a consequence of Lemma 6.9. In other words,

$$px = p(x_0, x_1, x_2, \dots) = (0, x_0^p, x_1^p, x_2^p, \dots),$$

and thus $p^2 x = (0, 0, x_0^{p^2}, x_1^{p^2}, \dots)$, and so on. Also

$$(*) \qquad \mathbf{V}^m x \cdot \mathbf{V}^n y = \mathbf{V}^{m+n}\big(\mathbf{F}^n(x)\mathbf{F}^m(y)\big).$$

To see this, note that upon setting $x = \mathbf{F}^m u$ and $y = \mathbf{F}^n z$ with $u, z \in W[\boldsymbol{k}]$, the identity becomes $p^m u \cdot p^n z = p^{m+n} uz$.

We define $v : W[\boldsymbol{k}] \to \mathbb{Z} \cup \{\infty\}$ by

$$v(\mathbf{0}) = \infty, \qquad vx = n \text{ if } x_n \neq 0 \text{ and } x_i = 0 \text{ for all } i < n.$$

6.10. Theorem. *$W[\boldsymbol{k}]$ is a complete DVR with normalized valuation v, fraction field of characteristic 0, and maximal ideal $pW[\boldsymbol{k}]$. The map $x \mapsto x_0 : W[\boldsymbol{k}] \to \boldsymbol{k}$ is a ring morphism with kernel $pW[\boldsymbol{k}]$, and thus induces an isomorphism of the residue field of $W[\boldsymbol{k}]$ with the field $\boldsymbol{k}$. Upon identifying $\boldsymbol{k}$ with the residue field via this isomorphism, the Teichmüller map $\boldsymbol{k} \to W[\boldsymbol{k}]$ is given by $a \mapsto [a]$, and for $x \in W[\boldsymbol{k}]$ we have*

$$x = \sum_{n=0}^{\infty} [x_n^{p^{-n}}]p^n.$$

Proof. Note that $vx \geq n$ iff $x = \mathbf{V}^n u$ for some $u \in W[\boldsymbol{k}]$ (and in that case, $vx = n$ iff $u_0 \neq 0$). Hence $v(x+y) \geq \min(vx, vy)$ by the additivity of $\mathbf{V}$. We also get $v(xy) = vx + vy$ by the identity $(*)$, and the fact that this identity clearly holds when $vx = vy = 0$. Thus $W[\boldsymbol{k}]$ is a domain, and v is a valuation on this domain. Next, we claim that $v(x-y) \geq n$ iff $x_i = y_i$ for all $i < n$. To see this, write $x = y + z$, so the claim becomes: $v(z) \geq n$ iff $x_i = y_i$ for all $i < n$. Now decompose each of x, y, z according to identity (2) of Lemma 6.8, and use the remark following this lemma to establish the claim. From this claim we get that $W[\boldsymbol{k}]$ is complete with respect to the ultranorm $|x| := p^{-vx}$. Identity (2) of Lemma 6.8, together with $[a] = \mathbf{F}^n[a^{p^{-n}}]$ for $a \in \boldsymbol{k}$, now yields

$$x = \sum_{n=0}^{\infty} \mathbf{V}^n[x_n] = \sum_{n=0}^{\infty} [x_n^{p^{-n}}]p^n.$$

If $|x| = 1$, then $x_0 \neq 0$, and thus by (2) and (3) of Lemma 6.8, $[x_0^{-1}]x = \mathbf{1} + y$ with $|y| < 1$, so $x \in U(W[\boldsymbol{k}])$. We have now shown that $W[\boldsymbol{k}]$ is a local domain with maximal ideal

$$\{x : vx > 0\} = \mathbf{V}\big(W[\boldsymbol{k}]\big) = \mathbf{V}\big(\mathbf{F}(W[\boldsymbol{k}])\big) = pW[\boldsymbol{k}].$$

It also follows that $vx = n$ iff $x = p^n u$ with $u \in U(W[\boldsymbol{k}])$. Thus $W[\boldsymbol{k}]$ is a complete DVR with normalized valuation v and residue field isomorphic to $\boldsymbol{k}$. Since $p \cdot \mathbf{1} = (0, 1, 0, 0, \dots) \neq \mathbf{0}$, the fraction field of $W[\boldsymbol{k}]$ has characteristic 0. The rest of the theorem now follows easily. □

In particular, $W[\boldsymbol{k}]$ is a strict local p-ring with residue field isomorphic to $\boldsymbol{k}$. This property determines the ring $W[\boldsymbol{k}]$ up to isomorphism, as a consequence of the next theorem. (It is this consequence that is crucial in the proof of the AKE-results in the unramified mixed characteristic case.)

