Master-Arbeit

Die Tilting-Äquivalenz für perfektoide Körper

Von der Fakultät für Mathematik der Universität Duisburg-Essen
zur Erlangung des akademischen Titels Master of Science Mathematik

von

Anna Katharina Janiszczak

DS02258256

Betreuer und Erstprüfer: Prof. Dr. Kohlhaase

Zweitprüfer: Prof. Dr. Paskunas

Danksagung

An dieser Stelle möchte ich mich bei allen bedanken, die mich bei dieser Masterarbeit und meinem Studium unterstützt haben. Dabei gilt zunächst mein Dank Herrn Prof. Kohlhaase für die interessante Themenstellung und seine Betreuung meiner Masterarbeit.
Außerdem möchte ich meinen Eltern meinen besonderen Dank aussprechen, welche mir stets mit Rat und Tat zur Seite standen.

Inhaltsverzeichnis

0 Einleitung

Im Jahr 1979 bewiesen Fontaine und Wintenberger [2], dass die Galoisgruppen der Vervollständigung von $\mathbb{Q}_p[\mu_{p^\infty}]$ und die Galoisgruppen der Vervollständigung von $\bigcup_{n\in\mathbb{N}} \mathbb{F}_p((t))[t^{\frac{1}{p^n}}]$ isomorph sind. Später wurde diese Aussage von Scholze verallgemeinert [1]. Diese Verallgemeinerung besagt, dass die Galoisgruppen eines perfektoiden Körpers K und seines sogenannten Tilts $K^\flat$ isomorph sind. Ein Körper K mit einem nicht-archimedischen Absolutbetrag $|\cdot|$ und Restklassenkörper der Charakteristik p ist perfektoid, wenn er vollständig ist, $|K^\times|$ dicht in $\mathbb{R}_{\geqslant 0}$ liegt und der Frobenius auf $\mathcal{O}_K/p\mathcal{O}_K$ surjektiv ist. Der Tilt von K ist der Quotientenkörper des Rings $\mathcal{O}_{K^\flat} := \{(a_n)_{n\geqslant 0} \in \prod_{n\geqslant 0} \mathcal{O}_K/p\mathcal{O}_K : a_{n+1}^p = a_n\}$, wobei $\mathcal{O}_K$ der Bewertungsring des Körpers K bzgl. seines nicht-archimedischen Absolutbetrags ist. Dieser ist ein perfektoider Körper der Charakteristik p.
Die vorliegende Arbeit handelt von der Tilting-Äquivalenz zwischen den endlichen Körpererweiterungen eines perfektoiden Körpers K und den endlichen Körpererweiterungen seines Tilts $K^\flat$. Darüberhinaus wird gezeigt, dass $L|K$ genau dann Galois ist, wenn $L^\flat|K^\flat$ Galois und $Gal(L|K)$ isomorph zu $Gal(L^\flat|K^\flat)$ ist. Zunächst muss dazu bewiesen werden, dass für endliche Körpererweiterungen $L|K$ auch der Körper L ein perfektoider Körper ist. Im Fall $char(K) = p$ ist dies relativ leicht zu sehen, jedoch für den Fall $char(K) = 0$ ist dies nicht unmittelbar klar. Für einen perfektoiden Körper F der Charakteristik p lässt sich mithilfe des Rings der Wittvektoren mit Koeffizienten in F, welcher mit $W(F)$ bezeichnet wird, ein perfektoider Körper der Charakteristik 0 konstruieren, sodass sein Tilt isomorph ist zu F. Die Elemente des Rings sind Folgen, dessen Folgenglieder in F liegen. Für die Konstruktion eines perfektoiden Körpers der Charaktersitik 0 aus F wird ein spezielles Element aus $W(\mathcal{O}_F)$ gewählt und das davon erzeugte Ideal aus $W(\mathcal{O}_F)$ herausfaktorisiert. Der Tilt des Quotientenkörper dieses Rings ist isomorph zu F. Andererseits gibt es für einen perfektoiden Körper K der Charakteristik 0 einen Isomorphismus $W(\mathcal{O}_{K^\flat})/zW(\mathcal{O}_{K^\flat}) \cong \mathcal{O}_K$, wobei z Erzeuger des Kernes eines gewissen surjektiven Ringhomomorphismus $\vartheta : W(\mathcal{O}_{K^\flat}) \to \mathcal{O}_K$ ist. Dadurch ist die Abbildung $\{E : E|K\text{endl. Körpererw. }\} \to \{E' : E'|K^\flat\text{endl. Körpererw.}\}, E \mapsto E^\flat$ bijektiv.
Ein wichtiges Ziel dieser Arbeit war die Beweisstrategien transparent darzustellen und die Beweise detailliert auszuführen. Grundlegend waren dazu die Vorlesung „p-adic Galois representations “ von Herrn Prof. Dr. Kohlhaase und die Arbeit „New methods for (φ, Γ)-modules “ von Kiran Kedlaya [7]. Zunächst werden im ersten Kapitel die Grundlagen besprochen. Da perfektoide Körper einen nicht-archimedischen Absolutbetrag besitzen, werden Absolutbeträge und die daraus resultierenden Bewertungsringe thematisiert. Darüberhinaus beschäftigt man sich mit der Vervollständigung eines Körpers mit nicht-archimedischen Absolutbetrag und der Fortsetzung eines nicht-archimedischen Absolutbetrags eines vollständigen Körpers mithilfe der Körpernorm. Der projektive Limes wird im Abschluss des Kapitels besprochen. Vor allem bei der Vollständigkeitsfrage bestimmter Ringe ist dieser hilfreich. Das zweite Kapitel handelt von dem Tilt eines perfektoiden Körpers. Dort wird gezeigt, dass auch der Tilt ein perfektoider Körper ist und das Tilting funktoriell ist. Im dritten Kapitel wird eine neue Ringstruktur auf $B^{\mathbb{N}}$ für einen Ring B definiert. Diese heißt „Ring der Wittvektoren mit Koeffizienten in B “ welche im darauffolgenden Kapitel eine große Rolle spielt, denn wie oben schon erwähnt wurde ist diese ein Werkzeug zur Konstruktion eines perfektoiden Körpers der Charakteristik 0 aus einem perfektoiden Körper der Charakteristik p. Darüberhinaus wird im vierten Kapitel die Isomorphie zwischen dem Tilt des konstruierten Körpers und dem zugrunde liegenden Körper überprüft. Im letzten Kapitel wird gezeigt, dass für endliche Körpererweiterungen eines perfektoiden Körpers der Charakteristik 0 der Erweiterungskörper auch perfektoid und das Tilting graderhaltend und bijektiv

ist. Abschließend wird bewiesen, dass eine endliche Körpererweiterung $L|K$ eines perfektoiden Körpers K der Charakteristik 0 genau dann Galois ist, wenn $L^\flat|K^\flat$ Galois ist. Darüberhinaus sind ihrer Galoisgruppen isomorph.

Abschließend ist noch zur Notation Folgendes zu bemerken. Sei R ein Ring und I ein Ideal in R. Mit $q_{R,I}$ wird in dieser Arbeit stets die Quotientenabbildung $q_{R,I} : R \to R/I, \quad r \mapsto r + I$ bezeichnet. Mit pr_i wird die Projektion bezeichnet, welche eine Folge auf sein i-tes Folgenglied abbildet. Fortsetzungen und Einschränkungen von Homomorphismen werden zur Vereinfachung in dieser Arbeit mit dem gleichen Homomorphismus bezeichnet. Ist zwischen zwei Körpern K und L ein Körperhomomorphismus $K \to L$ gegeben, so wird K einfachheitshalber als Unterkörper von L aufgefasst. Für zwei Körperelemente $a, b \in K$ sind ab^{-1} und $\frac{a}{b}$ gleichbedeutend.

1 Grundlagen

Basis für die Ausführung der Unterkapitel 1.2 , 1.3 und 1.4 ist [4] Kapitel 2. Grundlegend für 1.5 war die Vorlesung „p-adic Galois representations " von Herrn Prof. Dr. Kohlhaase.

1.1 Allgemeines zu Ringen

Lemma 1.1.1
Sei R ein Integritätsring.

i) Ist $char(R) = p \neq 0$ und I ein echtes Ideal von R, so ist $char(R/I) = p$.

ii) Sei I ein Ideal von R. Ist die Charaktersitik von R/I eine Primzahl p, so ist $char(R) = p$ oder $char(R) = 0$.

Beweis: i) Da R ein Integritätsring ist, ist seine Charaktersitik eine Primzahl. Angenommen es gilt $char(R/I) = n < p$. Dann ist $p = nr + s$ mit $0 < s < n$. Dies impliziert $s + I = p + I - rn + I = 0 + I$. Das ist ein Widerspruch zu $char(R/I) = n$.
ii) Angenommen $char(R) = q > p$ und $char(R/I) = p$. Dann gibt es $r, s \in \mathbb{N}$ mit $q = pr + s$ und $0 < s < p$. Dann ist $0 + I = pr + I + s + I = s + I$ und somit ist $char(R/I) \leqslant s < p$. Dies widerspricht $char(R/I) = p$. □

Lemma 1.1.2
Seien R ein kommutativer Ring mit Eins , p eine Primzahl und I ein Ideal mit $p1 \in I$. Seien ferner $a, b \in R$ und $m \in \mathbb{N}$ mit $a \equiv b \mod I^m$. Dann ist $a^{p^n} \equiv b^{p^n} \mod I^{m+n}$ für alle $n \in \mathbb{N}$.

Beweis: Der Beweis verläuft induktiv über n. Sei also $n = 1$ und $P(X, Y) := \sum_{i=0}^{p-1} X^i Y^{p-1-i} \in \mathbb{Z}[X, Y]$. Dann ist $P(a, b) \equiv P(a, a) = pa^{p-1} \mod I^m$ und somit $P(a, b) \in I$, da $pa^{p-1} \in I$. Es ergibt sich also $a^p - b^p = (a - b)P(a, b) \in I^m I$.
Gelte die Aussage für $n \geqslant 0$. Damit ist nach Voraussetzung einerseits $a \equiv b \mod I^m$ und andererseits $a^{p^n} \equiv b^{p^n} \mod I^{m+n}$. Es ergibt sich insgesamt $(a^{p^n})^{p^1} \equiv (b^{p^n})^{p^1} \mod I^{m+n+1}$, also $a^{p^{n+1}} \equiv b^{p^{n+1}} \mod I^{m+n+1}$. □

Sei R ein kommutativer Ring mit Eins. Besitzt R genau ein maximales Ideal, so heißt R **lokaler Ring**. Offensichtlich ist die Menge aller Nichteinheiten von R das maximale Ideal, denn ein von einer Nichteinheit erzeugtes Ideal liegt in diesem maximalen Ideal.
Für eine Nichteinheit $x \in R$ ist das Element $1-x$ eine Einheit. Angenommen $1-x$ ist eine Nichteinheit, so ist auch $1 - x + x = 1$ eine Nichteinheit.

Lemma 1.1.3
Sei R ein lokaler Ring, dessen maximales Ideal $\mathfrak{m} = mR$ ein Hauptideal ist und für den $\bigcap_{j \in \mathbb{N}} \mathfrak{m}^j = 0$ ist. Dann ist jedes von Null verschiedene Ideal $\mathfrak{a}$ von der Form $\mathfrak{m}^j := m^j R$ für ein $j \in \mathbb{N}$.

Beweis: Für ein Element $r \in R \backslash \{0\}$ gibt es genau ein $n \in \mathbb{N}$ mit $r \in \mathfrak{m}^n \backslash \mathfrak{m}^{n+1}$, da $\bigcap_{j \in \mathbb{N}} \mathfrak{m}^j = 0$ und $r \neq 0$ ist. Es gilt dann $r = m^n u$ mit $u \in R \backslash \mathfrak{m} = R^\times$. Sei $\mathfrak{a} \neq 0$ ein Ideal . Wählt man $r \in \mathfrak{a} \backslash \{0\}$ und schreibt man $r = m^n u$ wie oben, so folgt $m^n \in \mathfrak{a}$. Nun wähle $n \in \mathbb{N}$ minimal mit $m^n \in \mathfrak{a}$. Damit gilt

die Inklusion $\mathfrak{m}^n \subseteq \mathfrak{a}$.
Sei $x \in \mathfrak{a} \backslash \{0\}$. Dann gibt es genau ein $s \in \mathbb{N}$ mit $x \in \mathfrak{m}^s \backslash \mathfrak{m}^{s+1}$. Wegen der Minimalität von n gilt $s \geqslant n$. Also gibt es ein $r_2 \in R$ mit $x = m^n r_2$ und somit ist $\mathfrak{a} \subseteq \mathfrak{m}^n$. □

1.2 Absolutbeträge und Bewertungen

Ein **Absolutbetrag** eines Körpers K ist eine Funktion $|\cdot| : K \to \mathbb{R}_{\geqslant 0}$ mit folgenden Eigenschaften:

i) $|x| = 0 \Leftrightarrow x = 0$

ii) $|xy| = |x||y|$ für alle $x, y \in K$

iii) $|x + y| \leqslant |x| + |y|$ für alle $x, y \in K$ (Dreiecksungleichung)

Er heißt **nicht-archimedisch**, wenn zusätzlich die verschärfte Dreiecksungleichung

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

für alle $x, y \in K$ gilt. Im Folgenden bezeichnet $(K, |\cdot|)$ einen Körper K mit einem Absolutbetrag $|\cdot|$ und heißt **bewerteter Körper**. Ist der Absolutbetrag nicht-archimedisch, so sagt man, dass $(K, |\cdot|)$ ein **nicht-archimedischer Körper** ist.
Folgendes sind Absolutbeträge.

