Chapter 2. Normed Rings

Norms $\|\cdot\|$ of associative rings are generalizations of absolute values $|\cdot|$ of integral domains, where the inequality $\|xy\| \leq \|x\| \cdot \|y\|$ replaces the standard multiplication rule $|xy| = |x| \cdot |y|$. Starting from a complete normed commutative ring A, we study the ring $A\{x\}$ of all formal power series with coefficients in A converging to zero. This is again a complete normed ring (Lemma 2.2.1). We prove an analog of the Weierstrass division theorem (Lemma 2.2.4) and the Weierstrass preparation theorem for $A\{x\}$ (Corollary 2.2.5). If A is a field K and the norm is an absolute value, then $K\{x\}$ is a principal ideal domain, hence a factorial ring (Proposition 2.3.1). Moreover, $\text{Quot}(K\{x\})$ is a Hilbertian field (Theorem 2.3.3). It follows that $\text{Quot}(K\{x\})$ is not a Henselian field (Corollary 2.3.4). In particular, $\text{Quot}(K\{x\})$ is not separably closed in K((x)). In contrast, the field $K((x))_0$ of all formal power series over K that converge at some element of K is algebraically closed in K((x))(Proposition 2.4.5).

2.1 Normed Rings

In Section 4.4 we construct patching data over fields K(x), where K is a complete ultrametric valued field. The 'analytic' fields P_i will be the quotient fields of certain rings of convergent power series in several variables over K. At a certain point in a proof by induction we consider a ring of convergent power series in one variable over a complete ultrametric valued ring. So, we start by recalling the definition and properties of the latter rings.

Let A be a commutative ring with 1. An **ultrametric absolute value** of A is a function $| : A \to \mathbb{R}$ satisfying the following conditions:

(1a) $|a| \ge 0$, and |a| = 0 if and only if a = 0.

(1b) There exists $a \in A$ such that 0 < |a| < 1.

(1c) $|ab| = |a| \cdot |b|$.

(1d) $|a+b| \le \max(|a|, |b|).$

By (1a) and (1c), A is an integral domain. By (1c), the absolute value of A extends to an absolute value on the quotient field of A (by $|\frac{a}{b}| = \frac{|a|}{|b|}$). It follows also that |1| = 1, |-a| = |a|, and (1d') if |a| < |b|, then |a + b| = |b|.

Denote the ordered additive group of the real numbers by \mathbb{R}^+ . The function $v: \operatorname{Quot}(A) \to \mathbb{R}^+ \cup \{\infty\}$ defined by $v(a) = -\log |a|$ satisfies the following conditions:

(2a) $v(a) = \infty$ if and only if a = 0.

- (2b) There exists $a \in \text{Quot}(A)$ such that $0 < v(a) < \infty$.
- (2c) v(ab) = v(a) + v(b).

(2d) $v(a+b) \ge \min\{v(a), v(b)\}$ (and v(a+b) = v(b) if v(b) < v(a)).

In other words, v is a **real valuation** of Quot(A). Conversely, every real valuation v: $\text{Quot}(A) \to \mathbb{R}^+ \cup \{\infty\}$ gives rise to a nontrivial ultrametric absolute value $|\cdot|$ of Quot(A): $|a| = \varepsilon^{v(a)}$, where ε is a fixed real number between 0 and 1.

An attempt to extend an absolute value from A to a larger ring A' may result in relaxing Condition (1c), replacing the equality by an inequality. This leads to the more general notion of a 'norm'.

Definition 2.1.1: Normed rings. Let R be an associative ring with 1. A **norm** on R is a function $\| \|: R \to \mathbb{R}$ that satisfies the following conditions for all $a, b \in R$:

(3a) $||a|| \ge 0$, and ||a|| = 0 if and only if a = 0; further ||1|| = ||-1|| = 1.

(3b) There is an $x \in R$ with 0 < ||x|| < 1.

(3c) $||ab|| \le ||a|| \cdot ||b||$.

(3d) $||a+b|| \le \max(||a||, ||b||).$

The norm $\| \|$ naturally defines a topology on R whose basis is the collection of all sets $U(a_0, r) = \{a \in R | \|a - a_0\| < r\}$ with $a_0 \in R$ and r > 0. Both addition and multiplication are continuous under that topology. Thus, R is a **topological ring**.

Definition 2.1.2: Complete rings. Let R be a normed ring. A sequence a_1, a_2, a_3, \ldots of elements of R is **Cauchy** if for each $\varepsilon > 0$ there exists m_0 such that $||a_n - a_m|| < \varepsilon$ for all $m, n \ge m_0$. We say that R is **complete** if every Cauchy sequence converges.

Lemma 2.1.3: Let R be a normed ring and let $a, b \in R$. Then:

(a) ||-a|| = ||a||.

- (b) If ||a|| < ||b||, then ||a + b|| = ||b||.
- (c) A sequence a_1, a_2, a_3, \ldots of elements of R is Cauchy if for each $\varepsilon > 0$ there exists m_0 such that $||a_{m+1} - a_m|| < \varepsilon$ for all $m \ge m_0$.
- (d) The map $x \to ||x||$ from R to \mathbb{R} is continuous.
- (e) If R is complete, then a series $\sum_{n=0}^{\infty} a_n$ of elements of R converges if and only if $a_n \to 0$.
- (f) If R is complete and ||a|| < 1, then $1-a \in R^{\times}$. Moreover, $(1-a)^{-1} = 1+b$ with ||b|| < 1.

Proof of (a): Observe that $||-a|| \le ||-1|| \cdot ||a|| \le ||a||$. Replacing a by -a, we get $||a|| \le ||-a||$, hence the claimed equality.

Proof of (b): Assume ||a+b|| < ||b||. Then, by (a), $||b|| = ||(-a) + (a+b)|| \le \max(||-a||, ||a+b||) < ||b||$, which is a contradiction.

Proof of (c): With m_0 as above let $n > m \ge m_0$. Then

$$||a_n - a_m|| \le \max(||a_n - a_{n-1}||, \dots, ||a_{m+1} - a_m||) < \varepsilon.$$

Proof of (d): By (3d), $||x|| = ||(x-y) + y|| \le \max(||x-y||, ||y||) \le ||x-y|| + ||y||$. Hence, $||x|| - ||y|| \le ||x-y||$. Symmetrically, $||y|| - ||x|| \le ||y-x|| = ||y-x|| = ||y-x|| = ||y||$.

||x - y||. Therefore, $|||x|| - ||y|| | \le ||x - y||$. Consequently, the map $x \mapsto ||x||$ is continuous.

Proof of (e): Let $s_n = \sum_{i=0}^n a_i$. Then $s_{n+1} - s_n = a_{n+1}$. Thus, by (c), s_1, s_2, s_3, \ldots is a Cauchy sequence if and only if $a_n \to 0$. Hence, the series $\sum_{n=0}^{\infty} a_n$ converges if and only if $a_n \to 0$.

Proof of (f): The sequence a^n tends to 0. Hence, by (e), $\sum_{n=0}^{\infty} a^n$ converges. The identities $(1-a) \sum_{i=0}^{n} a^i = 1 - a^{n+1}$ and $\sum_{i=0}^{n} a^i (1-a) = 1 - a^{n+1}$ imply that $\sum_{n=0}^{\infty} a^n$ is both the right and the left inverse of 1-a. Moreover, $\sum_{n=0}^{\infty} a^n = 1 + b$ with $b = \sum_{n=1}^{\infty} a^n$ and $\|b\| \le \max_{n\ge 1} \|a\|^n < 1$.

Example 2.1.4:

(a) Every field K with an ultrametric absolute value is a normed ring. For example, for each prime number p, \mathbb{Q} has a *p*-adic absolute value $|\cdot|_p$ which is defined by $|x|_p = p^{-m}$ if $x = \frac{a}{b}p^m$ with $a, b, m \in \mathbb{Z}$ and $p \nmid a, b$.

(b) The ring \mathbb{Z}_p of *p*-adic integers and the field \mathbb{Q}_p of *p*-adic numbers are complete with respect to the *p*-adic absolute value.

(c) Let K_0 be a field and let $0 < \varepsilon < 1$. The ring $K_0[[t]]$ (resp. field $K_0((t))$) of formal power series $\sum_{i=0}^{\infty} a_i t^i$ (resp. $\sum_{i=m}^{\infty} a_i t^i$ with $m \in \mathbb{Z}$) with coefficients in K_0 is complete with respect to the absolute value $|\sum_{i=m}^{\infty} a_i t^i| = \varepsilon^{\min(i \mid a_i \neq 0)}$.

(d) Let $\|\cdot\|$ be a norm of a commutative ring A. For each positive integer n we extend the norm to the associative (and usually not commutative) ring $M_n(A)$ of all $n \times n$ matrices with entries in A by

$$||(a_{ij})_{1 \le i,j \le n}|| = \max(||a_{ij}||_{1 \le i,j \le n}).$$

If $b = (b_{jk})_{1 \le j,k \le n}$ is another matrix and c = ab, then $c_{ik} = \sum_{j=1}^{n} a_{ij} b_{jk}$ and $\|c_{ik}\| \le \max(\|a_{ij}\| \cdot \|b_{jk}\|) \le \|a\| \cdot \|b\|$. Hence, $\|c\| \le \|a\| \|b\|$. This verifies Condition (3c). The verification of (3a), (3b), and (3d) is straightforward. Note that when $n \ge 2$, even if the initial norm of A is an absolute value, the extended norm satisfies only the weak condition (3c) and not the stronger condition (1c), so it is not an absolute value.