6.11. Theorem. *Let A be a strict local p-ring and let $\phi : \boldsymbol{k} \to \boldsymbol{k}_A$ be a field embedding of $\boldsymbol{k}$ into the residue field $\boldsymbol{k}_A$ of A. Then there is a unique ring morphism $f : W[\boldsymbol{k}] \to A$ such that the diagram*

$$\begin{array}{ccc} W[\boldsymbol{k}] & \xrightarrow{f} & A \\ \downarrow & & \downarrow \\ \boldsymbol{k} & \xrightarrow[\phi]{} & \boldsymbol{k}_A \end{array}$$

commutes. The map f is injective. If ϕ is an isomorphism, so is f.

Proof. Let τ be the Teichmüller map of A. To simplify notation we identify $\boldsymbol{k}$ with a subfield of $\boldsymbol{k}_A$ via ϕ. We define $f : W[\boldsymbol{k}] \to A$ by

$$f(x) = \sum_{i=0}^{\infty} \tau(x_i^{p^{-i}})p^i.$$

It is clear that $f(\mathbf{0}) = 0$ and $f(\mathbf{1}) = 1$. Let $x + y = z$ in $W[\boldsymbol{k}]$. To prove $f(x) + f(y) = f(z)$, put

$$\mathbf{F}^{-n}x := \big(x_0^{p^{-n}}, x_1^{p^{-n}}, x_2^{p^{-n}}, \dots\big) \in W[\boldsymbol{k}],$$
$$\tau(\mathbf{F}^{-n}x) := \big(\tau(x_0^{p^{-n}}), \tau(x_1^{p^{-n}}), \tau(x_2^{p^{-n}}), \dots\big) \in W[A].$$

Then

$$\big(\tau(\mathbf{F}^{-n}x)\big)^{(n)} = \sum_{i=0}^{n} \tau(x_i^{p^{-i}})p^i \in A,$$

so

$$\lim_{n\to\infty} \big(\tau(\mathbf{F}^{-n}x)\big)^{(n)} = f(x).$$

Now $\mathbf{F}^{-n}x + \mathbf{F}^{-n}y = \mathbf{F}^{-n}z$ in $W[\boldsymbol{k}]$, so for all $\nu \in \mathbb{N}$:

$$\big(\tau(\mathbf{F}^{-n}x) + \tau(\mathbf{F}^{-n}y)\big)_\nu \equiv \big(\tau(\mathbf{F}^{-n}z)\big)_\nu \mod pA,$$

and thus by Lemma 6.4:

$$\big(\tau(\mathbf{F}^{-n}x)\big)^{(n)} + \big(\tau(\mathbf{F}^{-n}y)\big)^{(n)} \equiv \big(\tau(\mathbf{F}^{-n}z)\big)^{(n)} \mod p^{n+1}A.$$

Taking the limit as n goes to infinity yields $f(x) + f(y) = f(z)$. Likewise one shows that $f(x)f(y) = f(xy)$, so f is a ring morphism lifting ϕ. The other claims of the theorem are easy consequences of Corollary 6.2. □

For $A = \mathbb{Z}_p$ and residue field $\mathbb{F}_p$ this theorem yields a ring isomorphism

$$W[\mathbb{F}_p] \cong \mathbb{Z}_p, \quad x = (x_0, x_1, \dots) \mapsto \sum_{i=0}^{\infty} \tau(x_n)p^n,$$

where τ is the Teichmüller map of $\mathbb{Z}_p$ (which assigns to each $\eta \in \mathbb{F}_p^\times$ the unique $\zeta \in \mathbb{Z}_p$ with $\zeta^{p-1} = 1$ that has residue class a.) It is usual to identify the rings $W[\mathbb{F}_p]$ and $\mathbb{Z}_p$ via this isomorphism.

Exercises. Show:

$$\{x \in W[\boldsymbol{k}] : \mathbf{F}x = x^p\} \;=\; \{[a] : a \in \boldsymbol{k}\}.$$

With $\mathrm{Aut}(R)$ denoting the group of automorphisms of a ring R, show that

$$\phi \mapsto W[\phi] \;:\; \mathrm{Aut}(\boldsymbol{k}) \to \mathrm{Aut}(W[\boldsymbol{k}])$$

is a group isomorphism.

6.3 Coarsening

To obtain AKE-type results for unramified henselian valued fields of mixed characteristic we proceed as follows: in a sufficiently saturated model we can *coarsen* the valuation to have equicharacteristic zero and a residue field that is complete with respect to a discrete valuation. Using the uniqueness theorem at the end of the previous subsection, this allows us to reduce the problem to an equicharacteristic zero situation. In this short subsection we just consider the operation of coarsening in general.