Beispiel 1.2.1

i)
$$|x| := \begin{cases} 1 & , \quad x \in K \backslash \{0\} \\ 0 & , \quad x = 0 \end{cases}$$

ii) Sei $K \in \{\mathbb{Q}, \mathbb{R}\}$.
$$|x|_K := \begin{cases} x & , \quad x \geqslant 0 \\ -x & , \quad x < 0 \end{cases}$$

Der Absolutbetrag in Beispiel i) wird auch **trivialer Absolutbetrag** genannt.

Lemma 1.2.2
Sei $(K, |\cdot|)$ ein bewerteter Körper. Dann gilt $\big|\, |x| - |y| \,\big|_{\mathbb{R}} \leqslant |x - y|$.

Beweis: Es gelten $|x| \leqslant |x - y| + |y|$ und $|y| \leqslant |x| + |x - y|$. Damit ist $|x| - |y| \leqslant |x - y|$ und $-(|x| - |y|) \leqslant |x - y|$. Also gilt $\big|\, |x| - |y| \,\big|_{\mathbb{R}} \leqslant |x - y|$. □

Sei $(K, |\cdot|)$ ein Körper. Mit $d(x, y) := |x - y|$ wird K zu einem metrischen und somit zu einem topologischen Raum.
Für einen Absolutbetrag $|\cdot|$ ist $|1| = 1$, da $|1| = |1 \cdot 1| = |1||1|$ und $|1| \neq 0$.

Zwei Absolutbeträge von K heißen **äquivalent**, wenn sie die gleiche Topologie auf K definieren.

Lemma 1.2.3
Zwei Absolutbeträge $|\cdot|_1$ *und* $|\cdot|_2$ *von* K *sind genau dann äquivalent, wenn* $|x|_1 = |x|_2^s$ *für alle* $x \in K$ *mit festem* $s \in \mathbb{R}_{>0}$ *ist.*

Beweis: Seien $|\cdot|_1$ und $|\cdot|_2$ äquivalent. Dies impliziert, dass die Mengen der konvergenten Folgen, bzw. die Mengen der Nullfolgen bzgl. $|\cdot|_1$ und $|\cdot|_2$ gleich sind. Sei zunächst $|\cdot|_1$ der triviale Absolutbetrag. Eine Folge $(x_n)_{n\geqslant 0}$ konvergiert bzgl. $|\cdot|_1$ genau dann gegen x, wenn ein $N \in \mathbb{N}$ existiert, sodass $x_m = x$ ist für alle $m \geqslant N$. Angenommen $|\cdot|_2$ ist nicht trivial. Dann gibt es ein $x \in K$ mit $0 < |x|_2 < 1$. Die Folge $(x^n)_{n\geqslant 0}$ ist eine Nullfolge, welche bzgl $|\cdot|_1$ nicht konvergiert. Das steht im Widerspruch zur Äquivalenz. In diesem Fall ist $s = 1$.
Seien nun beide Absolutbeträge nicht trivial.
Für einen Absolutbetrag $|\cdot|$ ist die Folge $(x^n)_{n\geqslant 0}$ genau dann eine Nullfoge bzgl. $|\cdot|$, wenn $|x| < 1$ ist. Damit ist also für $|x|_1 < 1$ die Folge $(x^n)_{n\geqslant 0}$ eine Nullfolge bzgl. $|\cdot|_1$ und somit eine Nullfolge bzgl. $|\cdot|_2$. Folglich ist $|x|_2 < 1$.
Sei $y \in K$ mit $|y|_1 > 1$ und $x \in K\backslash\{0\}$. Dann ist $|x|_1 = |y|_1^\beta$ für ein $\beta \in \mathbb{R}$, da $f : \mathbb{R} \to \mathbb{R}_{>0},\ z \mapsto a^z$ mit festem $a \in \mathbb{R}_{>0}\backslash\{1\}$ eine stetige und bijektive Abbildung ist. Sei $(\frac{m_i}{n_i})_{i\geqslant 0}$ mit $n_i > 0$ rationale Folge, die von oben gegen β konvergiert. Dann ist $|x|_1 = |y|_1^\beta < |y|_1^{\frac{m_i}{n_i}}$. Aufgrund der zweiten Eigenschaft eines Absolutbetrags folgt $|\frac{x^{n_i}}{y^{m_i}}|_1 < 1$ und wegen der Äquivalenz ist $|\frac{x^{n_i}}{y^{m_i}}|_2 < 1$. Damit ergibt sich $|x|_2 < |y|_2^{\frac{m_i}{n_i}}$. Wegen der Stetigkeit der Abbildung f gilt $|x|_2 \leqslant |y|_2^\beta$. Analog folgt $|x|_2 \geqslant |y|_2^\beta$ und somit ist $|x|_2 = |y|_2^\beta$. Sei $s := \frac{\log|y|_1}{\log|y|_2}$. Dann ist $|x|_1 = |x|_2^s$ für alle $x \in K\backslash\{0\}$, da nach o.g. stets $\frac{\log|x|_1}{\log|x|_2} = \frac{\log|y|_1}{|y|_2}$ gilt.
Existiere nun umgekehrt ein $s \in \mathbb{R}_{>0}$ mit $|x|_1 = |x|_2^s$ für alle $x \in K$. Sei zunächst $|\cdot|_1$ der triviale Absolutbetrag. Dann gilt für alle $x \in K\backslash\{0\}$, dass $1 = |x|_1 = |x|_2^s$ ist. Damit ist $|x|_2 = |y|_2$ für alle $x, y \in K\backslash\{0\}$ und somit $|x|_2 = |1|_2 = 1$. In diesem Fall wird also offensichtlich die Äquivalenz der beiden Absolutbeträge erfüllt.
Seien beide Absolutbeträge nicht trivial mit $|x|_1 = |x|_2^s$ für ein $s \in \mathbb{R}_{>0}$ und sei U eine offene Menge bzgl. $|\cdot|_1$ und $x \in U$. Dann gibt es ein $\epsilon > 0$, sodass $B_{|\cdot|_1}(x,\epsilon) := \{y \in K : |x-y|_1 < \epsilon\} = \{y \in K : |x-y|_2^s < \epsilon^s\} = \{y \in K : |x-y|_2 < \epsilon^{s^{-1}}\} = B_{|\cdot|_2}(x, \epsilon^{s^{-1}}) \subseteq U$. Die Menge U ist also auch eine offene Menge bzgl. $|\cdot|_2$. Umgekehrte Inklusion folgt analog. □

Lemma 1.2.4
Seien $|\cdot|_1$ *und* $|\cdot|_2$ *nicht-triviale Absolutbeträge von* K*. Die beiden Absolutbeträge sind genau dann äquivalent, wenn für* $x \in K$ *mit* $|x|_1 < 1$ *folgt, dass* $|x|_2 < 1$ *ist.*

Beweis: Die erste Implikation folgt aus 1.2.3.
Sei $x \in K^\times$ mit $|x|_1 > 1$. Dieses x existiert, da $|\cdot|_1$ nicht-trivialer Betrag ist. Seien $y \in K^\times$ und $\beta := \frac{\log|x|_1}{\log|y|_1}$. Dann ist $|x|_1 = |y|_1^\beta$. Sei $(\frac{m_i}{n_i})_{i\geqslant 0}$ eine rationale Folge mit $n_i > 0$, die von oben gegen β konvergiert. Dann gilt $|x|_1 = |y|_1^\beta < |y|_1^{\frac{m_i}{n_i}}$. Damit ist $|\frac{x^{n_i}}{y^{m_i}}|_1 < 1$. Nach Voraussetzung gilt demnach $|\frac{x^{n_i}}{y^{m_i}}|_2 < 1$, also $|x|_2 < |y|_2^{\frac{m_i}{n_i}}$. Es folgt $|x|_2 \leqslant |y|_2^\beta$. Ist nun $(\frac{m_i}{n_i})_{i\geqslant 0}$ rationale Folge, die von unten gegen β konvergiert, so ist $|x|_2 \geqslant |y|_2^\beta$. Insgesamt folgt $|x|_2 = |y|_2^\beta$. Setze nun $s := \frac{\log|x|_1}{\log|x|_2} = \frac{\log|y|_1}{\log|y|_2}$. Dann $|x|_1 = |x|_2^s$ für alle $x \in K$. Mit 1.2.3 folgt, dass $|\cdot|_1$ und $|\cdot|_2$ äquivalent sind. □

Sei K ein Körper. Eine Funktion $\nu : K \to \mathbb{R} \cup \{\infty\}$ mit

i) $\nu(x) = \infty \Leftrightarrow x = 0$

ii) $\nu(xy) = \nu(x) + \nu(y)$

iii) $\nu(x + y) \geqslant \min\{\nu(x), \nu(y)\}$

heißt **Bewertung** von K.
Für Elemente $x \in K^\times$ ist $\nu(x) = \nu(-x)$, da $\nu(1) = 0$ ist. Dies folgt aus der Gleichung $\nu(1) = \nu(1) + \nu(1)$.

Lemma 1.2.5
Für $\nu(x) \neq \nu(y)$ gilt $\nu(x + y) = \min\{\nu(x), \nu(y)\}$.

Beweis: Sei o.B.d.A. $\nu(x) < \nu(y)$. Angenommen $\nu(x + y) > \min\{\nu(x), \nu(y)\} = \nu(x)$. Dann ist $\nu(x) = \nu((x + y) - y) \geqslant \min\{\nu(x + y), \nu(y)\}$.
Ist $\nu(x + y) \geqslant \nu(y)$, dann folgt $\nu(x) \geqslant \nu(y)$. Dies ist ein Widerspruch zur Voraussetzung.
Ist $\nu(y) \geqslant \nu(x + y)$, so folgt $\nu(x) \geqslant \nu(x + y) > \nu(x)$. Dieser weitere Widerspruch liefert die Behauptung. □

Genauso kann man zeigen, dass für einen nicht-archimedischen Absolutbetrag mit $|x| \neq |y|$ die Gleichung $|x + y| = \max\{|x|, |y|\}$ gilt.
Für eine Bewertung ν von K und $q \in \mathbb{R}_{>1}$ ist $|\cdot|_\nu := q^{-\nu(\cdot)}$ ein nicht-archimedischer Absolutbetrag von K, da für $x, y \in K$ die Ungleichung $|x + y|_\nu = q^{-\nu(x+y)} \leqslant q^{-\min\{\nu(x),\nu(y)\}} = q^{\max\{-\nu(x),-\nu(y)\}} = \max\{-\nu(x), -\nu(y)\} = \max\{|x|_\nu, |y|_\nu\}$ gilt. Dieser heißt, der zu **ν und q zugehörige Absolutbetrag**.

Beispiel 1.2.6

i) Seien $q \in \mathbb{R}_{>1}$ und $|\cdot|$ ein nicht-archimedischer Absolutbetrag von K und sei

$$\nu_{|\cdot|}(x) = \begin{cases} -\log_q |x| & , \quad x \neq 0 \\ \infty & , \quad x = 0. \end{cases}$$

Dann ist $\nu_{|\cdot|}$ eine Bewertung von K. Die ersten beiden Eigenschaften sind offensichtlich erfüllt. Seien $x, y \in K\backslash\{0\}$, dann ist

$$\nu(x + y) = -\log_q |x + y| \geqslant -\log_q \max\{|x|, |y|\} = \min\{-\log_q |x|, -\log_q |y|\} = \min\{\nu(x), \nu(y)\},$$

da $\log_q$ für $q > 1$ monoton steigend ist.

ii) Sei p eine Primzahl. Dann ist

$$\nu_p(x) = \begin{cases} \infty & , \quad x = 0 \\ m - n & , \quad x = \frac{ap^m}{bp^n}, \end{cases}$$

eine Bewertung von $\mathbb{Q}$, wobei $a, b, m, n \in \mathbb{Z}$ und $a, b \notin (p) := p\mathbb{Z}$. Wiederum sind die ersten beiden Eigenschaften erfüllt. Seien $x = \frac{ap^m}{bp^n}, y = \frac{cp^r}{dp^s} \in \mathbb{Q}$ mit $a, b, c, d, m, n, r, s \in \mathbb{Z}$ und $a, b, c, d \notin (p)$.

Dann ist $\nu_p(x) = m - n$ und $\nu_p(y) = r - s$. Es gilt $\nu_p(x + y) = \nu_p(\frac{ap^{m+s}d+cbp^{r+n}}{bdp^{n+s}})$.
Für $m + s = \min\{m + s, r + n\}$ ist

$$\min\{m + s, r + n\} - (n + s) = m + s - n - s = m - n \geqslant \min\{m - n, r - s\}.$$

Aus $r + n = \min\{m + s, r + n\}$ folgt

$$\min\{m + s, r + n\} - (n + s) = r + n - n - s = r - s \geqslant \min\{m - n, r - s\}.$$

Die Bewertung in Beispiel ii) wird als **p-adische Bewertung** bezeichnet. Der zu ν_p zugehörige Absolutbetrag $|\cdot|_p := p^{-\nu_p(\cdot)}$ heißt **p-adischer Absolutbetrag**.

Zwei Bewertungen ν_1, ν_2 heißen **äquivalent**, wenn ein $s \in \mathbb{R}_{>0}$ existiert, sodass $\nu_1 = s\nu_2$ ist. Offensichtlich folgt aus der Äquivalenz der Bewertungen die Äquivalenz der zugehörigen Absolutbeträge.

Sei ν eine Bewertung von K mit zugehörigem Absolutbetrag $|\cdot|_\nu$. Dann definiert man $\mathcal{O}_K := \{x \in K : \nu(x) \geqslant 0\} = \{x \in K : |x|_\nu \leqslant 1\}$, $\mathcal{O}^\times = \{x \in K : \nu(x) = 0\} = \{x \in K : |x|_\nu = 1\}$ und $\mathfrak{m}_K = \{x \in K : \nu(x) > 0\} = \{x \in K : |x|_\nu < 1\}$. Falls klar ist, über welchen Körper $\mathcal{O}_K$ und $\mathfrak{m}_K$ betrachtet werden, werden diese Mengen mit $\mathcal{O}$ und $\mathfrak{m}$ abgekürzt.