If A is complete, then so is $M_n(A)$. Indeed, let $a_i = (a_{i,rs})_{1 \le r,s \le n}$ be a Cauchy sequence in $M_n(A)$. Since $||a_{i,rs} - a_{j,rs}|| \le ||a_i - a_j||$, each of the sequences $a_{1,rs}, a_{2,rs}, a_{3,rs}, \ldots$ is Cauchy, hence converges to an element b_{rs} of A. Set $b = (b_{rs})_{1 \le r,s \le n}$. Then $a_i \to b$. Consequently, $M_n(A)$ is complete.

(e) Let \mathfrak{a} be a proper ideal of a Noetherian domain A. By a theorem of Krull, $\bigcap_{n=0}^{\infty} \mathfrak{a}^n = 0$ [AtM69, p. 110, Cor. 10.18]. We define an \mathfrak{a} -adic norm on A by choosing an ε between 0 and 1 and setting $||a|| = \varepsilon^{\max(n)} a^{\epsilon \mathfrak{a}^n}$. If $||a|| = \varepsilon^m$ and $||b|| = \varepsilon^n$, and say $m \leq n$, then $\mathfrak{a}^n \subseteq \mathfrak{a}^m$, so $a + b \in \mathfrak{a}^m$, hence $||a + b|| \leq \varepsilon^m = \max(||a||, ||b||)$. Also, $ab \in \mathfrak{a}^{m+n}$, so $||ab|| \leq ||a|| \cdot ||b||$. \Box

Like absolute valued rings, every normed ring has a completion:

LEMMA 2.1.5: Every normed ring (R, || ||) can be embedded into a complete normed ring $(\hat{R}, || ||)$ such that R is dense in \hat{R} and the following universal condition holds:

(4) Each continuous homomorphism f of R into a complete ring S uniquely extends to a continuous homomorphism $\hat{f}: \hat{R} \to S$.

The normed ring $(\hat{R}, \| \|)$ is called the **completion** of $(R, \| \|)$.

Proof: We consider the set A of all Cauchy sequences $\mathbf{a} = (a_n)_{n=1}^{\infty}$ with $a_n \in R$. For each $\mathbf{a} \in A$, the values $||a_n||$ of its components are bounded. Hence, A is closed under componentwise addition and multiplication and contains all constant sequences. Thus, A is a ring. Let \mathbf{n} be the ideal of all sequences that converge to 0. We set $\hat{R} = A/\mathbf{n}$ and identify each $x \in R$ with the coset $(x)_{n=1}^{\infty} + \mathbf{n}$.

If $\mathbf{a} \in A \setminus \mathbf{n}$, then $||a_n||$ eventually becomes constant. Indeed, there exists $\beta > 0$ such that $||a_n|| \ge \beta$ for all sufficiently large n. Choose n_0 such that $||a_n - a_m|| < \beta$ for all $n, m \ge n_0$. Then, $||a_n - a_{n_0}|| < \beta \le ||a_{n_0}||$, so $||a_n|| = ||(a_n - a_{n_0}) + a_{n_0}|| = ||a_{n_0}||$. We define $||\mathbf{a}||$ to be the eventual absolute value of a_n and note that $||\mathbf{a}|| \ne 0$. If $\mathbf{b} \in \mathbf{n}$, we set $||\mathbf{b}|| = 0$ and observe that $||\mathbf{a} + \mathbf{b}|| = ||\mathbf{a}||$. It follows that $||\mathbf{a} + \mathbf{n}|| = ||\mathbf{a}||$ is a well defined function on \hat{R} which extends the norm of R.

One checks that $\| \|$ is a norm on \hat{R} and that R is dense in \hat{R} . Indeed, if $\mathbf{a} = (a_n)_{n=1}^{\infty} \in A$, then $a_n + \mathbf{n} \to \mathbf{a} + \mathbf{n}$. To prove that \hat{R} is complete under $\| \|$ we consider a Cauchy sequence $(a_k)_{k=1}^{\infty}$ of elements of \hat{R} . For each k we choose an element $b_k \in R$ such that $\| b_k - a_k \| < \frac{1}{k}$. Then $(b_k)_{k=1}^{\infty}$ is a Cauchy sequence of R and the sequence $(\mathbf{a}_k)_{k=1}^{\infty}$ converges to the element $(b_k)_{k=1}^{\infty} + \mathbf{n}$ of \hat{R} .

Finally, let S be a complete normed ring and $f: R \to S$ a continuous homomorphism. Then, for each $\mathbf{a} = (a_n)_{n=1}^{\infty} \in A$, the sequence $(f(a_n))_{n=1}^{\infty}$ of S is Cauchy, hence it converges to an element s. Define $\hat{f}(\mathbf{a} + \mathbf{n}) = s$ and check that \hat{f} has the desired properties.

Example 2.1.6: Let A be a commutative ring. We consider the ring $R = A[x_1, \ldots, x_n]$ of polynomials over A in the variables x_1, \ldots, x_n and the ideal \mathfrak{a} of R generated by x_1, \ldots, x_n . The completion of R with respect to \mathfrak{a} is the ring $\hat{R} = A[[x_1, \ldots, x_n]]$ of all formal power series $f(x_1, \ldots, x_n) = \sum_{i=0}^{\infty} f_i(x_1, \ldots, x_n)$, where $f_i \in A[x_1, \ldots, x_n]$ is a homogeneous polynomial of degree i. Moreover, $\hat{R} = A[[x_1, \ldots, x_{n-1}]][[x_n]]$ and \hat{R} is complete with respect to the ideal $\hat{\mathfrak{a}}$ generated by x_1, \ldots, x_n [Lan93, Chap. IV, Sec. 9]. If R is a Noetherian integral domain, then so is \hat{R} [Lan93, p. 210, Cor. 9.6]. If A = K is a field, then \hat{R} is a unique factorization domain [Mat94, Thm. 20.3].

If A is an integral domain, then the function $v: \hat{R} \to \mathbb{Z} \cup \{\infty\}$ defined for f as in the preceding paragraph by $v(f) = \min_{i \ge 0} (f_i \ne 0)$ satisfies Condition (2), so it extends to a discrete valuation of $\hat{K} = \text{Quot}(\hat{R})$. However, by Weissauer, \hat{K} is Hilbertian if $n \ge 2$. [FrJ08, Example 15.5.2]. Hence, \hat{K}

is Henselian with respect to no valuation [FrJ08, Lemma 15.5.4]. Since v is discrete, \hat{K} is not complete with respect to v.

2.2 Rings of Convergent Power Series

Let A be a complete normed commutative ring and x a variable. Consider the following subset of A[[x]]:

$$A\{x\} = \left\{ \sum_{n=0}^{\infty} a_n x^n \mid a_n \in A, \lim_{n \to \infty} \|a_n\| = 0 \right\}.$$

For each $f = \sum_{n=0}^{\infty} a_n x^n \in A\{x\}$ we define $||f|| = \max(||a_n||)_{n=0,1,2,\dots}$. This definition makes sense because $a_n \to 0$, hence $||a_n||$ is bounded.

We prove the Weierstrass division and the Weierstrass preparation theorems for $A\{x\}$ in analogy to the corresponding theorems for the ring of formal power series in one variable over a local ring.

LEMMA 2.2.1:

(a) $A\{x\}$ is a subring of A[[x]] containing A.

- (b) The function $|| ||: A\{x\} \to \mathbb{R}$ is a norm.
- (c) The ring $A\{x\}$ is complete under that norm.
- (d) Let B be a complete normed ring extension of A. Then each $b \in B$ with $||b|| \le 1$ defines an evaluation homomorphism $A\{x\} \to B$ given by

$$f = \sum_{n=0}^{\infty} a_n x^n \mapsto f(b) = \sum_{n=0}^{\infty} a_n b^n$$

Proof of (a): We prove only that $A\{x\}$ is closed under multiplication. To that end let $f = \sum_{i=0}^{\infty} a_i x^i$ and $g = \sum_{j=0}^{\infty} b_j x^j$ be elements of $A\{x\}$. Consider $\varepsilon > 0$ and let n_0 be a positive number such that $||a_i|| < \varepsilon$ if $i \ge \frac{n_0}{2}$ and $||b_j|| < \varepsilon$ if $j \ge \frac{n_0}{2}$. Now let $n \ge n_0$ and i + j = n. Then $i \ge \frac{n_0}{2}$ or $j \ge \frac{n_0}{2}$. It follows that $||\sum_{i+j=n}^{\infty} a_i b_j|| \le \max(||a_i|| \cdot ||b_j||)_{i+j=n} \le \varepsilon \cdot \max(||f|, ||g||)$. Thus, $fg = \sum_{n=0}^{\infty} \sum_{i+j=n}^{\infty} a_i b_j x^n$ belongs to $A\{x\}$, as claimed.

Proof of (b): Standard checking.