Let Γ be an ordered abelian group. A subgroup Δ of Γ is said to be *convex* (in Γ) if for all $\gamma \in \Gamma$ and $\delta \in \Delta$,

$$|\gamma| < |\delta| \implies \gamma \in \Delta.$$

Given any $\gamma \in \Gamma$ there is a smallest convex subgroup of Γ that contains γ, namely

$$\{\delta \in \Gamma : |\delta| \leq n|\gamma| \text{ for some } n\},$$

If $\gamma \in \Gamma$ and $\gamma \neq 0$, there is also a largest convex subgroup of Γ that does not contain γ, namely

$$\{\delta \in \Gamma : |\delta| < n|\gamma| \text{ for all } n\}.$$

The subgroups $\{0\}$ and Γ of Γ are convex, and Γ is archimedean iff there are no other convex subgroups of Γ. The set of all convex subgroups of Γ is linearly ordered by inclusion.

Let Δ be a convex subgroup of Γ. Then we make the quotient group Γ/Δ into an ordered abelian group, by defining $\gamma + \Delta > 0 + \Delta$ if $\gamma > \Delta$. The natural map $\Gamma \to \Gamma/\Delta$ then preserves $\leq$: for $\gamma_1, \gamma_2 \in \Gamma$ we have

$$\gamma_1 \leq \gamma_2 \implies \gamma_1 + \Delta \leq \gamma_2 + \Delta.$$

Next, consider a valuation $v : K^\times \to \Gamma$ on a field K with valuation ring $\mathcal{O}$, maximal ideal $\mathfrak{m}$ of $\mathcal{O}$, and residue field $\boldsymbol{k} = \mathcal{O}/\mathfrak{m}$. Let a convex subgroup Δ of Γ be given. Then we define the *coarsening* $\dot{v}$ of v as follows:

$$\dot{v} : K^\times \to \dot{\Gamma} := \Gamma/\Delta, \qquad \dot{v}a := va + \Delta.$$

This coarsening is again a valuation on K, with valuation ring

$$\dot{\mathcal{O}} = \{a \in K : va \geq \delta \text{ for some } \delta \in \Delta\}.$$

The maximal ideal of $\dot{\mathcal{O}}$ is

$$\dot{\mathfrak{m}} = \{a \in K : va > \delta \text{ for all } \delta \in \Delta\}.$$

The information that gets lost by this coarsening can be recovered in the residue field $\dot{\boldsymbol{k}} = \dot{\mathcal{O}}/\dot{\mathfrak{m}}$ by means of the *induced* valuation

$$v : \dot{\boldsymbol{k}} \to \Delta, \qquad v(a + \dot{\mathfrak{m}}) := va \text{ for } a \in \dot{\mathcal{O}} \setminus \dot{\mathfrak{m}}.$$

(To keep notations simple we use the same letter v for the initial valuation on K and this induced valuation on $\dot{\boldsymbol{k}}$.) Note that $\dot{\mathfrak{m}}$ is a prime ideal of $\mathcal{O}$, and that the subring $\mathcal{O}/\dot{\mathfrak{m}}$ of $\dot{\mathcal{O}}/\dot{\mathfrak{m}} = \dot{\boldsymbol{k}}$ is the valuation ring of the induced valuation on $\dot{\boldsymbol{k}}$, with maximal ideal $\mathfrak{m}/\dot{\mathfrak{m}}$, and residue field $\boldsymbol{k}$ (after an obvious identification).

Thus in some sense the original valuation $v : K^\times \to \Gamma$ is decomposed into two simpler valuations, namely $\dot{v} : K^\times \to \dot{\Gamma}$ with residue field $\dot{k}$, and $v : \dot{k}^\times \to \Delta$.

Exercise. Show that $\mathcal{O}$ is henselian if and only if $\dot{\mathcal{O}}$ and $\mathcal{O}/\dot{\mathfrak{m}}$ are henselian.