Proposition 1.2.7
Sei K ein Körper mit einer Bewertung ν. Dann ist $\mathcal{O}$ ein lokaler Integritätsbereich mit Einheitengruppe $\mathcal{O}^\times$ und dem maximalen Ideal $\mathcal{O} \backslash \mathcal{O}^\times = \mathfrak{m}$.

Beweis: Die Ringaxiome etc. sind leicht nachzurechnen. □

Sei K ein Körper. R heißt **Bewertungsring** von K, falls für alle $x \in K$ folgt, dass $x \in R$ oder $x^{-1} \in R$. Ist R darüberhinaus ein Hauptidealring, so heißt er **diskreter Bewertungsring**.
$\mathcal{O}$ ist ein Bewertungsring von K, da für alle $x \in K$ die Gleichung $\nu(x^{-1}) = -\nu(x)$ gilt.
Für einen Integritätsring R wird mit $Quot(R)$ sein Quotintenkörper bezeichnet. Offensichtlich ist also $Quot(\mathcal{O}) = K$. Der Körper $\mathcal{O}/\mathfrak{m}$ heißt **Restklassenkörper** von $\mathcal{O}$.
Eine Bewertung ν von K heißt **diskret**, wenn $\nu(K)$ einen kleinsten positiven Wert s enthält.

Proposition 1.2.8
Sei ν eine diskrete Bewertung von K mit $s > 0$, sodass $\nu(x) = s > 0$ minimal für ein $x \in K^\times$. Dann ist $\nu(K^\times) = s\mathbb{Z}$.

Beweis: Sei $n \in \mathbb{N}$. Dann ist $\nu(x^n) = ns$ und $\nu((x^n)^{-1}) = -ns$. Daher gilt $s\mathbb{Z} \subseteq \nu(K^\times)$. Angenommen es existiert ein $y \in K^\times$ mit $\nu(y) \notin s\mathbb{Z}$ und o.B.d.A. $\nu(y) > 0$. Somit gibt es ein $m \in \mathbb{N}$, sodass $sm < \nu(y) < s(m + 1)$ ist. Daraus folgt die Ungleichungen $0 < \nu(y) - sm < s$. Also ist $0 < \nu(y) + \nu((x^m)^{-1}) < s$ und somit $0 < \nu(yx^{-m}) < s$. Dies steht im Widerspruch zur Minimalität von s. □

Eine diskrete Bewertung heißt **normiert**, falls der kleinste positive Wert $s = 1$ ist. Dividiert man eine diskrete Bewertung durch den kleinsten Wert, so erhält man eine zu ν äquivalente normierte

Bewertung. Dadurch ändern sich $\mathcal{O}, \mathcal{O}^\times$ und $\mathfrak{m}$ nicht.
Ein Element $\pi \in \mathcal{O}$ mit $\nu(\pi) = 1$ heißt **uniformisierendes Element**.

Lemma 1.2.9
Sei ν eine normierte Bewertung von K und sei π ein uniformisierendes Element. Ist $x \in K^\times$, dann gibt es eine eindeutige Darstellung $x = u\pi^m$ mit $m \in \mathbb{Z}$ und $u \in \mathcal{O}^\times$.

Beweis: Sei $x \in K^\times$ und $\nu(x) = m \in \mathbb{Z}$. Es gilt $\nu(\pi^{-m}) = -m$ und somit $\nu(x\pi^{-m}) = 0$. Also ist $u := x\pi^{-m} \in \mathcal{O}^\times$ und somit $x = u\pi^m$. Sei $x = u'\pi^n$ mit $u' \in \mathcal{O}^\times$ eine weitere Darstellung, so ist $m = n$, da $\nu(u') = 0$. Dies impliziert $(u - u')\pi^m = 0$. Da $\mathcal{O}$ ein Integritätsbereich ist, muss $u = u'$ sein. $\square$

Lemma 1.2.10
*Sei ν eine normierte Bewertung von K und sei π ein uniformisierendes Element.
Dann ist $\bigcap_{n\in\mathbb{N}} \pi^n\mathcal{O} = 0$.*

Beweis: Sei $x \in \bigcap_{n\in\mathbb{N}} \pi^n\mathcal{O}$. Angenommen es gilt $x \neq 0$. Nach 1.2.9 gibt es eine eindeutige Darstellung $x = u\pi^m$ mit $m \in \mathbb{N}$ und $u \in \mathcal{O}^\times$. Das Element x liegt demnach nicht in $\pi^{m+1}\mathcal{O}$. Dies widerspricht der Voraussetzung. $\square$

Korollar 1.2.11
Sei ν eine normierte diskrete Bewertung von K und $\mathcal{O}$ sein diskreter Bewertungsring. Die von Null verschiedenen Ideale des diskreten Bewertungsrings sind $\mathfrak{m}^n = \pi^n\mathcal{O} = \{x \in K : \nu(x) \geqslant n\}$ mit $n > 0$ und π uniformisierendes Element gegeben.

Beweis: Die Behauptung folgt unmittelbar aus 1.2.7, 1.2.10 und 1.1.3. $\square$

Lemma 1.2.12
Sei $(K, |\cdot|)$ ein bewerteter Körper und $\mathcal{O}$ sein Bewertungsring mit maximalen Ideal $\mathfrak{m}$. Für $m, n \in \mathfrak{m}$ ist genau dann $|m| \leqslant |n|$, wenn $m\mathcal{O} \subseteq n\mathcal{O}$ gilt.

Beweis: Seien $m, n \in \mathfrak{m}$ mit $|m| \leqslant |n|$. Im Fall $n = 0$ gilt auch $m = 0$ und daher auch $m\mathcal{O} = n\mathcal{O} = 0$. Andernfalls ist $n^{-1}m \in \mathcal{O}$, da $|n^{-1}m| = \frac{m}{n} \leqslant 1$. Für m gilt somit $nn^{-1}m \in n\mathcal{O}$.
Sei $m\mathcal{O} \subseteq n\mathcal{O}$. Dann gibt es $a \in \mathcal{O}$ mit $m = an$ und somit ist $|m| = |an| = |a||n| \leqslant |n|$. $\square$

Lemma 1.2.13
Sei $(K, |\cdot|)$ ein nicht-archimedischer Körper. Dann ist jedes Hauptideal in $\mathcal{O}$ abgeschlossen in K. Insbesondere ist $\mathcal{O}$ abgeschlossen.

Beweis: Sei $a \in \mathcal{O}$ und $x \in K\backslash a\mathcal{O}$. Dies ist nach 1.2.12 gleichbedeutend zu $|x| > |a|$. Dann ist $B_{|\cdot|}(x, |x|) = \{y \in K : |x - y| < |x|\} \subseteq K\backslash a\mathcal{O}$, da für $z \in B_{|\cdot|}(x, |x|)$ gilt $|z| = |z - x + x| = \max\{|z - x|, |x|\} = |x| > |a|$. $\square$

$(K, |\cdot|)$ heißt **vollständig**, wenn jede Cauchyfolge in K konvergiert.

Theorem 1.2.14
Sei K ein Körper mit diskreter Bewertung ν, der bzgl. des zugehörigen Absolutbetrags vollständig ist und dessen Restklassenkörper mit $char(\mathcal{O}/\mathfrak{m}) = p \neq 0$ perfekt ist, d.h. der Frobenius ist surjektiv. Dann gibt es eine eindeutige multiplikative Abbildung $s : \mathcal{O}/\mathfrak{m} \to \mathcal{O}$, sodass $q_{\mathcal{O},\mathfrak{m}} \circ s = id_{\mathcal{O}/\mathfrak{m}}$. Darüberhinaus ist $s(0) = 0$ und $s(1) = 1$.

Beweis: Sei $x \in \mathcal{O}/\mathfrak{m}$. Da $\mathcal{O}/\mathfrak{m}$ perfekt ist mit Charakteristik $p \neq 0$, gibt es $a_i \in \mathcal{O}$, sodass $_{\mathcal{O},\mathfrak{m}}(a_1)^p = x$ und $_{\mathcal{O},\mathfrak{m}}(a_{i+1})^p =_{\mathcal{O},\mathfrak{m}} (a_i)$ ist. Da $_{\mathcal{O},\mathfrak{m}}(a_{i+1})^p =_{\mathcal{O},\mathfrak{m}} (a_{i+1}^p) =_{\mathcal{O},\mathfrak{m}} (a_i)$, ist $a_{i+1}^p \equiv a_i \mod \mathfrak{m}$. Nach 1.1.2 gilt $a_{i+1}^{p^{i+1}} \equiv a_i^{p^i} \mod \mathfrak{m}^{i+1}$. Damit ist $(a_i^{p^i})_{i\geqslant 0}$ eine Cauchyfolge in $\mathcal{O}$ wegen 1.2.10 und konvergiert wegen 1.2.13 und der Vollständigkeit von K in $\mathcal{O}$. Setze $s(x) := \lim_{i\to\infty} a_i^{p^i}$. Da $_{\mathcal{O},\mathfrak{m}}$ per Definition stetig ist (Offenheit in $\mathcal{O}/\mathfrak{m}$ wird über $_{\mathcal{O},\mathfrak{m}}$ definiert), ist

$$_{\mathcal{O},\mathfrak{m}} \circ s(x) =_{\mathcal{O},\mathfrak{m}} (\lim_{i\to\infty} a_i^{p^i}) = \lim_{i\to\infty} {}_{\mathcal{O},\mathfrak{m}}(a_i^{p^i}) = \lim_{i\to\infty} = \lim_{i\to\infty} x = x.$$

Damit gilt $_{\mathcal{O},\mathfrak{m}} \circ s = id_{\mathcal{O}/\mathfrak{m}}$.
Es muss noch gezeigt werden, dass obige Konstruktion der Folge wohldefiniert ist. Sei dazu $(b_i)_{i\geqslant 0}$ wie oben konstruiert. Dann ist $_{\mathcal{O},\mathfrak{m}}(a_i)^{p^i} = x =_{\mathcal{O},\mathfrak{m}} (b_i)^{p^i}$ und wegen der Injektivität des Frobenius ist $_{\mathcal{O},\mathfrak{m}}(a_i) =_{\mathcal{O},\mathfrak{m}} (b_i)$ und somit $a_i \equiv b_i \mod \mathfrak{m}$ für alle $i \geqslant 0$. Mit 1.1.2 folgt nun $a_i^{p^i} \equiv b_i^{p^i} \mod \mathfrak{m}^{i+1}$ und es gilt nach 1.2.10 die Gleichheit $\lim_{i\to\infty} a_i^{p^i} = \lim_{i\to\infty} b_i^{p^i}$. Damit folgt automatisch die Multiplikativität von s, da der Limes multiplikativ ist und $s(0) = 0$ und $s(1) = 1$, da die Folgen entsprechend gewählt werden können.
Es ist nur noch die Eindeutigkeit zu zeigen. Sei dazu $\tilde{s} : \mathcal{O}/\mathfrak{m} \to \mathcal{O}$ eine multiplikative Abbildung mit $_{\mathcal{O},\mathfrak{m}} \circ \tilde{s} =_{\mathcal{O}/\mathfrak{m}}$ und $x \in \mathcal{O}/\mathfrak{m}$. Dann ist $_{\mathcal{O},\mathfrak{m}}(s(x^{p^{-i}})) =_{\mathcal{O},\mathfrak{m}} (\tilde{s}(x^{p^{-i}}))$, also $s(x^{p^{-i}}) \equiv \tilde{s}(x^{p^{-i}}) \mod \mathfrak{m}$ und mit 1.1.2 folgt

$$s(x) = s(x^{p^{-i}})^{p^i} \equiv \tilde{s}(x^{p^{-i}})^{p^i} = \tilde{s}(x) \mod \mathfrak{m}^{i+1}$$

für alle $i \geqslant 0$. Damit ist $s = \tilde{s}$. □

Lemma 1.2.15
Seien $\mathcal{O}_1$ und $\mathcal{O}_2$ Bewertungsringe mit den maximalen Idealen $\mathfrak{m}_1$ bzw. $\mathfrak{m}_2$ und $\gamma : \mathcal{O}_1 \to \mathcal{O}_2$ ein Ringhomomorphismus mit $\gamma(\mathfrak{m}_1) \subseteq \mathfrak{m}_2$. Dann ist γ stetig.

Beweis: Seien $|\cdot|_1$ und $|\cdot|_2$ jeweils die zu den Bewertungen von $\mathcal{O}_1$ und $\mathcal{O}_2$ zugehörigen Absolutbeträge und $x \in \mathcal{O}_1$ und $\epsilon > 0$. Seien ferner $m_1 \in \mathfrak{m}_1$ und $m_2 := \gamma(m_1)$. Dann gibt es ein $j \in \mathbb{N}$, sodass $\epsilon > |m_2|_2^j$ ist. Für $\delta = |m_1|_1^j$ und $y \in B_{|\cdot|_1}(x,\delta) = \{z \in \mathcal{O}_1 : |z - x|_1 < |m_1|_1^j\}$ gilt wegen 1.2.12 , dass $y - x \in m_1^j\mathcal{O}_1$ und somit $\gamma(y - x) \in m_2^j\mathcal{O}_2$. Damit ist $|\gamma(y) - \gamma(x)|_2 = |\gamma(x - y)|_2 \leqslant |m_2|_2^j < \epsilon$. □

1.3 Vervollständigung

Im Folgenden wird aus einem beliebigen bewerteten Körper $(K, |\cdot|)$ ein vollständiger Körper $(\widehat{K}, |\cdot|^\wedge)$ konstruiert, sodass K in $\widehat{K}$ dicht und isometrisch eingebettet werden kann. Dafür sind noch einige Vorbereitungen nötig.
Für einen bewerteten Körper $(K, |\cdot|)$ wird die Menge aller Cauchy- bzw. Nullfolgen mit $C(K)$ bzw. $N(K)$ bezeichnet.