Proof of (c): Let $f_i = \sum_{n=0}^{\infty} a_{in} x^n$, $i = 1, 2, 3, \ldots$, be a Cauchy sequence in $A\{x\}$. For each $\varepsilon > 0$ there exists i_0 such that $||a_{in} - a_{jn}|| \le ||f_i - f_j|| < \varepsilon$ for all $i, j \ge i_0$ and for all n. Thus, for each n, the sequence $a_{1n}, a_{2n}, a_{3n}, \ldots$ is Cauchy, hence converges to an element $a_n \in A$. If we let j tend to infinity in the latter inequality, we get that $||a_{in} - a_n|| < \varepsilon$ for all $i \ge i_0$ and all n. Set $f = \sum_{i=0}^{\infty} a_n x^n$. Then $a_n \to 0$ and $||f_i - f|| = \max(||a_{in} - a_n||)_{n=0,1,2,\ldots} < \varepsilon$ if $i \ge i_0$. Consequently, the f_i 's converge in $A\{x\}$.

Proof of (d): Note that $||a_n b^n|| \le ||a_n|| \to 0$, so $\sum_{n=0}^{\infty} a_n b^n$ is an element of B.

Definition 2.2.2: Let $f = \sum_{n=0}^{\infty} a_n x^n$ be a nonzero element of $A\{x\}$. We define the **pseudo degree** of f to be the integer $d = \max\{n \ge 0 \mid ||a_n|| = ||f||\}$ and set pseudo.deg(f) = d. The element a_d is the **pseudo leading coefficient** of f. Thus, $||a_d|| = ||f||$ and $||a_n|| < ||f||$ for each n > d. If $f \in A[x]$ is a polynomial, then pseudo.deg $(f) \le \deg(f)$. If a_d is invertible in A and satisfies $||ca_d|| = ||c|| \cdot ||a_d||$ for all $c \in A$, we call f regular. In particular, if A is a field and || || is an ultrametric absolute value, then each $0 \ne f \in A\{x\}$ is regular. The next lemma implies that in this case || || is an absolute value of $A\{x\}$.

LEMMA 2.2.3 (Gauss' Lemma): Let $f, g \in A\{x\}$. Suppose f is regular of pseudo degree d and $f, g \neq 0$. Then $||fg|| = ||f|| \cdot ||g||$ and pseudo.deg(fg) = pseudo.deg(f) + pseudo.deg(g).

Proof: Let $f = \sum_{i=0}^{\infty} a_i x^i$ and $g = \sum_{j=0}^{\infty} b_j x^j$. Let a_d (resp. b_e) be the pseudo leading coefficient of f (resp. g). Then $fg = \sum_{n=0}^{\infty} c_n x^n$ with $c_n = \sum_{i+j=n}^{\infty} a_i b_j$.

If i + j = d + e and $(i, j) \neq (d, e)$, then either i > d or j > e. In each case, $||a_ib_j|| \leq ||a_i|| ||b_j|| < ||f|| \cdot ||g||$. By our assumption on a_d , we have $||a_db_e|| = ||a_d|| \cdot ||b_e|| = ||f|| \cdot ||g||$. By Lemma 2.1.3(b), this implies $||c_{d+e}|| = ||f|| \cdot ||g||$.

If i+j > d+e, then either i > d and $||a_i|| < ||f||$ or j > e and $||b_j|| < ||g||$. In each case $||a_ib_j|| \le ||a_i|| \cdot ||b_j|| < ||f|| \cdot ||g||$. Hence, $||c_n|| < ||c_{d+e}||$ for each n > d+e. Therefore, c_{d+e} is the pseudo leading coefficient of fg, and the lemma is proved.

PROPOSITION 2.2.4 (Weierstrass division theorem): Let $f \in A\{x\}$ and let $g \in A\{x\}$ be regular of pseudo degree d. Then there are unique $q \in A\{x\}$ and $r \in A[x]$ such that f = qg + r and $\deg(r) < d$. Moreover,

(1)
$$||qg|| = ||q|| \cdot ||g|| \le ||f||$$
 and $||r|| \le ||f||$

Proof: We break the proof into several parts.

PART A: Proof of (1). First we assume that there exist $q \in A\{x\}$ and $r \in A[x]$ such that f = qg + r with $\deg(r) < d$. If q = 0, then (1) is clear. Otherwise, $q \neq 0$ and we let e = pseudo.deg(q). By Lemma 2.2.3, $\|qg\| = \|q\| \cdot \|g\|$ and pseudo.deg $(qg) = e + d > \deg(r)$. Hence, the coefficient c_{d+e} of x^{d+e} in qg is also the coefficient of x^{d+e} in f. It follows that $\|qg\| = \|c_{d+e}\| \le \|f\|$. Consequently, $\|r\| = \|f - qg\| \le \|f\|$.

PART B: Uniqueness. Suppose f = qg + r = q'g + r', where $q, q' \in A\{x\}$ and $r, r' \in A[x]$ are of degrees less than d. Then 0 = (q - q')g + (r - r'). By Part A, applied to 0 rather than to f, $||q - q'|| \cdot ||g|| = ||r - r'|| = 0$. Hence, q = q' and r = r'.

PART C: Existence if g is a polynomial of degree d. Write $f = \sum_{n=0}^{\infty} b_n x^n$ with $b_n \in A$ converging to 0. For each $m \ge 0$ let $f_m = \sum_{n=0}^{m} b_n x^n \in$ A[x]. Then the f_1, f_2, f_3, \ldots converge to f, in particular they form a Cauchy sequence. Since g is regular of pseudo degree d, its leading coefficient is invertible. Euclid's algorithm for polynomials over A produces $q_m, r_m \in A[x]$ with $f_m = q_m g + r_m$ and $\deg(r_m) < \deg(g)$. Thus, for all k, m we have $f_m - f_k = (q_m - q_k)g + (r_m - r_k)$. By Part A, $||q_m - q_k|| \cdot ||g||, ||r_m - r_k|| \leq ||f_m - f_k||$. Thus, $\{q_m\}_{m=0}^{\infty}$ and $\{r_m\}_{m=0}^{\infty}$ are Cauchy sequences in $A\{x\}$. Since $A\{x\}$ is complete (Lemma 2.2.1), the q_m 's converge to some $q \in A\{x\}$. Since A is complete, the r_m 's converge to an $r \in A[x]$ of degree less than d. It follows that f = qg + r

PART D: Existence for arbitrary g. Let $g = \sum_{n=0}^{\infty} a_n x^n$ and set $g_0 = \sum_{n=0}^{d} a_n x^n \in A[x]$. Then $||g-g_0|| < ||g||$. By Part C, there are $q_0 \in A\{x\}$ and $r_0 \in A[x]$ such that $f = q_0 g_0 + r_0$ and $\deg(r_0) < d$. By Part A, $||q_0|| \le \frac{||f||}{||g||}$ and $||r_0|| \le ||f||$. Thus, $f = q_0 g + r_0 + f_1$, where $f_1 = -q_0(g - g_0)$, and $||f_1|| \le \frac{||g-g_0||}{||g||} \cdot ||f||$.

Set $f_0 = f$. By induction we get, for each $k \ge 0$, elements $f_k, q_k \in A\{x\}$ and $r_k \in A[x]$ such that $\deg(r_k) < d$ and

$$f_{k} = q_{k}g + r_{k} + f_{k+1}, \quad ||q_{k}|| \leq \frac{||f_{k}||}{||g||}, \quad ||r_{k}|| \leq ||f_{k}||, \quad \text{and}$$
$$||f_{k+1}|| \leq \frac{||g - g_{0}||}{||g||} ||f_{k}||.$$

It follows that $||f_k|| \leq \left(\frac{||g-g_0||}{||g||}\right)^k ||f||$, so $||f_k|| \to 0$. Hence, also $||q_k||, ||r_k|| \to 0$. 0. Therefore, $q = \sum_{k=0}^{\infty} q_k \in A\{x\}$ and $r = \sum_{k=0}^{\infty} r_k \in A[x]$. By construction, $f = \sum_{n=0}^{k} q_n g + \sum_{n=0}^{k} r_n + f_{k+1}$ for each k. Taking k to infinity, we get f = qg + r and $\deg(r) < d$.

COROLLARY 2.2.5 (Weierstrass preparation theorem): Let $f \in A\{x\}$ be regular of pseudo degree d. Then f = qg, where q is a unit of $A\{x\}$ and $g \in A[x]$ is a monic polynomial of degree d with ||g|| = 1. Moreover, q and g are uniquely determined by these conditions.

Proof: By Proposition 2.2.4 there are $q' \in A\{x\}$ and $r' \in A[x]$ of degree < d such that $x^d = q'f + r'$ and $||r'|| \le ||x^d|| = 1$. Set $g = x^d - r'$. Then g is monic of degree d, g = q'f, and ||g|| = 1. It remains to show that $q' \in A\{x\}^{\times}$.

Note that g is regular of pseudo degree d. By Proposition 2.2.4, there are $q \in A\{x\}$ and $r \in A[x]$ such that f = qg + r and $\deg(r) < d$. Thus, f = qq'f + r. Since $f = 1 \cdot f + 0$, the uniqueness part of Proposition 2.2.4 implies that qq' = 1. Hence, $q' \in A\{x\}^{\times}$.

Finally suppose $f = q_1g_1$, where $q \in A\{x\}^{\times}$ and $g_1 \in A[x]$ is monic of degree d with $||g_1|| = 1$. Then $g_1 = (q_1^{-1}q_2)g$ and $g_1 = 1 \cdot g + (g_1 - g)$, where $g_1 = g$ is a polynomial of degree at most d - 1. By the uniqueness part of Proposition 2.2.4, $q_1^{-1}q_2 = 1$, so $q_1 = q_2$ and $g_1 = g$.