Let us next consider the situation where Γ has a smallest positive element, call it 1, and $\Delta = \mathbb{Z}1$ is the smallest convex subgroup of Γ that contains 1. Pick some $t \in \mathcal{O}$ with $vt = 1$. It is easy to check that then

$$\dot{\mathcal{O}} = \mathcal{O}[1/t], \quad \dot{\mathfrak{m}} = \cap_{n=0}^{\infty} t^n \mathcal{O}.$$

For later use we note:

6.12. Lemma. *If (K, v, Γ) is $\aleph_1$-saturated, then the discrete valued field $(\dot{k}, v, \mathbb{Z}1)$ is complete.*

6.4 AKE for unramified mixed characteristic

For perfect $\boldsymbol{k}$ of characteristic p we let $W(\boldsymbol{k})$ be the fraction field of $W[\boldsymbol{k}]$, and consider it as the *valued field* that has $W[\boldsymbol{k}]$ as its valuation ring. A valued field (K, v, Γ) of mixed characteristic $(0, p)$ is said to be *unramified* if vp is the smallest positive element of Γ. (For example, the valued field $W(\boldsymbol{k})$ with $\boldsymbol{k}$ as above is unramified.)

6.13. Theorem. *Let (K_1, v_1, Γ_1) and (K_2, v_2, Γ_2) be henselian unramified fields of mixed characteristic $(0, p)$, with perfect residue fields $\boldsymbol{k}_1$ and $\boldsymbol{k}_2$. Suppose that $\boldsymbol{k}_1 \equiv \boldsymbol{k}_2$ (as fields), and $\Gamma_1 \equiv \Gamma_2$ (as ordered abelian groups). Then $(K_1, v_1, \Gamma_1) \equiv (K_2, v_2, \Gamma_2)$.*

Proof. As in the proof of Theorem 5.11 we shall take a short cut by assuming CH. Then we can reduce to the case that (K_i, v_i, Γ_i) is saturated of size $\aleph_1$ for $i = 1, 2$, so that we have isomorphisms

$$\phi : \boldsymbol{k}_1 \cong \boldsymbol{k}_2, \qquad h : \Gamma_1 \cong \Gamma_2.$$

For $i = 1, 2$ we identify $\mathbb{Z}$ with the convex subgroup $\mathbb{Z} \cdot v_i p$ of Γ_i via $k \mapsto k \cdot v_i p$, and coarsen v_i accordingly, obtaining the valuation

$$\dot{v_i} \ : \ K_i^\times \to \dot{\Gamma_i} := \Gamma_i/\mathbb{Z}.$$

Its residue field $\dot{\boldsymbol{k}_i}$ carries the distinguished discrete valuation $v_i : \dot{\boldsymbol{k}_i}^\times \to \mathbb{Z}$. Then h induces an isomorphism $\dot{h} : \dot{\Gamma_1} \cong \dot{\Gamma_2}$. Because $\dot{\boldsymbol{k}_i}$ is complete with respect to v_i and has perfect residue field $\boldsymbol{k}_i$, we can use Theorem 6.11 to lift the isomorphism $\phi : \boldsymbol{k}_1 \cong \boldsymbol{k}_2$ to an isomorphism

$$(f, \mathrm{id}) \ : \ (\dot{\boldsymbol{k}_1}, v_1, \mathbb{Z}) \cong (\dot{\boldsymbol{k}_2}, v_2, \mathbb{Z}).$$

Since the valued field $(K_1, \dot{v}_1, \dot{\Gamma}_1)$ is henselian of equicharacteristic 0 we have a lifting $i_1 : \dot{\boldsymbol{k}}_1 \to K_1$ of the residue field of this valued field, and likewise we have a lifting $i_2 : \dot{\boldsymbol{k}}_2 \to K_2$ of the residue field of the valued field $(K_2, \dot{v}_2, \dot{\Gamma}_2)$. It can be shown that we also have $\times$-sections $s_i : \dot{\Gamma}_i \to K_i^\times$ of these valued fields. (.....this needs some explanation...) Under these circumstances the proof of Theorem 5.11 constructs an isomorphism

$$(F, \dot{h}, f) : (K_1, \dot{\Gamma}_1, \dot{\boldsymbol{k}}_1; \dot{v}_1, \dot{\pi}_1, s_1, i_1) \cong (K_2, \dot{\Gamma}_2, \dot{\boldsymbol{k}}_2; \dot{v}_2, \dot{\pi}_2, s_2, i_2),$$

where $\dot{\pi}_i : \dot{\mathcal{O}}_i \to \dot{\boldsymbol{k}}_i$ is the residue map of the valued field $(K_i, \dot{v}_i, \dot{\Gamma}_i)$. It follows easily that then we have an isomorphism

$$(F, h, \phi) : (K_1, \Gamma_1, \boldsymbol{k}_1; v_1, \pi_1) \cong (K_2, \Gamma_2, \boldsymbol{k}_2; v_2, \pi_2),$$

where $\pi_i : \mathcal{O}_i \to \boldsymbol{k}_i$ is the residue map of the valued field (K_i, v_i, Γ_i). $\square$