Lemma 1.3.1
$C(K)$ ist bzgl. der komponentenweise Addition und Multiplikation ein kommutativer Ring mit 1.

Beweis: Seien $(a_n)_{n\geqslant 0}, (b_n)_{n\geqslant 0} \in C(K)$ und $\epsilon > 0$. Dann gibt es ein $N \in \mathbb{N}$, sodass für alle $m, n \geqslant N$ gilt $|(a_m + b_m) - (a_n + b_n)| \leqslant |a_m - a_n| + |b_m - b_n| < \epsilon$. Daher ist $(C(K), +)$ abgeschlossen. Das zu $(a_n)_{n\geqslant 0}$ inverse Element ist $(-a_n)_{n\geqslant 0}$, welches offensichtlich in $C(K)$ liegt. Aufgrund der Beschränktheit der Cauchyfolgen gibt es ein $S \in \mathbb{R}_{\geqslant 0}$ mit $|a_n| \leqslant S$ und $|b_n| \leqslant S$ für alle $n \in \mathbb{N}$. Sei $N \in \mathbb{N}$, sodass für alle $m, n \geqslant N$ gilt $|a_m - a_n| < \frac{\epsilon}{2S}$ und $|b_m - b_n| < \frac{\epsilon}{2S}$. Dann gilt $|a_m b_m - a_n b_n| = |a_m b_m - b_n a_m + b_n a_m - a_n b_n| \leqslant |a_m||b_m - b_n| + |b_n||a_m - a_n| < S\frac{\epsilon}{2S} + S\frac{\epsilon}{2S} = \epsilon$. Damit ist $(C(K), \cdot)$ abgeschlossen und $(C(K), +, \cdot)$ ist ein Ring mit $1 = (1)_{n\geqslant 0}$. □

Lemma 1.3.2
Sei $(K, |\cdot|)$ ein nicht-archimedischer Körper. Seien ferner $(a_n)_{n\geqslant 0} \in C(K)\backslash N(K)$ und $(b_n)_{n\geqslant 0} \in C(K)$.

i) Eine Folge $(c_n)_{n\geqslant 0}$ ist genau dann eine Cauchyfolge in K, wenn für alle ϵ ein $N \in \mathbb{N}$ existiert, sodass für alle $n \geqslant N$ gilt $|c_n - c_{n+1}| < \epsilon$.

ii) Alle, bis auf endlich viele Folgenglieder von $(a_n)_{n\geqslant 0}$ sind von Null verschieden.

iii) Es gibt ein $\delta > 0$ und $N \in \mathbb{N}$, mit $|a_n| \geqslant \delta$ für alle $n \geqslant N$.

iv) Sei $b_n \neq 0$ für nur endlich viele n. Dann ist $(a_n)_{n\geqslant 0} + (b_n)_{n\geqslant 0} \in C(K)\backslash N(K)$.

Beweis: i) Sei $\epsilon > 0$ und $N \in \mathbb{N}$, sodass für alle $n \geqslant N$ gilt $|c_n - c_{n+1}| < \epsilon$. Aufgrund der verschärften Dreiecksungleichung ist $|c_m - c_n| = |c_m - c_{m-1} + c_{m-1} - c_{m-2} + c_{m-2} + ... + c_{n+1} - c_n| \leqslant \max\{|c_m - c_{m-1}|, \ldots, |c_{n+1} - c_n|\} < \epsilon$. Somit ist $(c_n)_{n\geqslant 0}$ eine Cauchyfolge.
ii) Angenommen es gibt unendlich viele $n \in \mathbb{N}$ mit $a_n = 0$. Da $(a_n)_{n\geqslant 0}$ eine Cauchyfolge ist, existiert nach i) ein $\epsilon > 0$ und ein $N \in \mathbb{N}$, sodass für alle $n \geqslant N$ gilt $|a_n - a_{n+1}| < \epsilon$. Da unendlich viele Folgenglieder gleich Null sind, gibt es ein $n_0 \geqslant N$ mit $a_{n_0} = 0$. Daher gilt für alle $n \geqslant n_0$ die Ungleichung $|a_n| = |a_n - a_{n_0}| = |a_n - a_{n-1} + a_{n-1} - ... + a_{n_0+1} - a_{n_0}| \leqslant max\{|a_n - a_{n-1}|, \ldots, |a_{n_0+1} - a_{n_0}|\} < \epsilon$. Das ist aber nicht möglich, da $(a_n)_{n\geqslant 0}$ keine Nullfolge ist.
iii) Angenommen für alle $\delta > 0$ und für alle $N \in \mathbb{N}$ gibt es ein $n \geqslant N$ mit $|a_n| < \delta$. Da $(a_n)_{n\geqslant 0}$ eine Cauchyfolge ist, gibt es für $\frac{\delta}{2} > 0$ ein $N \in \mathbb{N}$, sodass $|a_m - a_n| < \frac{\delta}{2}$ für alle $m, n \geqslant N$ ist. Sei $n_0 \geqslant N$ mit $|a_{n_0}| < \frac{\delta}{2}$. Für alle $n > n_0$ gilt dann $|a_n| = |a_n - a_{n_0} + a_{n_0}| \leqslant |a_n - a_{n_0}| + |a_{n_0}| < \delta$. Dies steht aber im Widerspruch zu $(a_n)_{n\geqslant 0} \notin N(K)$.
iv) Angenommen $(a_n + b_n)_{n\geqslant 0}$ ist eine Nullfolge. Sei $\epsilon > 0$. Dann gibt es ein $N \in \mathbb{N}$, sodass für alle $n \geqslant N$ gilt $|a_n + b_n| < \epsilon$. Nun wird $N_0 \geqslant N$ so gewählt, dass $b_n = 0$ für alle $n \geqslant N_0$ ist. Dann ist $|a_n| < \epsilon$ für alle $n \geqslant N_0$. Dies ist ein Widerspruch zur Voraussetzung. □

Lemma 1.3.3
$N(K)$ ist ein maximales Ideal in $C(K)$.

Beweis: Offensichtlich ist $N(K)$ ein Ideal in $C(K)$. Sei $\mathfrak{a}$ ein Ideal von $C(K)$ mit $\mathfrak{a} \supsetneq N(K)$. Ist $(a_n)_{n\geqslant 0} \in \mathfrak{a}\backslash N(K) \subseteq C(K)\backslash N(K)$, so sind nach 1.3.2 ii) fast alle Folgenglieder von Null verschieden. Sei $(b_n)_{n\geqslant 0}$ mit $b_i \neq 0$ für alle $i \in \mathbb{N}$ mit $a_i = 0$ und alle restlichen Folgenglieder gleich Null. Die Folge

$(b_n)_{n\geqslant 0}$ ist offensichtlich eine Nullfolge. Mit 1.3.2 iv) folgt $(c_n)_{n\geqslant 0} := (a_n + b_n)_{n\geqslant 0} \in C(K)\backslash N(K)$. Nach 1.3.2 iii) gibt es ein $\delta > 0$ und ein $N \in \mathbb{N}$, mit $|c_n| \geqslant \delta$ für alle $n \geqslant N$. Seien $\epsilon > 0$ und $N \in \mathbb{N}$, mit $|c_m - c_n| < \epsilon\delta^2$ für alle $m, n \geqslant N$. Dann ist $|\frac{1}{c_m} - \frac{1}{c_n}| = |\frac{c_n - c_m}{c_m c_n}| = |c_n - c_m|\frac{1}{|c_m|}\frac{1}{|c_n|} < \frac{\epsilon\delta^2}{\delta^2} = \epsilon$. Also ist $(\frac{1}{c_n})_{n\geqslant 0} \in C(K)$.
Damit ist für $(c_n)_{n\geqslant 0} \in \mathfrak{a}$ und $(\frac{1}{c_n})_{n\geqslant 0} \in C(K)$ auch $(c_n)_{n\geqslant 0}(\frac{1}{c_n})_{n\geqslant 0} = (1)_{n\geqslant 0} \in \mathfrak{a}$. Also ist $\mathfrak{a} = C(K)$ und $N(K)$ ist ein maximales Ideal. $\square$

Lemma 1.3.4
Sei A dicht in $(K, |\cdot|)$ und $f : A \to F$ eine Isometrie in einen vollständigen Körper $(F, |\cdot|_F)$. Dann gibt es eine eindeutige Isometrie $g : K \to F$, welche f fortsetzt.

Beweis: Da A dicht in K ist, gibt es für alle $a \in K$ eine Folge $(a_n)_{n\geqslant 0}$ in A, sodass a Grenzwert dieser Folge ist. Damit ist sie auch eine Cauchyfolge in A und folglich ist $(f(a_n))_{n\geqslant 0}$ eine Cauchyfolge in F, da f eine Isometrie ist. Aufgrund der Vollständigkeit des Körper F, konvergiert $(f(a_n))_{n\geqslant 0}$ in F. Folgende Zuordnung erfüllt die eindeutige Fortsetzung der Isometrie f :

$$\begin{aligned} g: \quad & K \longrightarrow F \\ & \lim_{n\to\infty}(a_n)_{n\geqslant 0} \mapsto \lim_{n\to\infty}(f(a_n))_{n\geqslant 0} \end{aligned}$$

Zunächst wird gezeigt, dass g wohldefiniert ist. Seien $(a_n)_{n\geqslant 0}$ und $(b_n)_{n\geqslant 0}$ Folgen in A, die gegen $a \in K$ konvergieren. Sei

$$(c_n)_{n\geqslant 0} := \left(\begin{cases} a_{\frac{n}{2}}, & n \text{ gerade} \\ b_{\frac{n+1}{2}}, & n \text{ ungerade} \end{cases}\right)_{n\geqslant 0} = (b_1, a_1, b_2, a_2, \ldots).$$

Sei $\epsilon > 0$ und seien $N_1, N_2 \in \mathbb{N}$, sodass für alle $n \geqslant N_1$ gilt $|a - a_n| < \epsilon$ und für alle $n \geqslant N_2$ gilt $|a - b_n| < \epsilon$. Dann wähle $N' = 2\max\{N_1, N_2\}$. Damit gilt für alle $n \geqslant N'$, dass $|a - c_n| < \epsilon$ ist. Die Folge $(f(c_n))_{n\geqslant 0}$ konvergiert gegen ein $b \in F$. Da $(f(a_n))_{n\geqslant 0}$ und $(f(b_n))_{n\geqslant 0}$ Teilfolgen der Folge $(f(c_n))_{n\geqslant 0}$ sind, konvergieren sie ebenfalls gegen $b \in F$.
Nun ist zu zeigen, dass $g\Big|_A = f$ ist.
Sei $a \in A$. Dann ist $g(a) = g(\lim_{n\to\infty}(a_n)_{n\geqslant 0}) = \lim_{n\to\infty}(f(a_n))_{n\geqslant 0} = f(a)$.
Seien $k_1, k_2 \in K$ und $(a_n)_{n\geqslant 0}, (b_n)_{n\geqslant 0}$ Folgen in A, sodass k_1 Grenzwert von $(a_n)_{n\geqslant 0}$ und k_2 Grenzwert von $(b_n)_{n\geqslant 0}$ ist. Dann ist

$$\begin{aligned} |g(k_1) - g(k_2)|_F &= |\lim_{n\to\infty} f(a_n) - \lim_{n\to\infty} f(b_n)|_F = \lim_{n\to\infty} |f(a_n) - f(b_n)|_F \\ &= \lim_{n\to\infty} |a_n - b_n| = |\lim_{n\to\infty} a_n - b_n| = |k_1 - k_2|. \end{aligned}$$

Da Isometrien stetig sind ($\delta = \epsilon$), gilt für konvergente Folgen $(a_n)_{n\geqslant 0}$ mit Grenzwert a, dass $\lim_{n\to\infty} f(a_n) = f(a)$ ist. Daher ist f per Konstruktion eindeutig, denn für eine Isometrie $h : K \to F$ gilt $h(a) = \lim_{n\to\infty} h(a_n) = \lim_{n\to\infty} f(a_n) = g(a)$. $\square$

Lemma 1.3.5
Sei $(K, |\cdot|)$ ein Körper, $(F, |\cdot|_F)$ vollständiger Körper und $\iota : K \to F$ eine Isometrie. Ist $\iota(K)$ dicht in F, so existiert für jeden vollständigen Körper $(L, |\cdot|_L)$ und jede Isometrie $\iota' : K \to L$ eine eindeutige

Isometrie $f : F \to L$, sodass das Diagramm

$$\begin{tikzcd} K \arrow[r, "\iota"] \arrow[d, "\iota'"'] & F \arrow[dl, "f"] \\ L & \end{tikzcd}$$

kommutiert.

Beweis: Sei $\iota(K)$ dicht in F und $(L, |\cdot|_L)$ vollständig. Da ι eine Isometrie und somit injektiv ist, ist $\iota^{-1} : \iota(K) \to K$ eine Isometrie. Sei $\iota' : K \to L$ eine Isometrie. Dann ist $h := \iota' \circ \iota^{-1} : \iota(K) \to L$ eine Isometrie. Nach 1.3.4 gibt es eine eindeutige Fortsetzung $f : F \to L$, sodass f eine Isometrie ist. Für alle $k \in K$ ist dann $f \circ \iota(k) = h \circ \iota(k) = \iota' \circ \iota^{-1} \circ \iota(x) = \iota'(x)$. □

Tatsächlich gilt von 1.3.5 auch die umgekehrte Implikation. Diese ist aber für Weiteres nicht relevant.