COROLLARY 2.2.6: Let $f = \sum_{n=0}^{\infty} a_n x^n$ be a regular element of $A\{x\}$ such that $||a_0b|| = ||a_0|| \cdot ||b||$ for each $b \in A$. Then $f \in A\{x\}^{\times}$ if and only if pseudo.deg(f) = 0 and $a_0 \in A^{\times}$.

Proof: If there exists $g \in \sum_{n=0}^{\infty} b_n x^n$ in $A\{x\}$ such that fg = 1, then pseudo.deg(f) + pseudo.deg(g) = 0 (Lemma 2.2.3 applied to 1 rather than to f), so pseudo.deg(f) = 0. In addition, $a_0b_0 = 1$, so $a_0 \in A^{\times}$.

Conversely, suppose pseudo.deg(f) = 0 and $a_0 \in A^{\times}$. Then f is regular. Hence, by Corollary 2.2.5, $f = q \cdot 1$ where $q \in A\{x\}^{\times}$.

Alternatively, $a_0^{-1}f = 1 - h$, where $h = -\sum_{n=1}^{\infty} a_0^{-1}a_nx^n$. By our assumption on a_0 , we have $||a_0^{-1}|| \cdot ||a_0|| = ||a_0^{-1}a_0|| = 1$, so $||a_0^{-1}|| = ||a_0||^{-1}$. Since pseudo.deg(f) = 0, we have $||a_0|| < ||a_n||$, so $||a_0^{-1}a_n|| \le ||a_0||^{-1}||a_n|| < 1$ for each $n \ge 1$. It follows that $||h|| = \max(||a_0^{-1}a_n||)_{n=1,2,3,...} < 1$. By Lemma 2.1.3(f), $a_0^{-1}f \in A\{x\}^{\times}$, so $f \in A\{x\}^{\times}$.

2.3 Properties of the Ring $K\{x\}$

We turn our attention in this section to the case where the ring A of the previous sections is a complete field K under an ultrametric absolute value | | and $O = \{a \in K | |a| \le 1\}$ its **valuation ring**. We fix K and O for the whole section and prove that $K\{x\}$ is a principal ideal domain and that $F = \text{Quot}(K\{x\})$ is a Hilbertian field.

Note that in our case $|ab| = |a| \cdot |b|$ for all $a, b \in K$ and each nonzero element of K is invertible. Hence, each nonzero $f \in K\{x\}$ is regular. It follows from Lemma 2.2.3 that the norm of $K\{x\}$ is multiplicative, hence it is an absolute value which we denote by || rather than by |||.

Proposition 2.3.1:

- (a) $K\{x\}$ is a principal ideal domain. Moreover, each ideal in $K\{x\}$ is generated by an element of O[x].
- (b) $K\{x\}$ a unique factorization domain.
- (c) A nonzero element $f \in K\{x\}$ is invertible if and only if pseudo.deg(f) = 0.
- (d) pseudo.deg(fg) = pseudo.deg(f) + pseudo.deg(g) for all $f, g \in K\{x\}$ with $f, g \neq 0$.
- (e) Every prime element f of K{x} can be written as f = ug, where u is invertible in K{x} and g is an irreducible element of K[x].
- (f) If a $g \in K[x]$ is monic of degree d, irreducible in K[x], and |g| = 1, then g is irreducible in $K\{x\}$.
- (g) There are irreducible polynomials in K[x] that are not irreducible in $K\{x\}$.
- (h) There are reducible polynomials in K[x] that are irreducible in $K\{x\}$.

Proof of (a): By the Weierstrass preparation theorem (Corollary 2.2.5) (applied to K rather than to A) each nonzero ideal \mathfrak{a} of $K\{x\}$ is generated by the ideal $\mathfrak{a} \cap K[x]$ of K[x]. Since K[x] is a principal ideal domain, $\mathfrak{a} \cap K[x] = fK[x]$

for some nonzero $f \in K[x]$. Consequently, $\mathfrak{a} = fK\{x\}$ is a principal ideal. Moreover, dividing f by one of its coefficients with highest absolute value, we may assume that $f \in O[x]$.

Proof of (b): Since every principal ideal domain has a unique factorization, (b) is a consequence of (a).

Proof of (c): Apply Corollary 2.2.6.

Proof of (d): Apply Lemma 2.2.3.

Proof of (e): By (a), $f = u_1 f_1$ with $u_1 \in K\{x\}^{\times}$ and $f_1 \in K[x]$. Write $f_1 = g_1 \cdots g_n$ with irreducible polynomials $g_1, \ldots, g_n \in K[x]$. Then $f = u_1 g_1 \cdots g_n$. Since f is irreducible in $K\{x\}$, one of the g_i 's, say g_n is irreducible in $K\{x\}$ and all the others, that is g_1, \ldots, g_{n-1} , are invertible in $K\{x\}$. Set $u = u_1 g_1 \cdots g_{n-1}$ and $g = g_n$. Then f = ug is the desired presentation.

Proof of (f): The irreducibility of g in K[x] implies that d > 0. Our assumptions imply that pseudo.deg(g) = d. Hence, by Corollary 2.2.6, $g \not K\{x\}^{\times}$.

Now assume $g = g_1g_2$, where $g_1, g_2 \in K\{x\}$ are nonunits. By Corollary 2.2.5, we may assume that $g_1 \in K[x]$ is monic, say of degree d_1 , and $|g_1| = 1$. Thus pseudo.deg $(g_1) = d_1$. By Euclid's algorithm, there are $q, r \in K[x]$ such that $g = qg_1 + r$ and deg $(r) < d_1$. Applying the additional presentation $g = g_2g_1 + 0$ and the uniqueness part of Proposition 2.2.4, we get that $g_2 = q \in K[x]$. Thus, either $g_1 \in K[x]^{\times} \subseteq K\{x\}^{\times}$ or $g_1 \in K[x]^{\times} \subseteq K\{x\}^{\times}$. In both cases we get a contradiction.

Proof of (g): Let a be an element of K with |a| < 1. Then ax - 1 is irreducible in K[x]. On the other hand, pseudo.deg(ax - 1) = 0, so, by (c), $ax - 1 \in K\{x\}^{\times}$. In particular, ax - 1 is not irreducible in $K\{x\}$.

Proof of (h): We choose a as in the proof of (f) and consider the reducible polynomial f(x) = (ax-1)(x-1). By the proof of (f), $ax-1 \in K\{x\}^{\times}$. Next we note that pseudo.deg(x-1) = 1, so by (d) and (c), x-1 is irreducible in $K\{x\}$. Consequently, f(x) is irreducible in $K\{x\}$.

Let E = K(x) be the field of rational functions over K in the variable x. Then $K[x] \subseteq K\{x\}$ and the restriction of | | to K[x] is an absolute value. By the multiplicativity of | |, it extends to an absolute value of E. Let \hat{E} be the completion of E with respect to | | [CaF67, p. 47]. For each $\sum_{n=0}^{\infty} a_n x^n \in K\{x\}$ we have, by definition, $a_n \to 0$, hence $\sum_{n=0}^{\infty} a_n x^n = \lim_{n \to \infty} \sum_{i=0}^{n} a_i x^i$. Thus, K[x] is dense in $K\{x\}$. Since $K\{x\}$ is complete (Lemma 2.2.1(c)), this implies that $K\{x\}$ is the closure of K[x] in \hat{E} .

Remark 2.3.2:

(a) |x| = 1.

(b) Let $\overline{K} \subseteq \overline{E}$ be the residue fields of $K \subseteq E$ with respect to | |. Denote the image in \overline{E} of an element $u \in K(x)$ with $|u| \leq 1$ by \overline{u} . Then \overline{x} is transcendental over \overline{K} . Indeed, let h be a monic polynomial over \overline{K} . Choose a monic polynomial p with coefficients in the valuation ring of K such that $\bar{p} = h$. Since |p(x)| = 1, we have $h(\bar{x}) = \bar{p}(\bar{x}) \neq 0$. It follows that $\bar{K}(\bar{x})$ is the field of rational functions over \bar{K} in the variable \bar{x} and $\bar{K}(\bar{x}) \subseteq \bar{E}$. Moreover, $\bar{K}(\bar{x}) = \bar{E}$. Indeed, let $u = \frac{f(x)}{g(x)}$ with $f = \sum_{i=0}^{m} a_i x^i$, $g = \sum_{j=0}^{n} b_j x^j \neq 0$, and $a_i, b_j \in K$ such that $|u| \leq 1$. Then $\max_i |a_i| \leq \max_j |b_j|$. Choose $c \in K$ with $|c| = \max_j |b_j|$. Then replace a_i with $c^{-1}a_i$ and b_j with $c^{-1}b_j$, if necessary, to assume that $|a_i|, |b_j| \leq 1$ for all i, j and there exists k with $|b_k| = 1$. Under these assumptions, $\bar{u} = \frac{\bar{f}(\bar{x})}{\bar{q}(\bar{x})} \in \bar{K}(\bar{x})$, as claimed.

(c) If $|\cdot|'$ is an absolute value of E which coincides with $|\cdot|$ on K and the residue x' of x with respect to $|\cdot|'$ is transcendental over \bar{K} , then $|\cdot|'$ coincides with $|\cdot|$.

Indeed, let $p(x) = \sum_{i=0}^{n} a_i x^i$ be a nonzero polynomial in K[x]. Choose a $c \in K^{\times}$ with $|c| = \max_i |a_i|$. Then $(c^{-1}p(x))' = \sum_{i=0}^{n} (c^{-1}a_i)'(x')^i \neq 0$ (the prime indicates the residue with respect to ||'), hence $|c^{-1}p(x)|' = 1$, so |p(x)|' = |c| = |p(x)|.

(d) It follows from (c) that if γ is an automorphism of E that leaves K invariant, preserves the absolute value of K, and $\overline{x^{\gamma}}$ is transcendental over \overline{K} , then γ preserves the absolute value of E.

In particular, γ is ||-continuous. Moreover, if $(x_1, x_2, x_3, ...)$ is a ||-Cauchy sequence in E, then so is $(x_1^{\gamma}, x_2^{\gamma}, x_3^{\gamma}, ...)$. Hence γ extends uniquely to a continuous automorphism of the ||-completion \hat{E} of E.

(e) Now suppose K is a finite Galois extension of a complete field K_0 with respect to | | and set $E_0 = K_0(x)$. Let $\gamma \in \text{Gal}(K/K_0)$ and extend γ in the unique possible way to an element $\gamma \in \text{Gal}(E/E_0)$. Then γ preserves | | on K. Indeed, $|z|' = |z^{\gamma}|$ is an absolute valued of K. Since K_0 is complete with respect to | |, K_0 is Henselian, so | |' is equivalent to | |. Thus, there exists $\varepsilon > 0$ with $|z^{\gamma}| = |z|^{\varepsilon}$ for each $z \in K$. In particular, $|z| = |z|^{\varepsilon}$ for each $z \in K_0$, so $\varepsilon = 1$, as claimed. In addition $x^{\gamma} = x$. By (d), γ preserves | | also on E.

(f) Under the assumptions of (e) we let \hat{E}_0 and \hat{E} be the ||-completions of E and E_0 , respectively. Then $\hat{E}_0 E$ is a finite separable extension of \hat{E}_0 in \hat{E} . As such $\hat{E}_0 E$ is complete [CaF67, p. 57, Cor. 2] and contains E, so $\hat{E}_0 E = \hat{E}$. Thus, \hat{E}/\hat{E}_0 is a finite Galois extension.

By (d) and (e) each $\gamma \in \text{Gal}(E/E_0)$ extends uniquely to a continuous automorphism γ of \hat{E} . Every $x \in \hat{E}_0$ is the limit of a sequence (x_1, x_2, x_3, \ldots) of elements of E_0 . Since $x_i^{\gamma} = x_i$ for each i, we have $x^{\gamma} = x$. It follows that res: $\text{Gal}(\hat{E}/\hat{E}_0) \to \text{Gal}(E/E_0)$ is an isomorphism.

(g) Finally suppose $y = \frac{ax+b}{cx+d}$ with $a, b, c, d \in K$ such that $|a|, |b|, |c|, |d| \leq 1$ and $\bar{a}\bar{d}-\bar{b}\bar{c}\neq 0$. Then $\bar{a}\bar{x}+\bar{b}$ and $\bar{c}\bar{x}+\bar{d}$ are nonzero elements of $\bar{K}(\bar{x})$, so $\bar{y} = \frac{\bar{a}\bar{x}+\bar{b}}{c\bar{x}+\bar{d}} \in \bar{K}(\bar{x})$. Moreover, $\bar{K}(\bar{x}) = \bar{K}(\bar{y})$, hence \bar{y} is transcendental over \bar{K} . We conclude from (c) that the map $x \mapsto y$ extends to a K-automorphism of K(x) that preserves the absolute value. It therefore extends to an isomorphism $\sum a_n x^n \to \sum a_n y^n$ of $K\{x\}$ onto $K\{y\}$.

In the following theorem we refer to an equivalence class of a valuation of a field F as a **prime** of F. For each prime \mathfrak{p} we choose a valuation $v_{\mathfrak{p}}$ representing the prime and let $O_{\mathfrak{p}}$ be the corresponding valuation ring.

We say that an ultrametric absolute value | | of a field K is **discrete**, if the group of all values |a| with $a \in K^{\times}$ is isomorphic to \mathbb{Z} .

THEOREM 2.3.3: Let K be a complete field with respect to a nontrivial ultrametric absolute value | |. Then $F = \text{Quot}(K\{x\})$ is a Hilbertian field.

Proof: Let $O = \{a \in K \mid |a| \le 1\}$ be the valuation ring of K with respect to | | and let $D = O\{x\} = \{f \in K\{x\} \mid |f| \le 1\}$. Each $f \in K\{x\}$ can be written as af_1 with $a \in K$, $f_1 \in D$, and $|f_1| = 1$. Hence, Quot(D) = F.

We construct a set S of prime divisors of F that satisfies the following conditions:

- (1a) For each $\mathfrak{p} \in S$, $v_{\mathfrak{p}}$ is a real valuation (i.e. $v_{\mathfrak{p}}(F) \subseteq \mathbb{R}$).
- (1b) The valuation ring $O_{\mathfrak{p}}$ of $v_{\mathfrak{p}}$ is the local ring of D at the prime ideal $\mathfrak{m}_{\mathfrak{p}} = \{f \in D \mid v_{\mathfrak{p}}(f) > 0\}.$
- (1c) $D = \bigcap_{\mathfrak{p} \in S} O_{\mathfrak{p}}.$
- (1d) For each $f \in F^{\times}$ the set $\{\mathfrak{p} \in S \mid v_{\mathfrak{p}}(f) \neq 0\}$ is finite.
- (1e) The Krull dimension of D is at least 2.

Then D is a generalized Krull domain of dimension exceeding 1. A theorem of Weissauer [FrJ05, Thm. 15.4.6] will then imply that F is Hilbertian.

THE CONSTRUCTION OF S: The absolute value | | of $K\{x\}$ extends to an absolute value of F. The latter determines a prime \mathfrak{M} of F with a real valuation $v_{\mathfrak{M}}$ (Section 2.1). Each $u \in F$ with $|u| \leq 1$ can be written as $u = a \frac{f_1}{g_1}$ with $a \in O$ and $f_1, g_1 \in D$, $|f_1| = |g_1| = 1$. Hence, $O_{\mathfrak{M}} = D_{\mathfrak{m}}$, where $\mathfrak{m} = \{f \in D \mid |f| < 1\}$.

By Proposition 2.3.1, each nonzero prime ideal of $K\{x\}$ is generated by a prime element $p \in K\{x\}$. Divide p by its pseudo leading coefficient, if necessary, to assume that |p| = 1. Then let v_p be the discrete valuation of F determined by p and let \mathfrak{p}_p be its equivalence class. We prove that p is a prime element of D. This will prove that pD is a prime ideal of D and its local ring will coincide with the valuation ring of v_p .

Indeed, let f, g be nonzero elements of D such that p divides fg in D. Write $f = af_1, g = bg_1$ with nonzero $a, b \in O$, $f_1, g_1 \in D$, $|f_1| = |g_1| =$ 1. Then p divides f_1g_1 in $K\{x\}$ and therefore it divides, say, f_1 in $K\{x\}$. Thus, there exists $q \in K\{x\}$ with $pq = f_1$. But then |q| = 1, so $q \in D$. Consequently, p divides f in D, as desired.

Let P be the set of all prime elements p as in the paragraph before the preceding one. Then $S = \{\mathfrak{p}_p \mid p \in P\} \cup \{\mathfrak{M}\}$ satisfies (1a) and (1b).

By Proposition 2.3.1(b), $K\{x\}$ is a unique factorization domain, hence $K\{x\} = \bigcap_{p \in P} O_p$, hence $\bigcap_{\mathfrak{p} \in S} O_{\mathfrak{p}} = \{f \in K\{x\} \mid |f| \leq 1\} = D$. This settles (1c).

Next observe that for each $f \in F^{\times}$ there are only finitely many $p \in P$ such that $v_p(f) \neq 0$, so (1d) holds.

Finally note that if $f = \sum_{n=0}^{\infty} a_n x^n$ is in D, then $|a_n| \leq 1$ for all n and $|a_n| < 1$ for all large n. Hence $D/\mathfrak{m} \cong \overline{K}[\overline{x}]$, where \overline{K} and \overline{x} are as in Remark 2.3.2(b). Since \overline{x} is transcendental over \overline{K} , \mathfrak{m} is a nonzero prime ideal and $\mathfrak{m} + Ox$ is a prime ideal of D that properly contains \mathfrak{m} . This proves (1e) and concludes the proof of the theorem.

COROLLARY 2.3.4: $Quot(K\{x\})$ is not a Henselian field.

Proof: Since $K\{x\}$ is Hilbertian (Theorem 2.3.3), $K\{x\}$ can not be Henselian [FrJ08, Lemma 15.5.4].

2.4 Convergent Power Series

Let K be a complete field with respect to an ultrametric absolute value | |. We say that a formal power series $f = \sum_{n=m}^{\infty} a_n x^n$ in K((x)) converges at an element $c \in K$, if $f(c) = \sum_{n=m}^{\infty} a_n c^n$ converges, i.e. $a_n c^n \to 0$. In this case f converges at each $b \in K$ with $|b| \leq |c|$. For example, each $f \in K\{x\}$ converges at 1. We say that f converges if f converges at some $c \in K^{\times}$.

We denote the set of all convergent power series in K((x)) by $K((x))_0$ and prove that $K((x))_0$ is a field that contains $K\{x\}$ and is algebraically closed in K((x)).