Theorem 1.3.6
Sei $(K, |\cdot|)$ ein nicht-archimedischer Körper. Dann gibt es einen bis auf isometrische Isomorphie eindeutigen nicht-archimedischen Körper $(\widehat{K}, |\cdot|^\wedge)$ und einen Körperhomomorphismus $\iota : K \to \widehat{K}$ mit

i) ι ist eine Isometrie.

ii) $\iota(K) \subseteq \widehat{K}$ ist dicht.

iii) $(\widehat{K}, |\cdot|^\wedge)$ ist vollständig.

Beweis: Sei $\widehat{K} := C(K)/N(K)$. Dies ist nach 1.3.3 ein Körper. Im Folgenden wird gezeigt, dass die Zuordnung

$$\begin{array}{rrcl} |\cdot|^\wedge : & \widehat{K} & \to & \mathbb{R}_{\geqslant 0} \\ & (a_n)_{n\geqslant 0} + N(K) & \mapsto & \lim_{n\to\infty} |a_n| \end{array}$$

ein Absolutbetrag von $\widehat{K}$ ist. Zunächst wird gezeigt, dass $|(a_n)_{n\geqslant 0} + N(K)|^\wedge \in \mathbb{R}_{\geqslant 0}$ ist. Sei dafür $(a_n)_{n\geqslant 0} \in C(K)$. Dann gibt es für $\epsilon > 0$ ein $N \in \mathbb{N}$, sodass für alle $m, n \geqslant N$ gilt $|a_n - a_m| < \epsilon$. Mit 1.2.2 folgt dann $|\,|a_n| - |a_m|\,|_{\mathbb{R}} \leqslant |a_n - a_m| < \epsilon$. Damit ist $(|a_n|)_{n\geqslant 0}$ eine Cauchyfolge in $\mathbb{R}$ und somit konvergent und der Grenzwert ist nicht negativ.
Seien $(a_n)_{n\geqslant 0}, (b_n)_{n\geqslant 0} \in C(K)$ mit $(a_n - b_n)_{n\geqslant 0} \in N(K)$. Dann ist $0 \leqslant \lim_{n\to\infty} |\,|a_n| - |b_n|\,|_{\mathbb{R}} \leqslant \lim_{n\to\infty} |a_n - b_n| = 0$. Die Folgen $(|a_n|)_{n\geqslant 0}$ und $(|b_n|)_{n\geqslant 0}$ haben somit den gleichen Grenzwert und $|\cdot|^\wedge$ ist eine wohldefinierte Abbildung und offenbar ein Absolutbetrag.
Die Abbildung $|\cdot|^\wedge$ ist offenbar ein Absolutbetrag.
Der Körperhomomorphismus

$$\begin{array}{rrcl} \iota & : K & \to & \widehat{K} \\ & a & \mapsto & (a)_{n\geqslant 0} + N(K) \end{array}$$

ist eine Isometrie, da $|\iota(a)|^\wedge = |(a)_{n\geqslant 0} + N(K)|^\wedge = \lim_{n\to\infty} |a| = |a|$.
Ferner ist $\iota(K) \subseteq \widehat{K}$ dicht. Sei dazu $(a_n)_{n\geqslant 0} + N(K) \in \widehat{K}$. Dann konvergiert die Folge $((a_m)_{n\geqslant 0} + N(K))_{m\geqslant 0} = ((a_0)_{n\geqslant 0} + N(K), (a_1)_{n\geqslant 0} + N(K), (a_2)_{n\geqslant 0} + N(K), \ldots)$ gegen $(a_n)_{n\geqslant 0} + N(K)$, da

$$\lim_{m\to\infty} |(a_n)_{n\geqslant 0} + N(K) - ((a_m)_{n\geqslant 0} + N(K))|^\wedge = \lim_{m\to\infty} \lim_{n\to\infty} |a_n - a_m| = 0.$$

Es ist noch zu zeigen, dass $(\widehat{K}, |\cdot|^\wedge)$ vollständig ist. Sei $(A_n)_{n\geqslant 0}$ eine Cauchyfolge in $\widehat{K}$. Da $\iota(K)$ dicht in $\widehat{K}$ ist, gibt es $a_m \in K$, sodass $0 \leqslant |A_m - ((a_m)_{n\geqslant 0} + N(K))|^\wedge < \frac{1}{m}$. Damit ist die Folge $(A_m - ((a_m)_{n\geqslant 0} + N(K)))_{m\geqslant 0}$ eine Nullfolge in $\widehat{K}$. Also ist $((a_m)_{n\geqslant 0} + N(K))_{m\geqslant 0} = (A_m)_{m\geqslant 0} - (A_m - ((a_m)_{n\geqslant 0} + N(K)))_{m\geqslant 0}$ eine Cauchyfolge. Es ist $|a_k - a_l| = |\iota(a_k - a_l)|^\wedge = |\iota(a_k) - \iota(a_l)|^\wedge = |(a_k)_{n\geqslant 0} + N(K) - (a_l)_{n\geqslant 0} + N(K)|^\wedge$. Damit ist auch $(a_n)_{n\geqslant 0}$ eine Cauchyfolge in K. Sei $A := (a_n)_{n\geqslant 0} + N(K)$. Dann ist

$$\begin{aligned}(A - A_m)_{m\geqslant 0} &= (A - ((a_m)_{n\geqslant 0} + N(K)))_{m\geqslant 0} - (A_m - ((a_m)_{n\geqslant 0} + N(K)))_{m\geqslant 0}\\ &= ((a_n - a_m)_{n\geqslant 0} + N(K))_{m\geqslant 0} - (A_m - (a_m)_{n\geqslant 0} + N(K))_{m\geqslant 0},\end{aligned}$$

wobei der erste Summand eine Nullfolge ist, weil $(a_n)_{n\geqslant 0}$ eine Cauchyfolge ist und der zweite Summand aufgrund obiger Konstruktion eine Nullfolge ist. Somit ist $(\widehat{K}, |\cdot|^\wedge)$ vollständig.
Zuletzt ist noch zu zeigen, dass $(\widehat{K}, |\cdot|^\wedge)$ bis auf Isomorphie eindeutig ist. Seien dazu $(K, |\cdot|)$ ein Körper, $(\widehat{K}, |\cdot|^\wedge)$ und $(\widetilde{K}, |\cdot|^\sim)$ vollständige Körper mit Isometrien $\iota : K \to \widehat{K}$ und $\tilde{\iota} : K \to \widetilde{K}$, sodass $\iota(K) \subseteq \widehat{K}$ dicht und $\tilde{\iota}(K) \subseteq \widetilde{K}$ dicht ist. Dann gibt es nach 1.3.5 eindeutige Isometrien $f : \widehat{K} \to \widetilde{K}$ und $g : \widetilde{K} \to \widehat{K}$, sodass

$$\begin{tikzcd} K \arrow[r, "\iota"] \arrow[dr, "\tilde{\iota}"] \arrow[ddr, "\iota"'] & \widehat{K} \arrow[d, "f"] \\ & \widetilde{K} \arrow[d, "g"] \\ & \widehat{K} \end{tikzcd} \qquad \begin{tikzcd} K \arrow[r, "\tilde{\iota}"] \arrow[dr, "\iota"] \arrow[ddr, "\tilde{\iota}"'] & \widetilde{K} \arrow[d, "g"] \\ & \widehat{K} \arrow[d, "f"] \\ & \widetilde{K} \end{tikzcd}$$

Dann muss $g \circ f = id_{\widehat{K}}$ und $f \circ g = id_{\widetilde{K}}$ sein. Die Körper $\widetilde{K}$ und $\widehat{K}$ sind also isometrisch isomorph. □

Der Körper $(\widehat{K}, |\cdot|^\wedge)$ wird **Vervollständigung** von $(K, |\cdot|)$ genannt.

Proposition 1.3.7
Sei $(K, |\cdot|)$ ein vollständiger diskreter Körper mit Bewertung ν und $S \subseteq \mathcal{O}_K$ ein Repräsentantensystem von $\mathcal{O}_K/\mathfrak{m}$ mit $0 \in S$ und π uniformisierendes Element.

i) Für $m_0 \in \mathbb{Z}$ und $a_m \in S$ und $m \geqslant m_0$ konvergiert die Reihe $\sum_{m\geqslant m_0} a_m \pi^m$ in K.

ii) Jedes Element $x \in K$ ist von der Form $\sum_{m\in\mathbb{Z}} a_m \pi^m$ mit eindeutigen Elementen $a_m \in S$, sodass für fast alle $m \in \mathbb{Z}_{<0}$ gilt $a_m = 0$. Insbesondere gilt

$$\nu(x) = \begin{cases} \infty, & a_m = 0 \textit{ für alle } m \in \mathbb{Z} \\ \min\{m \in \mathbb{Z} : a_m \neq 0\}, & \textit{sonst} \end{cases}.$$

Beweis: i) Es gilt $\nu(a_m \pi^m) = \nu(a_m) + m \geqslant m$, da $a_m \in \mathcal{O}_K$ ist und somit $\nu(a_m) \geqslant 0$ gilt. Damit ist $(a_m \pi^m)_{m\geqslant m_0}$ bzgl $|\cdot| = q^{-\nu(\cdot)}$ mit $q > 1$ eine Nullfolge in K. Die Folge $(\sum_{i=m_0}^n a_i \pi^i)_{n\geqslant m_0}$ ist eine Cauchyfolge, denn für $\epsilon > 0$ und N_ϵ mit $\epsilon > q^{-N_\epsilon}$ gilt für alle $m \geqslant n \geqslant N_\epsilon$

$$\begin{aligned}|\textstyle\sum_{i=m_0}^m a_i \pi^i - \sum_{i=m_0}^n a_i \pi^i|_\nu &= |\textstyle\sum_{i=n+1}^m a_i \pi^i|_\nu \leqslant \max_{n+1\leqslant i\leqslant m}\{|a_i \pi^i|_\nu\} \leqslant q^{-(n+1)}\\ &< q^{-N_\epsilon} < \epsilon\end{aligned}$$

Dabei gilt $\max_{n+1\leqslant i\leqslant m}\{|a_i\pi^i|_\nu\} \leqslant q^{-(n+1)}$, da für $a_i \neq 0$ ist $a_i \in \mathcal{O}_K^\times = \mathcal{O}_K \backslash \mathfrak{m}$. Also ist $|a_i|_\nu = 1$ und somit $|a_i\pi^i|_\nu = q^{-i}$.
Da K vollständig ist, konvergiert die Reihe $\sum_{m\geqslant m_0} a_m\pi^m$.
ii) Sei $x \in K^\times$. Induktiv wird nun die Existenz einer solchen Reihendarstellung für x gezeigt. Dazu wird eine Nullfolge $(x - s_m)_{m\geqslant m_0}$ konstruiert mit $s_m = \sum_{n=m_0}^m a_n\pi^n$. Sei $m_0 := \nu(x) \in \mathbb{Z}$. Es genügt zu zeigen, dass es $a_i \in S$ gibt mit $\nu(x - s_m) > m$ für alle $m \geqslant m_0$, denn dann ist für $\epsilon > 0$ mit $N_\epsilon \in \mathbb{N}$ und $\epsilon > q^{-N_\epsilon}$ offensichtlich $|x - s_m|_\nu < \epsilon$ für alle $m \geqslant N_\epsilon$. Für $m = m_0$ gilt $\nu(x\pi^{-m_0}) = \nu(x) - \nu(\pi^{m_0}) = 0$. Damit ist $x\pi^{-m_0} \in \mathcal{O}_K^\times$. Es gibt also ein $a_{m_0} \in S\backslash\{0\}$, sodass $x\pi^{-m_0} - a_{m_0} \in \mathfrak{m}$ und somit $\nu(x\pi^{-m_0} - a_{m_0}) > 0$ ist. Dies impliziert $\nu(x - a_{m_0}\pi^{m_0}) > \nu(\pi^{m_0}) = m_0$. Gelte nun nach Induktionsvoraussetzung $\nu(x - s_m) \geqslant m + 1$ und somit $\nu((x - s_m)\pi^{-(m+1)}) \geqslant 0$. Also ist $(x - s_m)\pi^{-(m+1)} \in \mathcal{O}_K$ und somit gibt es $a_{m+1} \in S$, sodass $(x - s_m)\pi^{-(m+1)} - a_{m+1} \in \mathfrak{m}$ ist. Folglich ist $\nu(x - s_{m+1}) = \nu(x - s_m - a_{m+1}\pi^{m+1}) > m + 1$.
Nun muss noch die Eindeutigkeit dieser Darstellung gezeigt werden. Zunächst wird gezeigt, dass die Reihe, wie in obiger Konstruktion bei m_0 beginnt. Dafür wird die Gleichheit $\nu(\sum_{m\geqslant m_0} a_m\pi^m) = \min\{m \in \mathbb{Z} : a_m \neq 0\}$ bewiesen. Sei dazu $n = \min\{m \in \mathbb{Z} : a_m \neq 0\} < \infty$. Dann gilt für alle $m > n$, dass $a_m\pi^m \in \pi^{n+1}\mathcal{O}_K$ ist. Da nach 1.2.13 $\pi^{n+1}\mathcal{O}_K$ eine abgeschlossene Menge in K ist, konvergiert die Folge $(\sum_{i=n+1}^m a_i\pi^i)_{m\geqslant n+1}$ in $\pi^{n+1}\mathcal{O}_K$. Dann ist

$$\begin{aligned}\nu(\textstyle\sum_{m=n}^\infty a_m\pi^m) &= \nu(a_n\pi^n + \sum_{m>n} a_m\pi^m) = \min\{\nu(a_n\pi^n), \nu(\sum_{m>n} a_m\pi^m)\} \\ &= n = \min_{m\in\mathbb{Z}}\{a_m \neq 0\},\end{aligned}$$

da $a_n \in \mathcal{O}_K^\times$, also $\nu(a_n) = 0$ und $\nu(\sum_{m>n} a_m\pi^m) \geqslant n + 1$ ist Also muss die Reihe bei m_0 beginnen.
Sei $x = \sum_{m\geqslant m_0} a_m\pi^m = \sum_{m\geqslant m_0} b_m\pi^m$ mit $a_m, b_m \in S$. Für $x = 0$ sind für alle $m \in \mathbb{Z}$ die Koeffizienten a_m, b_m gleich Null, da $\nu(x) = \nu(0) = \infty = \min\{m \in \mathbb{Z} : a_m \neq 0\}$ ist.
Sei nun $x \neq 0$. Es gilt $(a_{m_0} - b_{m_0})\pi^{m_0} = \sum_{m>m_0}(b_m - a_m)\pi^m$ und deshalb gilt $\nu((a_{m_0} - b_{m_0})\pi^{m_0}) > m_0$. Somit ist $a_{m_0} - b_{m_0} \in \mathfrak{m}$, da aber a_{m_0}, b_{m_0} im Repräsentantensystem S von $\mathcal{O}_K/\mathfrak{m}$ liegen, ist $a_{m_0} = b_{m_0}$. Induktiv folgt nun, dass $a_m = b_m$ für alle $m \geqslant m_0$ ist. □