LEMMA 2.4.1: A power series $f = \sum_{n=m}^{\infty} a_n x^n$ in K((x)) converges if and only if there exists a positive real number γ such that $|a_n| \leq \gamma^n$ for each $n \geq 0$.

Proof: First suppose f converges at $c \in K^{\times}$. Then $a_n c^n \to 0$, so there exists $n_0 \ge 1$ such that $|a_n c^n| \le 1$ for each $n \ge n_0$. Choose

$$\gamma = \max\{|c|^{-1}, |a_k|^{1/k} \mid k = 0, \dots, n_0 - 1\}.$$

Then $|a_n| \leq \gamma^n$ for each $n \geq 0$.

Conversely, suppose $\gamma > 0$ and $|a_n| \leq \gamma^n$ for all $n \geq 0$. Increase γ , if necessary, to assume that $\gamma > 1$. Then choose $c \in K^{\times}$ such that $|c| \leq \gamma^{-1.5}$ and observe that $|a_n c^n| \leq \gamma^{-0.5n}$ for each $n \geq 0$. Therefore, $a_n c^n \to 0$, hence f converges at c.

LEMMA 2.4.2: $K((x))_0$ is a field that contains $\operatorname{Quot}(K\{x\})$, hence also K(x).

Proof: The only difficulty is to prove that if $f = 1 + \sum_{n=1}^{\infty} a_n x^n$ converges, then also $f^{-1} = 1 + \sum_{n=1}^{\infty} a'_n x^n$ converges.

Indeed, for $n \geq 1$, a'_n satisfies the recursive relation $a'_n = -a_n - \sum_{i=1}^{n-1} a_i a'_{n-i}$. By Lemma 2.4.1, there exists $\gamma > 1$ such that $|a_i| \leq \gamma^i$ for each $i \geq 1$. Set $a'_0 = 1$. Suppose, by induction, that $|a'_j| \leq \gamma^j$ for $j = 1, \ldots, n-1$. Then $|a'_n| \leq \max_i(|a_i| \cdot |a'_{n-i}|) \leq \gamma^n$. Hence, f^{-1} converges.

Let v be the valuation of K((x)) defined by

$$v(\sum_{n=m}^{\infty} a_n x^n) = m$$
 for $a_m, a_{m+1}, a_{m+2}, \ldots \in K$ with $a_m \neq 0$

It is discrete, complete, its valuation ring is K[[x]], and v(x) = 1. The residue of an element $f = \sum_{n=0}^{\infty} a_n x^n$ of K[[x]] at v is a_0 , and we denote it by \overline{f} . We also consider the valuation ring $O = K[[x]] \cap K((x))_0$ of $K((x))_0$ and denote the restriction of v to $K((x))_0$ also by v. Since $K((x))_0$ contains K(x), it is v-dense in K((x)). Finally, we also denote the unique extension of v to the algebraic closure of K((x)) by v.

Remark 2.4.3: $K((x))_0$ is not complete. Indeed, choose $a \in K$ such that |a| > 1. Then there exists no $\gamma > 0$ such that $|a^{n^2}| \leq \gamma^n$ for all $n \geq 1$. By Lemma 2.4.1, the power series $f = \sum_{n=0}^{\infty} a^{n^2} x^n$ does not belong to $K((x))_0$. Therefore, the valued field $(K((x))_0, v)$ is not complete.

LEMMA 2.4.4: The field $K((x))_0$ is separably algebraically closed in K((x)).

Proof: Let $y = \sum_{n=m}^{\infty} a_n x^n$, with $a_n \in K$, be an element of K((x)) which is separably algebraic of degree d over $K((x))_0$. We have to prove that $y \in K((x))_0$.

PART A: A shift of y. Assume that d > 1 and let y_1, \ldots, y_d , with $y = y_1$, be the (distinct) conjugates of y over $K((x))_0$. In particular $r = \max(v(y - y_i) | i = 2, \ldots, d)$ is an integer. Choose $s \ge r + 1$ and let

$$y'_{i} = \frac{1}{x^{s}} (y_{i} - \sum_{n=m}^{s} a_{n} x^{n}), \qquad i = 1, \dots, d.$$

Then y'_1, \ldots, y'_d are the distinct conjugates of y'_1 over $K((x))_0$. Also, $v(y'_1) \ge 1$ and $y'_i = \frac{1}{x^s}(y_i - y) + y'_1$, so $v(y'_i) \le -1$, $i = 2, \ldots, d$. If y'_1 belongs to $K((x))_0$, then so does y, and conversely. Therefore, we replace y_i by y'_i , if necessary, to assume that

(1)
$$v(y) \ge 1 \text{ and } v(y_i) \le -1, \ i = 2, \dots, d$$

In particular $y = \sum_{n=0}^{\infty} a_n x^n$ with $a_0 = 0$. The elements y_1, \ldots, y_d are the roots of an irreducible separable polynomial

$$h(Y) = p_d Y^d + p_{d-1} Y^{d-1} + \dots + p_1 Y + p_0$$

with coefficients $p_i \in O$. Let $e = \min(v(p_0), \ldots, v(p_d))$. Divide the p_i , if necessary, by x^e , to assume that $v(p_i) \ge 0$ for each *i* between 0 and *d* and that $v(p_i) = 0$ for at least one *j* between 0 and *d*.

PART B: We prove that $v(p_0), v(p_d) > 0$, $v(p_k) > v(p_1)$ if $2 \le k \le d-1$ and $v(p_1) = 0$. Indeed, since v(y) > 0 and h(y) = 0, we have $v(p_0) > 0$. Since $v(y_2) < 0$ and $h(y_2) = 0$, we have $v(p_d) > 0$. Next observe that

$$\frac{p_1}{p_d} = \pm y_2 \cdots y_d \pm \sum_{i=2}^d \frac{y_1 \cdots y_d}{y_i}.$$

If $2 \le i \le d$, then $v(y_i) < v(y_1)$, so $v(y_2 \cdots y_d) < v(\frac{y_1}{y_i}) + v(y_2 \cdots y_d) = v(\frac{y_1 \cdots y_d}{y_i})$. Hence,

(2)
$$v\left(\frac{p_1}{p_d}\right) = v(y_2\cdots y_d).$$

For k between 1 and d-2 we have

(3)
$$\frac{p_{d-k}}{p_d} = \pm \sum_{\sigma} \prod_{i=1}^k y_{\sigma(i)},$$

where σ ranges over all monotonically increasing maps from $\{1, \ldots, k\}$ to $\{1, \ldots, d\}$. If $\sigma(1) \neq 1$, then $\{y_{\sigma(1)}, \ldots, y_{\sigma(k)}\}$ is properly contained in $\{y_2, \ldots, y_d\}$. Hence, $v(\prod_{i=1}^k y_{\sigma(i)}) > v(y_2 \cdots y_d)$. If $\sigma(1) = 1$, then

$$v\left(\prod_{i=1}^{k} y_{\sigma(i)}\right) > v\left(\prod_{i=2}^{k} y_{\sigma(i)}\right) > v(y_2 \cdots y_d).$$

Hence, by (2) and (3), $v(\frac{p_d-k}{p_d}) > v(\frac{p_1}{p_d})$, so $v(p_{d-k}) > v(p_1)$. Since $v(p_j) = 0$ for some j between 0 and d, since $v(p_i) \ge 0$ for every i between 0 and d, and since $v(p_0), v(p_d) > 0$, we conclude that $v(p_1) = 0$ and $v(p_i) > 0$ for all $i \ne 1$. Therefore,

(4)
$$p_k = \sum_{n=0}^{\infty} b_{kn} x^n, \qquad k = 0, \dots, d$$

with $b_{kn} \in K$ such that $b_{1,0} \neq 0$ and $b_{k,0} = 0$ for each $k \neq 1$. In particular, $|b_{1,0}| \neq 0$ but unfortunately, $|b_{1,0}|$ may be smaller than 1.

PART C: Making $|b_{1,0}|$ large. We choose $c \in K$ such that $|c^{d-1}b_{1,0}| \ge 1$ and let z = cy. Then z is a zero of the polynomial $g(Z) = p_d Z^d + cp_{d-1}Z^{d-1} + \cdots + c^{d-1}p_1Z + c^dp_0$ with coefficients in O. Relation (4) remains valid except that the zero term of the coefficient of Z in g becomes $c^{d-1}b_{1,0}$. By the choice of c, its absolute value is at least 1. So, without loss, we may assume that

(5)
$$|b_{1,0}| \ge 1.$$

PART D: An estimate for $|a_n|$. By Lemma 2.4.1, there exists $\gamma > 0$ such that $|b_{kn}| \leq \gamma^n$ for all $0 \leq k \leq d$ and $n \geq 1$. By induction we prove that $|a_n| \leq \gamma^n$ for each $n \geq 0$. This will prove that $y \in O$ and will conclude the proof of the lemma.

Indeed, $|a_0| = 0 < 1 = \gamma^0$. Now assume that $|a_m| \leq \gamma^m$ for each $0 \leq m \leq n-1$. For each k between 0 and d we have that $p_k y^k = \sum_{n=0}^{\infty} c_{kn} x^n$, where

$$c_{kn} = \sum_{\sigma \in S_{kn}} b_{k,\sigma(0)} \prod_{j=1}^{k} a_{\sigma(j)},$$

and

$$S_{kn} = \{ \sigma \colon \{0, \dots, k\} \to \{0, \dots, n\} \mid \sum_{j=0}^{k} \sigma(j) = n \}.$$

It follows that

(6)
$$c_{0n} = b_{0n}$$
 and $c_{1n} = b_{1,0}a_n + b_{11}a_{n-1} + \dots + b_{1,n-1}a_1$

For $k \ge 2$ we have $b_{k,0} = 0$. Hence, if a term $b_{k,\sigma(0)} \prod_{j=1}^{k} a_{\sigma(j)}$ in c_{kn} contains a_n , then $\sigma(0) = 0$, so $b_{k,\sigma(0)} = 0$. Thus,

(7)
$$c_{kn} = \text{sum of products of the form } b_{k,\sigma(0)} \prod_{j=1}^{k} a_{\sigma(j)},$$

with $\sigma(j) < n, \ j = 1, \dots, k.$

From the relation $\sum_{k=0}^{d} p_k y^k = h(y) = 0$ we conclude that $\sum_{k=0}^{d} c_{kn} = 0$ for all *n*. Hence, by (6),

$$b_{1,0}a_n = -b_{0n} - b_{11}a_{n-1} - \dots - b_{1,n-1}a_1 - c_{2n} - \dots - c_{dn}.$$

Therefore, by (7),

(8)
$$b_{1,0}a_n = \text{sum of products of the form } -b_{k,\sigma(0)} \prod_{j=1}^k a_{\sigma(j)},$$
with $\sigma \in S_{kn}, \ 0 \le k \le d$, and $\sigma(j) < n, \ j = 1, \dots, k$

Note that $b_{k,0} = 0$ for each $k \neq 1$ (by (4)), while $b_{1,0}$ does not occur on the right hand side of (8). Hence, for a summand in the right hand side of (8) indexed by σ we have

$$|b_{k,\sigma(0)}\prod_{j=1}^k a_{\sigma(j)}| \le \gamma^{\sum_{j=0}^k \sigma(j)} = \gamma^n.$$

We conclude from $|b_{1,0}| \ge 1$ that $|a_n| \le \gamma^n$, as contended.

PROPOSITION 2.4.5: The field $K((x))_0$ is algebraically closed in K((x)). Thus, each $f \in K((x))$ which is algebraic over K(x) converges at some $c \in K^{\times}$. Moreover, there exists a positive integer m such that f converges at each $b \in K^{\times}$ with $|b| \leq \frac{1}{m}$.

Proof: In view of Lemma 2.4.4, we have to prove the proposition only for char(K) > 0. Let $f = \sum_{n=m}^{\infty} a_n x^n \in K((x))$ be algebraic over $K((x))_0$. Then $K((x))_0(f)$ is a purely inseparable extension of a separable algebraic extension of $K((x))_0$. By Lemma 2.4.4, the latter coincides with $K((x))_0$. Hence, $K((x))_0(f)$ is a purely inseparable extension of $K((x))_0$.

Thus, there exists a power q of char(K) such that $\sum_{n=m}^{\infty} a_n^q x^{nq} = f^q \in K((x))_0$. By Lemma 2.4.1, there exists $\gamma > 0$ such that $|a_n^q| \leq \gamma^{nq}$ for all $n \geq 1$. It follows that $|a_n| \leq \gamma^n$ for all $n \geq 1$. By Lemma 2.4.1, $f \in K((x))_0$, so there exists $c \in K^{\times}$ such that f converges at c. If $\frac{1}{m} \leq |c|$, then f converges at each $b \in K^{\times}$ with $|b| \leq \frac{1}{m}$.

COROLLARY 2.4.6: The valued field $(K((x))_0, v)$ is Henselian.

Proof: Consider the valuation ring $O = K[[x]] \cap K((x))_0$ of $K((x))_0$ at v. Let $f \in O[X]$ be a monic polynomial and $a \in O$ such that v(f(a)) > 0 and $v(f'(a)) \neq 0$. Since (K((x)), v) is Henselian, there exists $z \in K[[x]]$ such that f(z) = 0 and v(z - a) > 0. By Proposition 2.4.5, $z \in K((x))_0$, hence $z \in O$. It follows that $(K((x))_0, v)$ is Henselian.

2.5 The Regularity of $K((x))/K((x))_0$

Let K be a complete field with respect to an ultrametric absolute value | |. We extend | | in the unique possible way to \tilde{K} . We also consider the discrete valuation v of K(x)/K defined by v(a) = 0 for each $a \in K^{\times}$ and v(x) = 1. Then K((x)) is the completion of K(x) at v. Let $K((x))_0$ be the subfield of K((x)) of all convergent power series.

Proposition 2.4.5 states that $K((x))_0$ is algebraically closed in K((x)). In this section we prove that K((x)) is even a regular extension of $K((x))_0$. To do this, we only have to assume that $p = \operatorname{char}(K) > 0$ and prove that $K((x))/K((x))_0$ is a separable extension. In other words, we have to prove that K((x)) is linearly disjoint from $K((x))_0^{1/p}$ over $K((x))_0$. We do that in several steps.

LEMMA 2.5.1: The fields K((x)) and $K((x^{1/p}))_0$ are linearly disjoint over $K((x))_0$.

Proof: First note that $1, x^{1/p}, \ldots, x^{p-1/p}$ is a basis for $K(x^{1/p})$ over K(x). Then $1, x^{1/p}, \ldots, x^{p-1/p}$ have distinct v-values modulo $\mathbb{Z} = v(K((x)))$, so they are linearly independent over K((x)).

Next we observe that $1, x^{1/p}, \ldots, x^{p-1/p}$ also generate $K((x^{1/p}))$ over K((x)). Indeed, each $f \in K((x^{1/p}))$ may be multiplied by an appropriate

power of x to be presented as

(1)
$$f = \sum_{n=0}^{\infty} a_n x^{n/p},$$

with $a_0, a_1, a_2, \ldots \in K$. We write each n as n = kp + l with integers $k \ge 0$ and $0 \le l \le p - 1$ and rewrite f as

(2)
$$f = \sum_{l=0}^{p-1} \left(\sum_{k=0}^{\infty} a_{kp+l} x^k \right) x^{l/p}.$$

If $f \in K((x^{1/p}))_0$, then there exists $b \in K^{\times}$ such that $\sum_{n=0}^{\infty} a_n b^{n/p}$ converges in K, hence $a_n b^{n/p} \to 0$ as $n \to \infty$, so $a_{kp+l} b^k b^{l/p} \to 0$ as $k \to \infty$ for each l. Therefore, for each l, we have $a_{kp+l} b^k \to 0$ as $k \to \infty$, hence $\sum_{k=0}^{\infty} a_{kp+l} x^k$ converges, so belongs to $K((x))_0$.

It follows that $1, x^{1/p}, \ldots, x^{p-1/p}$ form a basis for $K((x^{1/p}))_0/K((x))_0$ as well as for $K((x^{1/p}))/K((x))$. Consequently, K((x)) is linearly disjoint from $K((x^{1/p}))_0$ over $K((x))_0$.

We set $K[[x]]_0 = K[[x]] \cap K((x))_0$.

LEMMA 2.5.2: Let $u_1, \ldots, u_m \in \tilde{K}[[x]]_0$ and $f_1, \ldots, f_m \in K[[x]]$. Set $u_{i0} = u_i(0)$ for $i = 1, \ldots, m$ and

(3)
$$f = \sum_{i=1}^{m} f_i u_i.$$

Suppose u_{10}, \ldots, u_{m0} are linearly independent over K, $f \in \tilde{K}[[x]]_0$, and f(0) = 0. Then $f_1, \ldots, f_m \in K[[x]]_0$.

Proof: We break up the proof into several parts.

PART A: Comparison of norms. We consider the K-vector space $V = \sum_{i=1}^{m} K u_{i0}$ and define a function $\mu: V \to \mathbb{R}$ by

(4)
$$\mu(\sum_{i=1}^{m} a_i u_{i0}) = \max(|a_1|, \dots, |a_m|).$$

It satisfies the following rules:

(5a) $\mu(v) > 0$ for each nonzero $v \in V$.

(5b) $\mu(v+v') \le \max(\mu(v), \mu(v'))$ for all $v, v' \in V$.

(5c) $\mu(av) = |a|\mu(v)$ for all $a \in K$ and $v \in V$.

Thus, v is a **norm** of V. On the other hand, | | extends to an absolute value of \tilde{K} and its restriction to V is another norm of V. Since K is complete under | |, there exists a positive real number s such that

(6) $\mu(v) \le s|v|$ for all $v \in V$

[CaF67, p. 52, Lemma].

PART B: Power series. For each *i* we write $u_i = u_{i0} + u'_i$ where $u'_i \in \tilde{K}[[x]]_0$ and $u'_i(0) = 0$. Then

(7a)
$$f = \sum_{n=1}^{\infty} a_n x^n \quad \text{with } a_1, a_2, \dots \in \tilde{K},$$

(7b)
$$u'_{i} = \sum_{n=1}^{\infty} b_{in} x^{n} \quad \text{with } b_{i1}, b_{i2}, \ldots \in \tilde{K}, \text{ and}$$

(7c)
$$f_i = \sum_{n=0}^{\infty} a_{in} x^n$$
 with $a_{i0}, a_{i1}, a_{i2}, \ldots \in K$.