Lemma 1.3.8
Sei $(K, |\cdot|)$ ein nicht-archimedischer Körper der Charakteristik 0 mit Bewertungsring $\mathcal{O}_K$ und $char(\mathcal{O}_K/\mathfrak{m}_K) = p$. Sei $\mathcal{O}_{\widehat{K}}$ der Bewertungsring der Vervollständigung $\widehat{K}$ von K. Dann ist

$$\mathcal{O}_K/p\mathcal{O}_K \cong \mathcal{O}_{\widehat{K}}/p\mathcal{O}_{\widehat{K}}.$$

Beweis: Betrachte die Zuordnung

$$\begin{aligned}\iota' : \quad \mathcal{O}_K/p\mathcal{O}_K &\to \mathcal{O}_{\widehat{K}}/p\mathcal{O}_{\hat{K}} \\ a + p\mathcal{O}_K &\mapsto \iota(a) + p\mathcal{O}_{\widehat{K}},\end{aligned}$$

wobei ι wie im Beweis von 1.3.6 definiert ist. Die Behauptung ist, dass ι' ein Ringisomorphismus ist.

Seien $a + p\mathcal{O}_K, b + p\mathcal{O}_K \in \mathcal{O}_K/p\mathcal{O}_K$ mit $\iota(a) + p\mathcal{O}_{\widehat{K}} = \iota(b) + p\mathcal{O}_{\widehat{K}}$. Dann ist

$$\begin{aligned} \iota(a) + p\mathcal{O}_{\widehat{K}} = \iota(b) + p\mathcal{O}_{\widehat{K}} \quad &\Leftrightarrow \quad (a-b)_{i\geqslant 0} + N(\mathcal{O}_K) \in p\mathcal{O}_{\widehat{K}} \\ &\overset{1.2.12}{\Leftrightarrow} \quad |(a-b)_{i\geqslant 0} + N(\mathcal{O}_K)|^\wedge \leqslant |p| \\ &\Leftrightarrow \quad \lim_{i\to\to\infty} |a-b| = |a-b| \leqslant |p| \\ &\Leftrightarrow \quad a - b \in p\mathcal{O}_K. \end{aligned}$$

Also ist ι' eine injektive Abbildung. Sei $y + p\mathcal{O}_{\widehat{K}} \in \mathcal{O}_{\widehat{K}}/p\mathcal{O}_{\widehat{K}}$. Da nach 1.3.6 $\iota(K)$ dicht in $\widehat{K}$ liegt, liegt $\iota(\mathcal{O}_K)$ dicht in $\mathcal{O}_{\widehat{K}}$. Damit existiert eine Folge $(\iota(a_i))_{i\geqslant 0}$ mit $a_i \in \mathcal{O}_K$, dessen Grenzwert y ist. Für $\epsilon = |p|$ gibt es damit ein $N \in \mathbb{N}$, sodass für $n \geqslant N$ gilt $|\iota(a_n) - y|^\wedge \leqslant |p|$. Somit gilt für $a_N \in \mathcal{O}_K$, dass $\iota(a_N) \equiv y \mod p\mathcal{O}_{\widehat{K}}$. Es folgt $\iota'(a_N + p\mathcal{O}_K) = \iota(a_N) + p\mathcal{O}_{\widehat{K}} = y + p\mathcal{O}_{\widehat{K}}$. Somit ist ι' surjektiv. Die Linearität folgt aus der von ι. □

Lemma 1.3.9
Der Ring $\mathcal{O}_K$ ist genau dann vollständig, wenn K vollständig ist.

Beweis: Sei zunächst $\mathcal{O}_K$ vollständig. Sei dazu $(x_n)_{n\geqslant 0}$ eine Cauchyfolge in $K = Quot(\mathcal{O}_K)$. Da jede Cauchyfolge bzgl. eines Absolutbetrags beschränkt ist, gibt es ein $y \in K$ mit $|x_n| \leqslant |y|$ für alle $n \in \mathbb{N}$. Damit ist $y^{-1}x_n$ eine Cauchyfolge in $\mathcal{O}_K$ mit Grenzwert x'. Die Folge $(x_n)_{n\geqslant 0}$ konvergiert somit gegen yx'.
Ist K vollständig, so ist auch $\mathcal{O}_K$ vollständig, da der Bewertungsring nach 1.2.13 abgeschlossen ist. □

Lemma 1.3.10
Seien $K \subseteq F$ zwei nicht-archimedische Körper, wobei der Absolutbetrag von F eine Fortsetzung des Absolutbetrags von K ist. Liegt K dicht in F, so sind ihre Vervollständigungen isometrisch isomorph.

Beweis: Der Körper $\widehat{F}$ ist die Vervollständigung von K, da für $\iota : F \to \widehat{F}$ der Körperhomomorphismus $\iota|_K : K \to \widehat{F}$ die Eigenschaften i) bis iii) in 1.3.6 erfüllt. Daher sind $\widehat{F}$ und $\widehat{K}$ isometrisch isomorph. □

1.4 Fortsetzung des Absolutbetrags auf einen Erweiterungskörper

Ziel dieses Abschnitts ist die Fortsetzung des Absolutbetrags $|\cdot|$ eines vollständigen Körpers K auf einen Erweiterungskörper L mit $[L : K] = n$. Diese ist eindeutig und hat die Gestalt $|x|_L := \sqrt[n]{|N_{L|K}(x)|}$, wobei $N_{L|K}$ die Normfunktion ist.

Sei $(K, |\cdot|)$ ein nicht-archimedischer Körper mit Absolutbetrag $|\cdot|$. Ist V ein $K-$Vektorraum, dann ist eine Abbildung $||\cdot|| : V \to \mathbb{R}_{\geqslant 0}$ eine **Norm von V**, wenn sie für alle $v, w \in V$ und alle $x \in K$ folgende Eigenschaften erfüllt:

i) $||v|| = 0 \Leftrightarrow v = 0$

ii) $||xv|| = |x|\ ||v||$

iii) $||v+w|| \leqslant \max\{||v||, ||w||\}$.

Beispiel 1.4.1
Sei $(K, |\cdot|)$ ein nicht-archimedischer Körper. Dann ist offenbar

$$\begin{array}{rcll} ||\cdot|| & : & K[X] & \to & \mathbb{R}_{\geqslant 0} \\ & & \sum\limits_{i=0}^{m} b_i X^i & \mapsto & \max_{i \in \{0,\dots,m\}}\{|b_i|\}. \end{array}$$

eine Norm von $K[X]$.

Die Norm in Beispiel 1.4.1 heißt **Gauß-Norm**.

Lemma 1.4.2
Für die Gauß-Norm gilt $||fg|| = ||f||\ ||g||$ für alle $f, g \in K[X]$.

Beweis: Seien $f = \sum_{i=0}^{n} b_i X^i$ und $g = \sum_{i=0}^{m} c_i X^i$ mit minimalen $q, l \in \mathbb{N}$, sodass $||f|| = |b_q|$ und $||g|| = |c_l|$ ist. Dann ist $fg = \sum_{s=0}^{n+m} e_s X^s$ mit $e_s = \sum_{r=0}^{s} b_{s-r} c_r$ und $b_t = 0$ für $t > n$ und $c_t = 0$ für $t > m$. Der l-te Summand des Koeffizients $e_{q+l} = \sum_{r=0}^{q+l} b_{q+l-r} c_r$ ist $b_q c_l$. Für alle übrigen Summanden von e_{l+q} gilt $|b_{q+l-r} c_r| < |b_q c_l|$, denn für $r < l$ ist $|c_r| < |c_l|$, also $|b_{q+l-r} c_r| < |b_q c_l|$ und für $r > l$ ist $|b_{q+l-r}| < |b_q|$, also $|b_{q+l-r} c_r| < |b_q c_l|$. Damit ist $|e_{q+l}| = \max_{r \in \{0,\dots,q+l\}}\{|b_{ql-r} c_r|\} = |b_q c_l|$. Darüberhinaus ist $|e_s| \leqslant |e_{q+l}|$ für alle $s \in \{0, \dots, m+n\}$, da $|e_s| \leqslant \max_{r \in \{0,\dots,s\}}\{|b_{s-r} c_r|\} \leqslant |b_q c_l|$ ist. Insgesamt folgt die Behauptung, denn

$$||fg|| = ||\sum_{i=0}^{n+m} e_s X^s|| = \max_{s \in \{0,\dots,m+n\}}\{|e_s|\} = |e_{q+l}| = |b_q c_l| = |b_q||c_l| = ||f||\ ||g||.$$

□

Zwei Normen $||\cdot||_1$ und $||\cdot||_2$ von V heißen **äquivalent**, wenn es $C, D \in \mathbb{R}_{>0}$ gibt, sodass $C||v||_1 \leqslant ||v||_2 \leqslant D||v||_1$ für alle $v \in V$ gilt.

Lemma 1.4.3
Zwei äquivalente Normen induzieren die gleiche Topologie.

Beweis: Seien $||\cdot||_1$ und $||\cdot||_2$ äquivalente Normen des $(K, |\cdot|)-$Vektorraums V. Dann gibt es $C, D \in \mathbb{R}_{>0}$, sodass $C||v||_1 \leqslant ||v||_2 \leqslant D||v||_1$ für alle $v \in V$ ist. Sei nun $U \subseteq V$ bzgl. $||\cdot||_1$ offen und $x \in U$. Dann existiert ein $\epsilon > 0$, sodass $U \supseteq B_{||\cdot||_1}(x, \epsilon) = \{y \in V : ||x-y||_1 < \epsilon\} \supseteq \{y \in V : ||x-y||_2 < C\epsilon\} = B_{||\cdot||_2}(x, C\epsilon)$ ist. Die andere Inklusion folgt analog. □

Proposition 1.4.4
Sei $(K, |\cdot|)$ ein nicht-archimedischer und vollständiger Körper und sei V ein $n-$dimensionaler normierter K-Vektorraum. Dann sind alle Normen von V äquivalent und V ist vollständig.

Beweis: Sei $B_V = \{v_1, \ldots, v_n\}$ eine Basis von V und sei $||\sum_{i=1}^n x_i v_i||_{\max} := \max\limits_{i=1,\ldots,n}\{|x_i|\}$ mit $x_i \in K$ für alle $i \in \{1, \ldots, n\}$. Offensichtlich ist $||\cdot||_{\max}$ eine Norm von V. Sei $||\cdot||_1$ eine beliebige Norm von V und sei $D := \max_{i=1,\ldots,n}\{||v_i||_1\}$. Dann ist $||\sum_{i=1}^n x_i v_i||_1 \leqslant \max_{i=1,\ldots,n}\{||v_i||_1|x_i|\} \leqslant \max_{i=1,\ldots,n}\{|v_i|_1\}\max\{|x_i|\} = D||\sum_{i=1}^n x_i v_i||_{\max}$. Die andere Abschätzung wird nun induktiv über die Dimension des Vektorraums gezeigt. Ist die Dimension gleich 1 so wählt man $C = ||v_1||_1$ und V ist vollständig, da K vollständig ist. Gelte nun die Behauptung für Vektorräume der Dimension kleiner n. Sei V_i das Erzeugnis von $B_{V_i} = \{v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n\}$. Dann ist V_i bzgl. der Einschränkung auf $||\cdot||_1$ nach Induktionsvoraussetzung vollständig und somit abgeschlossen in V. Dann sind auch die Nebenklassen $V_i^0 := v_i + V_i$ offensichtlich abgeschlossen. Folglich ist auch $\bigcup_{i=1}^n V_i^0$ abgeschlossen. Wegen $0 \notin \bigcup_{i=1}^n V_i^0$ ist $V \backslash \bigcup_{i=1}^n V_i^0$ eine nicht-leere offene Menge. Es gibt also eine Umgebung von 0, deren Schnitt mit $\bigcup_{i=1}^n V_i^0$ trivial ist, d.h. es gibt ein $\epsilon > 0$, sodass $||w_i + v_i||_1 \geqslant \epsilon$ für alle $w_i \in V_i$ und alle $i \in \{1, \ldots, n\}$ ist. Nun setze man $C := \epsilon$. Sei $x = \sum_{i=1}^n x_i v_i \neq 0$. Dann gilt für $|x_r| = \max_{i=1,\ldots,n}\{|x_i|\}$ die Ungleichung $||\frac{x}{x_r}||_1 = ||\sum_{i=1}^n \frac{x_i}{x_r} v_i||_1 \geqslant \epsilon$, da $\sum_{i=1}^n \frac{x_i}{x_r} v_i \in V_r^0$ ist. Insgesamt ergibt sich $||x||_1 \geqslant C|x_r| = C||x||_{\max}$.
Alle Normen sind äquivalent, denn für zwei Normen $||\cdot||_1$ und $||\cdot||_2$ von V und $C_1, C_2, D_1, D_2 \in \mathbb{R}_{>0}$ mit

$$C_1||v||_1 \leqslant ||v||_{\max} \leqslant D_1||v||_1 \text{ und } C_2||v||_2 \leqslant ||v||_{\max} \leqslant D_2||v||_2$$

für alle $v \in V$ folgt $\frac{C_1}{D_2}||v||_1 \leqslant ||v||_2 \leqslant \frac{D_1}{C_2}||v||_1$. Es ist noch zu zeigen, dass V vollständig ist. Wegen 1.4.3 genügt es zu zeigen, dass V bzgl. der Maximumsnorm vollständig ist. Sei also $(\sum_{i=1}^n v_i x_i^{(m)})_{m \geqslant 0}$ eine Cauchyfolge bzgl. $||\cdot||_{\max}$. Dann gibt es für $\epsilon > 0$ ein $N \in \mathbb{N}$, sodass für alle $m_1, m_2 \geqslant N$ gilt

$$\begin{aligned} ||\sum_{i=1}^n v_i x_i^{(m_1)} - \sum_{i=1}^n v_i x_i^{(m_2)}||_{\max} &= ||\sum_{i=1}^n v_i(x_i^{(m_1)} - x_i^{(m_2)})||_{\max} \\ &= \max_{i=1,\ldots,n}\{|x_i^{(m_1)} - x_i^{(m_2)}|\} < \epsilon. \end{aligned}$$