If a power series converges at a certain element of \tilde{K}^{\times} , it converges at each element with a smaller absolute value. Since to each element of \tilde{K}^{\times} there exists an element of K^{\times} with a smaller absolute value, there exists $d \in K^{\times}$ such that $\sum_{n=1}^{\infty} a_n d^n$ and $\sum_{n=1}^{\infty} b_{in} d^n$, $i = 1, \ldots, m$, converge. In particular, the numbers $|a_n d^n|$ and $|b_{in} d^n|$ are bounded. It follows from the identities $|a_n c^n| = |a_n d^n| \cdot |\frac{c}{d}|^n$ and $|b_{in} c^n| = |b_{in} d^n| \cdot |\frac{c}{d}|^n$ that there exists $c \in K^{\times}$ such that

(8)
$$\max_{n \ge 1} |a_n c^n| \le s^{-1}$$
 and $\max_{n \ge 1} |b_{in} c^n| \le s^{-1}$

for i = 1, ..., m.

PART C: Claim: $|a_{in}c^n| \leq 1$ for i = 1, ..., m and n = 0, 1, 2, ... To prove the claim we substitute the presentations (7) of f, u'_i, f_i in the relation (3) and get:

(9)
$$\sum_{n=1}^{\infty} a_n x^n = \sum_{n=0}^{\infty} \sum_{j=1}^m a_{jn} u_{j0} x^n + \sum_{n=1}^{\infty} \sum_{j=1}^m \sum_{k=0}^{n-1} a_{jk} b_{j,n-k} x^n.$$

In particular, for n = 0 we get $0 = \sum_{j=1}^{m} a_{j0}u_{j0}$. Since u_{10}, \ldots, u_{m0} are linearly independent over K and $a_{10}, \ldots, a_{m0} \in K$, we get $a_{10} = \cdots = a_{m0} = 0$, so our claim holds in this case.

Proceeding by induction, we assume $|a_{ik}c^k| \leq 1$ for $i = 1, \ldots, m$ and $k = 0, \ldots, n-1$. By (5) and (6),

$$|a_{in}| \le \max(|a_{1n}|, \dots, |a_{mn}|) = \mu(\sum_{j=1}^m a_{jn}u_{j0}) \le s|\sum_{j=1}^m a_{jn}u_{j0}|,$$

hence

(10)
$$|a_{in}c^n| \le s |\sum_{j=1}^m a_{jn}u_{j0}c^n|.$$

Next we compare the coefficients of x^n on both sides of (9),

$$a_n = \sum_{j=1}^m a_{jn} u_{j0} + \sum_{j=1}^m \sum_{k=0}^{n-1} a_{jk} b_{j,n-k},$$

change sides and multiply the resulting equation by c^n :

$$\sum_{j=1}^{m} a_{jn} u_{j0} c^{n} = a_{n} c^{n} - \sum_{j=1}^{m} \sum_{k=0}^{n-1} a_{jk} c^{k} \cdot b_{j,n-k} c^{n-k}.$$

By the induction hypothesis and by (8),

(11)
$$\left|\sum_{j=1}^{m} a_{jn} u_{j0} c^{n}\right| \leq \max\left(\left|a_{n} c^{n}\right|, \max_{1 \leq j \leq m} \max_{0 \leq k \leq n-1} \left|a_{jk} c^{k}\right| \cdot \left|b_{j,n-k} c^{n-k}\right|\right)$$

 $\leq \max(s^{-1}, 1 \cdot s^{-1}) = s^{-1}$

It follows from (10) and (11) that $|a_{in}c^n| \leq 1$. This concludes the proof of the claim.

PART D: End of the proof. We choose $a \in K^{\times}$ such that |a| < |c|. Then $|a_{in}a^n| = |a_{in}c^n(\frac{a}{c})^n| \le |\frac{a}{c}|^n$. Since the right hand side tends to 0 as $n \to \infty$, so does the left hand side. We conclude that f_i converges at a.

LEMMA 2.5.3: The fields K((x)) and $K^{1/p}((x))_0$ are linearly disjoint over $K((x))_0$.

Proof: We have to prove that every finite extension F' of $K((x))_0$ in $K^{1/p}((x))_0$ is linearly disjoint from K((x)) over $K((x))_0$.

If $F' = K((x))_0$, there is nothing to prove, so we assume F' is a proper extension of K((x)). Each element $f' \in F'$ has the form $f' = \sum_{i=k}^{\infty} b_i x^i$ with $b_i \in K^{1/p}$ and $\sum_{i=k}^{\infty} b_i c^i$ converges for some $c \in (K^{1/p})^{\times}$. Thus, $(f')^p = \sum_{i=k}^{\infty} b_i^p x^{ip} \in K((x))$ and $\sum_{i=k}^{\infty} b_i^p (c^p)^i$ converges, so $(f')^p \in K((x))_0$. We may therefore write F' = F(f), where F is a finite extension of $K((x))_0$ in F' and [F':F] = p.

By induction on the degree, F is linearly disjoint from K((x)) over $K((x))_0$. Let $m = [F : K((x))_0]$.

Moreover, K((x)) is the completion of K(x), so also of $K((x))_0$. Hence, $\hat{F} = K((x))F$ is the completion of F under v. By the linear disjointness, $[\hat{F}:K((x))] = m$.

The residue field of K((x)) and of $K((x))_0$ is K and the residue field of \hat{F} is equal to the residue field \bar{F} of F. Both K((x)) and $K^{1/p}((x))$ have the same valuation group under v, namely \mathbb{Z} . Therefore, also $v(\hat{F}^{\times}) = \mathbb{Z}$, so $e(\hat{F}/K((x))) = 1$. Since K((x)) is complete and discrete, $[\hat{F} : K((x))] =$ $e(\hat{F} : K((x)))[\bar{F} : K] = [\bar{F} : K]$ [CaF65, p. 19, Prop. 3]. Notes

Now we choose a basis u_{10}, \ldots, u_{m0} for \overline{F}/K and lift each u_{i0} to an element u_i of $F \cap \tilde{K}[[x]]_0$. Then, u_1, \ldots, u_m are linearly independent over $K((x))_0$ and over K((x)), hence they form a basis for $F/K((x))_0$ and for $\hat{F}/K((x))$.

As before, $\widehat{F'} = K((x))F'$ is the completion of F'. Again, both F' and $\widehat{F'}$ have the same residue field $\overline{F'}$ and $[\widehat{F'}:\widehat{F}] = [\overline{F'}:\overline{F}]$. Note that $\overline{F'} \subseteq K^{1/p}$ and $[\overline{F'}:\overline{F}] \leq [F':F] = p$. Therefore, $\overline{F'} = \overline{F}$ or $[\overline{F'}:\overline{F}] = p$.

In the first case $f \in \hat{F}$, so by the paragraph before the preceding one, there exist $f_1, \ldots, f_m \in K((x))$ such that $f = \sum_{i=1}^m f_i u_i$. Multiplying both sides by a large power of x, we may assume that $f_1, \ldots, f_m \in K[[x]]$ and f(0) = 0. By Lemma 2.5.2, $f_1, \ldots, f_m \in K((x))_0$, hence $f \in F$. This contradiction to the choice of f implies that $[\overline{F'}:\overline{F}] = p$. Hence, [K((x))F': $K((x))F] = [\widehat{F'}:\widehat{F}] = p = [F':F]$. This implies that \widehat{F} and F' are linearly disjoint over F. By the tower property of linear disjointness, K((x)) and F'are linearly disjoint over $K((x))_0$, as claimed. \Box

PROPOSITION 2.5.4: Let K be a complete field under an ultrametric absolute value | | and denote the field of all convergent power series in x with coefficients in K by $K((x))_0$. Then K((x)) is a regular extension of $K((x))_0$.

Proof: In view of Proposition 2.4.5, it suffices to assume that $p = \operatorname{char}(K) > 0$ and to prove that K((x)) is linearly disjoint from $K((x))_0^{1/p}$ over $K((x))_0$.

Indeed, by Lemma 2.5.3, K((x)) is linearly disjoint from $K^{1/p}((x))_0$ over $K((x))_0$. Next observe that $K^{1/p}$ is also complete under ||. Hence, by Lemma 2.5.1, applied to $K^{1/p}$ rather than to K, $K^{1/p}((x))$ is linearly disjoint from $K^{1/p}((x^{1/p}))_0$ over $K^{1/p}((x))_0$.

Finally we observe that $K((x))_0^{1/p} = K^{1/p}((x^{1/p}))_0$ to conclude that K((x)) is linearly disjoint from $K((x))_0^{1/p}$ over $K((x))_0$.

Notes

The rings of convergent power series in one variable introduced in Section 2.2 are the rings of holomorphic functions on the closed unit disk that appear in [FrP04, Example 2.2]. Weierstrass Divison Theorem (Proposition 2.2.4) appears in [FrP, Thm. 3.1.1]. Our presentation follows the unpublished manuscript [Har05].

Proposition 2.4.5 appears as [Art67, p. 48, Thm. 14]. The proof given by Artin uses the method of Newton polynomials.

The property of $K\{x\}$ of being a principle ideal domain appears in [FrP, Thm. 2.2.9].

The proof that $K((x))/K((x))_0$ is a separable extension (Proposition 2.5.4) is due to Kuhlmann and Roquette [KuR96].



http://www.springer.com/978-3-642-15127-9

Algebraic Patching Jarden, M. 2011, XXIV, 292 p., Hardcover ISBN: 978-3-642-15127-9