Also gilt insbesondere $|x_i^{(m_1)} - x_i^{(m_2)}| < \epsilon$ für alle $i \in \{1, \ldots, n\}$. Damit ist für alle $i \in \{1, \ldots, n\}$ die Folge $(x_i^{(m)})_{m \geqslant 0}$ eine Cauchyfolge in K und ist somit konvergent. Sei x_i der Grenzwert der Folge $(x_i^{(m)})_{m \geqslant 0}$. Dann ist offenbar $\sum_{i=1}^n v_i x_i$ der Grenzwert der Folge $(\sum_{i=1}^n v_i x_i^{(m)})_{m \geqslant 0}$. Der Vektorraum V ist vollständig. □

Lemma 1.4.5
Sei R ein Ring mit Eins.

i) Für $f = \sum_{i=0}^n a_i X^i$ und $g = \sum_{i=0}^m b_i X^i \in R[X]$ mit $a_n, b_m \neq 0$, $b_m \in R^\times$ und $m \leqslant n$ gibt es ein $d \in R[X]$ mit $0 \leqslant \deg(f - dg) < n$.

ii) Seien $f, g \in R[X]$, wobei der Leitkoeffizient von g in $R^\times$ liegt. Dann gibt es $r, \phi \in R[X]$, sodass $f = \phi g + r$ mit $\deg(r) < \deg(g))$ ist.

Beweis: i) Sei $d = \frac{a_n}{b_m} X^{n-m}$. Dann ist

$$\begin{aligned} \deg(f - dg) &= \deg(\sum_{i=0}^n a_i X^i - (\tfrac{a_n}{b_m}) X^{n-m} \sum_{i=0}^m b_i X^i) \\ &= \deg(a_n X^n + \sum_{i=0}^{n-1} a_i X^i - a_n X^n - \sum_{i=n-m}^{n-1} (\tfrac{a_n}{b_m} b_{i-n-m} X^i)) < n. \end{aligned}$$

ii) Für den Fall $\deg(g) > \deg(f)$ werden $r = f$ und $\phi = 0$ gewählt.

Nun wird induktiv gezeigt, dass für $f, g \in R[X]$ mit $\deg(g) \leqslant \deg(f)$ Polynome $r, \phi \in R[X]$ existieren mit $f = \phi g + r$, sodass $\deg(r) < \deg(g)$ ist. Für den Fall $\deg(f) = 1$ mit $f = a_1X + a_0$ und $\deg(g) = 0$ mit $g = b_0 \in R^\times$ lässt sich f darstellen durch $f = \phi g + r$ mit $\phi = \frac{a_1}{b_0}X$ und $r = a_0$. Ist $\deg(g) = 1$ mit $g = b_1X + b_0$, wobei b_1 in $R^\times$ liegt, so lässt sich f darstellen durch $f = \phi g + r$ mit $\phi = \frac{a_1}{b_1}$ und $r = -\frac{a_1 b_0}{b_1} + a_0$.
Sei $\deg(f) = n \geqslant \deg(g)$. Es gibt nach i) ein Polynom $d \in R[X]$ mit $\deg(f - dg) < n$. Ist $\deg(g) \leqslant \deg(f - dg)$, so gibt es nach Induktionsvoraussetzung Polynome $\phi', r \in R[X]$ mit $f - dg = \phi' g + r$, sodass $\deg(r) < \deg(g)$ ist. Damit ist $f = \phi g + r$ mit $\phi = \phi' - d$. Ist $\deg(g) > \deg(f - dg)$, so wählt man $r = f - dg$ und $\phi = d$. Damit ist $f = \phi g + r$. □

Theorem 1.4.6
Sei $(K, |\cdot|)$ ein nicht-archimedischer vollständiger Körper und $\mathcal{O}$ sein Bewertungsring mit maximalem Ideal $\mathfrak{m}$. Bezeichne mit φ die Abbildung

$$\begin{aligned} \varphi : \quad \mathcal{O}[X] &\to \mathcal{O}/\mathfrak{m}[X] \\ \sum_{i=0}^{n} a_i X^i &\mapsto \sum_{i=0}^{n} (a_i + \mathfrak{m}) X^i. \end{aligned}$$

Sei $f \in \mathcal{O}[X]$ mit $\varphi(f) = \overline{g}\overline{h}$, $\overline{g}, \overline{h} \in \mathcal{O}/\mathfrak{m}[X]$ und $\gcd(\overline{g}, \overline{h}) = 1$. Dann gibt es eine Zerlegung $f = gh$ mit $g, h \in \mathcal{O}[X]$, sodass $\deg(g) = \deg(\overline{g})$, $\varphi(g) = \overline{g}$ und $\varphi(h) = \overline{h}$ ist.

Beweis: Sei $d = \deg(f)$ und $m = \deg(\overline{g})$. Damit ist $d - m \geqslant \deg(\overline{h})$. Da φ surjektiv ist, gibt es $g_0, h_0 \in \mathcal{O}[X]$ mit $\varphi(g_0) = \overline{g}, \varphi(h_0) = \overline{h}$ und $\deg(g_0) = m$ und $\deg(h_0) \leqslant d - m$. Da $\overline{g}$ und $\overline{h}$ teilerfremd sind, gibt es $a, b \in \mathcal{O}[X]$, sodass $\varphi(ag_0 + bh_0) = \varphi(1) = 1$ in $\mathcal{O}/\mathfrak{m}[X]$ ist. Es gilt $\varphi(f) = \varphi(g_0)\varphi(h_0)$. Damit liegen die Polynome $f - g_0h_0$ und $ag_0 + bh_0 - 1$ in $\mathfrak{m}[X]$. Sei Λ bzgl. $|\cdot|$ das Maximum unter den Koeffizienten dieser Polynome. Das Ziel ist es Polynome, $p_i, q_i \in \mathcal{O}[X]$ mit $\deg(p_i) < m$ und $\deg(q_i) \leqslant d - m$ zu finden mit

$$g_{n-1} := g_0 + \sum_{i=1}^{n-1} p_i \Lambda^i$$
$$h_{n-1} := h_0 + \sum_{i=1}^{n-1} q_i \Lambda^i,$$

sodass $f \equiv g_{n-1}h_{n-1} \mod (\Lambda^n)[X]$ ist. Falls dann die Aussagen

i) die Folgen $(g_n)_{n\geqslant 0}$ und $(h_n)_{n\geqslant 0}$ konvergieren in $\mathcal{O}[X]$

ii) $\bigcap_{n\geqslant 0}(\Lambda^n) = 0$

gelten, so folgt für die Grenzwerte g und h der Folgen $(g_n)_{n\geqslant 0}$ und $(h_n)_{n\geqslant 0}$, dass $\lim_{n\to\infty} f - g_{n-1}h_{n-1} = f - gh = 0$ ist und das Theorem ist bewiesen.
Zunächst werden i) und ii) gezeigt, unter der Annahme, dass p_i und q_i existieren.
i) Die Folge (g_n) ist eine Cauchyfolge in $\mathcal{O}[X]$: Seien $m, n \in \mathbb{N}$ mit $n \geqslant m$, dann ist $|g_n - g_m| = |p_n\Lambda^n + ... + p_{m+1}\Lambda^{m+1}|$. Für die Koeffizienten a_i des Polynoms $g_n - g_m$ gilt $\max_i\{|a_i|\} \leqslant |\Lambda^{m+1}|$, da Λ^{m+1} in jedem Koeffizienten vorhanden ist und alle übrigen Faktoren in $\mathcal{O}$ liegen und somit bzgl. $|\cdot| \leqslant 1$. Die Folge $(|\Lambda|^m)_{m\geqslant 0}$ ist eine Nullfolge und somit sind die Folgen der Koeffizienten von $(g_n)_{n\geqslant 0}$ Cauchyfolgen. Da $\mathcal{O} \subseteq K$ gilt, konvergieren diese, und aufgrund der Abgeschlossenheit von $\mathcal{O}$ liegen die Grenzwerte in $\mathcal{O}$. Da die Grade von g_0 und den p_i beschränkt sind, ist

$g := (\sum_{i=1}^{\infty} p_i \Lambda^i) + g_0 \in \mathcal{O}[X]$. Gleiches gilt für die Folge $(h_n)_{n\geqslant 0}$.
ii)Sei $x \in \bigcap_{n\geqslant 0}(\Lambda^n)$. Angenommen es gilt $x \neq 0$. Das bedeutet, es gibt ein $r \in \mathbb{R}$, sodass $|x| = r$ ist. Da $(|\Lambda|^n)_{n\geqslant 0}$ eine Nullfolge ist, gibt es ein $n \in \mathbb{N}$, sodass $|\Lambda|^n < r = |x|$. Dann ist $x \notin (\Lambda^n)$. Dies steht im Widerspruch zur Voraussetzung.
Im Folgenden wird nun induktiv gezeigt, dass $f \equiv g_{n-1}h_{n-1} \mod (\Lambda^n)[X]$ gilt. Für $n = 1$ gilt nach Konstruktion $\deg(g_0) = \deg(\overline{g})$ und $f - g_0h_0 \in (\Lambda)[X]$, da alle Koeffizienten a_i von $f - g_0h_0$ nach 1.2.12 in (Λ) liegen, da Λ maximal gewählt wurde. Sei nun für $n \geqslant 1$ die Kongruenz $f \equiv g_{n-1}h_{n-1} \mod (\Lambda^n)[X]$ erfüllt.
Nun werden $p_i, q_i \in \mathcal{O}[X]$ konstruiert, welche die Induktionsbehauptung erfüllen. Es sei dabei angemerkt, dass gilt

$$\begin{aligned} & f \equiv g_nh_n \mod (\Lambda^{n+1})[X] \\ \Leftrightarrow\ & f \equiv g_{n-1}h_{n-1} + \Lambda^n(g_{n-1}q_n + p_nh_{n-1}) \mod (\Lambda^{n+1})[X] \\ \Leftrightarrow\ & g_{n-1}q_n + h_{n-1}p_n \equiv g_0q_n + h_0p_n \equiv \Lambda^{-n}(f - g_{n-1}h_{n-1}) \mod (\Lambda)[X]. \end{aligned} \tag{1}$$

Sei $f_n := \Lambda^{-n}(f - g_{n-1}h_{n-1}) \in \mathcal{O}[X]$. Die Polynome $f - g_0h_0$ und $ag_0 + bh_0 - 1$ liegen in $\mathfrak{m}[X]$. Da Λ das Maximum der Koeffizienten dieser Polynome bzgl $|\cdot|$ ist, folgt mir 1.2.12, dass $g_0a + h_0b \equiv 1 \mod (\Lambda)[X]$ ist. Damit ist $g_0af_n + h_0bf_n \equiv f_n \mod (\Lambda)[X]$. Der Leitkoeffizient des Polynoms g_0 ist eine Einheit, da $\deg(g_0) = \deg(\overline{g})$. Nach 1.4.5 ii) gibt es somit $q, p_n \in \mathcal{O}[X]$, sodass $bf_n = qg_0 + p_n$ mit $\deg(p_n) < \deg(g_0) = m$ gilt. Dadurch ergibt sich

$$g_0(af_n + h_0q) + h_0p_n \equiv f_n \mod (\Lambda)[X] \tag{2}$$

Durch das Streichen der Koeffizienten, die im von Λ erzeugten Ideal liegen, ändert sich nichts an (2). Bezeichne das Polynom $af_n + h_0q$ nach Eliminierung dieser Koeffizienten mit q_n. Es gelten $\deg(f_n) \leqslant d$, $\deg(g_0) = m$ und $\deg(h_0p_n) < d - m + m = d$.
Angenommen $\deg(q_n) > d-m$. Dann ist $\deg(g_0q_n) > m+d-m = d$. Wegen (2) muss sein Leitkoeffizient in (Λ) liegen. Dies steht im Widerspruch zur Definition des Polynoms q_n. Also gilt $\deg(q_n) \leqslant d-m$. Es gibt also p_i und q_i, die (1) erfüllen. □

Korollar 1.4.7
Sei $(K, |\cdot|)$ ein vollständiger und nicht-archimedischer Körper und sei $f = \sum_{i=0}^{n} a_iX^i \in K[X]$ ein normiertes und irreduzibles Polynom mit $f(0) \in \mathcal{O}$. Dann ist $f \in \mathcal{O}[X]$.

Beweis: Es wird zunächst gezeigt, dass $\max_{i=0,\dots,n}\{|a_i|\} = \max\{|a_0|, |a_n|\}$ für ein irreduzibles Polynom $f = \sum_{i=0}^{n} a_iX^i \in K[X]$ gilt. Sei $|a_r| = \max_{i=0,\dots,n}\{|a_i|\}$ mit r minimal. Dann liegt das Polynom $g := \frac{f}{a_r} = \sum_{i=0}^{n} \frac{a_i}{a_r}X^i$ in $\mathcal{O}[X]$ und ist weiterhin irreduzibel. Angenommen $\max\{|a_0|, |a_n|\} < |a_r|$. Dann ist $\frac{f}{a_r} \equiv X^r(1 + \frac{a_{r+1}}{a_r}X + \dots + \frac{a_n}{a_r}X^{n-r}) \mod \mathfrak{m}[X]$, wobei $r \notin \{0, n\}$. Die Polynome X^r und $(1 + \frac{a_{r+1}}{a_r}X + \dots + \frac{a_n}{a_r}X^{n-r})$ sind offenbar teilerfremd und keine Einheiten. Das ist aber ein Widerspruch, da keine Polynome existieren, die 1.4.6 erfüllen.
Für ein normiertes, irreduzibles Polynom $f = \sum_{i=0}^{n} a_iX^i \in K[X]$ ist dann $\max_{i=0,\dots,n}\{|a_i|\} = \max\{|a_0|, |a_n|\} = 1$. Damit ist $f \in \mathcal{O}[X]$. □

Für das folgende Theorem sind ein paar Erkenntnisse der Körpernorm und ganzer Elemente eines Rings notwendig. Diese sind [4] und [5] entnommen. In den Beweisen werden nur Hinweise auf die

Literatur gegeben.
Sei $R \subseteq S$ eine Ringerweiterung. Ein Element $s \in S$ heißt **ganz über R**, falls ein normiertes Polynom $f(X) \in R[X] \backslash \{0\}$ existiert, sodass $f(s) = 0$ ist. Die Menge aller über R ganzen Elemente in S heißt der **ganze Abschluss von R in S** und wird mit $\overline{R}^S$ bezeichnet.

Lemma 1.4.8
Für eine Ringerweiterung $R \subseteq S$ ist $\overline{R}^S$ ein Unterring von S.

Beweis: Siehe [4] S.8. □

Lemma 1.4.9
Sei $L|K$ eine endliche Körpererweiterung vom Grad n.

i) Für $a \in K$ gilt $N_{L|K}(a) = a^n$.

ii) Sei $n = qr$, wobei r der Separabilitätsgrad von $L|K$ ist und $f_i \in Hom_K(L, \overline{K})$ mit $i \in \{1, \ldots, r\}$ alle K-Homomorphismen von L nach $\overline{K}$ sind. Für $a \in L$ gilt $N_{L|K}(a) = (\prod_{i=1}^r f_i(a))^q$.

iii) Für $a \in L$ sei $m(X) = X^d + \ldots + a_0 \in K[X]$ das Minimalpolynom von a und $r = [L : K(a)]$. Dann ist $N_{L|K}(a) = (-1)^{dr} a_0^r$.

iv) Ist $L|K$ eine Galoiserweiterung, so ist $N_{L|K}(a) = \prod_{\sigma \in Gal(L|K)} \sigma(a)$.

Beweis: i) Siehe [5] §4.7 Lemma 2 (i).
ii) Siehe [5] §4.7 Satz 4.
iii) Siehe [5] §4.7 Lemma 2 (ii) und Lemma 3.
iv) Folgt sofort aus ii), da der Separabilitätsgrad und der Grad der Körpererweiterung gleich sind. □

Theorem 1.4.10
Sei $(K, |\cdot|)$ vollständiger und nicht-archimedischer Körper und sei $L|K$ eine endliche Körpererweiterung vom Grad n. Dann ist $|l|_L := \sqrt[n]{|N_{L|K}(l)|}$ die eindeutige Fortsetzung von $|\cdot|$ auf L. Insbesondere ist $(L, |\cdot|_L)$ vollständig.

Beweis: Sei $\mathcal{O}$ der Bewertungsring von K bzgl. $|\cdot|$ und $\overline{\mathcal{O}}^L$ sein ganzer Abschluss in L. Sei ferner $x \in \overline{\mathcal{O}}^L$ und $g(X) := X^d + a^{d-1}X^{d-1} + \ldots + a_0 \in \mathcal{O}[X]$ mit $g(x) = 0$. Für $f \in Hom_K(L, \overline{K})$ ist auch $f(x)$ ein ganzes Element, da

$$0 = g(x) = f(g(x)) = f(x)^d + a^{d-1}(f(x))^{d-1} + \ldots + a_0.$$

Nach 1.4.8 ist $\overline{\mathcal{O}}^L$ ein Ring. Sei q der Inseparabilitätsgrad von $L|K$. Das Element $N_{L|K}(x) = (\prod_{f \in Hom_K(L,\overline{K})} f(x))^q$ liegt in K und wegen seiner Ganzheit in $\overline{\mathcal{O}}^K$. Es liegt sogar in $\mathcal{O}$. Angenommen $N_{L|K}(x) \in K \backslash \mathcal{O}$. Sei $h(X) := X^e + X^{e-1}b_{e-1} + \ldots + b_0 \in \mathcal{O}[X]$ mit $h(N_{L|K}(x)) = 0$. Das Polynom $k(X) := X + (b_{e-1} + \frac{b_{e-2}}{N_{L|K}(x)} + \ldots + \frac{b_0}{N_{L|K}(x)^{e-1}})$ liegt offensichtlich in $\mathcal{O}[X]$. Darüberhinaus ist $k(N_{L|K}(x)) = 0$, da $k(N_{L|K}(x)) = \frac{h(N_{L|K}(x))}{N_{L|K}(x)^{e-1}}$ ist. Dies würde aber bedeuten, dass das additive Inverse von $b_{e-1} + \frac{b_{e-2}}{N_{L|K}(x)} + \ldots + \frac{b_0}{N_{L|K}(x)^{e-1}}$ in $K \backslash \mathcal{O}$. Dies ist ein Widerspruch, da $\mathcal{O}$ ein Ring ist. Damit wurde gezeigt, dass $\overline{\mathcal{O}}^L \subseteq \{l \in L : N_{L|K}(l) \in \mathcal{O}\}$. Nun wird die umgekehrte Inklusion gezeigt.

Sei dazu $x \in L^\times$ mit $N_{L|K}(x) \in \mathcal{O}$ und $f := X^r + \sum_{i=0}^{r-1} a_i X^i \in K[X]$ sein Minimalpolynom über K und $[L : K(x)] = s$. Dann ist nach 1.4.9 iii) $N_{L|K}(x) = (-1)^{rs} a_0^s \in \mathcal{O}$. Dann ist $a_0 \in \mathcal{O}$. Mit 1.4.7 folgt, dass $f \in \mathcal{O}[X]$ und somit $x \in \overline{\mathcal{O}}_L$. Damit gilt

$$\overline{\mathcal{O}}^L = \{l \in L : N_{L|K}(l) \in \mathcal{O}\}. \tag{3}$$

Die ersten beiden Bedingungen eines Absolutbetrags erfüllt $|\cdot|_L$ offensichtlich. Es ist also nur noch die verschärfte Dreiecksungleichung zu zeigen. Seien dazu $a, b \in L$ mit $|a|_L \leqslant |b|_L \neq 0$. Dann ist $|\frac{a}{b}|_L \leqslant 1$. Wegen (3) ist $\frac{a}{b} \in \overline{\mathcal{O}}^L$. Damit ist auch sofort $\frac{a}{b} + 1 \in \overline{\mathcal{O}}^L$. Mit (3) gilt dann die Implikation $|\frac{a}{b}|_L \leqslant 1 \Rightarrow |\frac{a}{b}+1|_L \leqslant 1$. Also gilt folgende Implikation $|a|_L \leqslant |b|_L \Rightarrow |a+b|_L \leqslant |b|_L = \max\{|a|_L, |b|_L\}$. Da nach 1.4.9 i) $N_{L|K}(k) = k^n$ für alle $k \in K$ ist $|\cdot|_L$ eine Fortsetzung von K auf L mit Bewertungsring $\overline{\mathcal{O}}^L$.

Nun wird gezeigt, dass $|\cdot|_L$ eindeutig ist. Sei dazu $|\cdot|_K$ eine weitere Fortsetzung mit Bewertungsring $\mathcal{O}'$ und maximalem Ideal $\mathfrak{m}'$. Angenommen es gibt $a \in \overline{\mathcal{O}}^L \backslash \mathcal{O}'$. Dann ist $|a|_K > 1$, also $a^{-1} \in \mathcal{O}'$. Sei $f = X^d + \sum_{i=0}^{d-1} b_i X^i$ das Minimalpolynom von a über K. Dann ist $b_i \in \mathcal{O}$ für alle i und somit gilt $1 = -\sum_{i=0}^{d} b_i (a^{-1})^i \in \mathfrak{m}'$. Dies ist ein Widerspruch, da $\mathfrak{m}'$ keine Einheiten enthält. Somit gilt $\overline{\mathcal{O}}^L \subseteq \mathcal{O}'$. Sei $\mathfrak{m}$ das maximale Ideal von $\overline{\mathcal{O}}^L$. Die Menge $\mathfrak{m}' \cap \overline{\mathcal{O}}^L$ ist ein von Null verschiedenes Primideal von $\overline{\mathcal{O}}^L$ und somit gilt $\mathfrak{m} = \mathfrak{m}' \cap \overline{\mathcal{O}}^L \subseteq \mathfrak{m}'$. Dies ist äquivalent zur Implikation $|a|_L < 1 \Rightarrow |a|_K$. Mit 1.2.4 folgt die Äquivalenz der beiden Absolutbeträge. Da $|k| = |k|_L = |k|_K$ für alle $k \in K$ gilt und wegen 1.2.3 ein $s \in \mathbb{R}_{>0}$ gibt, sodass $|l|_L = |l|_K^s$ für alle $l \in L$, ist $s = 1$ und die Absolutbeträge gleich. Mit 1.4.4 folgt die Vollständigkeit von L. □

Korollar 1.4.11

Sei $(K, |\cdot|)$ ein vollständiger und nicht-archimedischer Körper und sei $L|K$ eine algebraische Körpererweiterung. Dann gibt es eine eindeutige Fortsetzung von $|\cdot|$ auf L.

Beweis: Da jede algebraische Erweiterung die Vereinigung seiner endlichen Teilerweiterungen ist, genügt es die Aussage für den endlichen Fall zu betrachten, also 1.4.10. □

Lemma 1.4.12

Sei $L|K$ eine Galoiserweiterung mit $[L : K] = n$. Dann ist jedes Element der Galoisgruppe eine Isometrie.

Beweis: Für alle $x \in L$ einer Galoiserweiterung $L|K$ gilt nach 1.4.9 iv)
$N_{L|K}(x) = \prod_{\sigma \in Gal(L|K)} \sigma(x)$. Damit ist mit der Normfortsetzung aus 1.4.10 und $\sigma' \in G := Gal(L|K)$

$$|\sigma'(x)|_L = \sqrt[n]{|N_{L|K}(\sigma'(x))|} = \sqrt[n]{|\prod_{\sigma \in G} \sigma \circ \sigma'(x)|} = \sqrt[n]{|\prod_{\sigma \in G} \sigma(x)|} = |x|_L.$$

□

Lemma 1.4.13

Sei $(K, |\cdot|)$ ein vollständiger, nicht-archimedischer Körper, $K \subseteq L \subseteq \overline{K}$ und $\alpha \in \overline{K}$ separabel über L.

Seien $\alpha := \alpha_1, \alpha_2, \ldots, \alpha_n \in \overline{K}$ die Nullstellen des Minimalpolynoms m von α über L. Gilt für $\beta \in \overline{K}$ die Abschätzung $|\alpha - \beta| < \min\{|\alpha - \alpha_i| : 2 \leqslant i \leqslant n\}$, so ist $L(\alpha) \subseteq L(\beta)$.

Beweis: Im Fall $n = 1$, also $\alpha \in L$ gilt obige Inklusion für alle $\beta \in \overline{K}$. Sei also $n \geqslant 2$ und $\beta \in \overline{K}$ mit $\alpha \notin L(\beta)$. Sei ferner $L'|L(\beta)$ der Zerfällungskörper des Minimalpolynoms m' von α über $L(\beta)$. Damit ist $L'|L(\beta)$ eine Galoiserweiterung vom Grad $\geqslant 2$. Da m' das Polynom m teilt, ist $(\sigma(\alpha))_{\sigma \in Gal(L'|L(\beta))}$ eine Teilfamilie von $(\alpha_i)_{i \in \{1,\ldots,n\}}$ und da $ord(Gal(L'|L(\beta))) = [L' : L(\beta)] \geqslant 2$ ist, gibt es ein $\sigma \in Gal(L'|L(\beta))$ für ein $i_0 \in \{2, \ldots, n\}$ mit $\sigma(\alpha) = \alpha_{i_0}$. Die Nullstellen $\alpha_1, \ldots, \alpha_n$ sind paarweise verschieden, da m separabel ist. Da $L(\beta)^{Gal(L'|L(\beta))} = L(\beta)$ und Elemente der Galoisgruppe Isometrien sind, ist

$$|\beta - \alpha_{i_0}| = |\beta - \sigma(\alpha)| = |\sigma(\beta - \alpha)| = |\beta - \alpha|.$$

Damit ist

$$\min_{2 \leqslant i \leqslant n} \{|\alpha - \alpha_i|\} \leqslant |\alpha - \alpha_{i_0}| \leqslant \max\{|\alpha - \beta|, |\beta - \alpha_{i_0}|\} = |\beta - \alpha|.$$

□

Korollar 1.4.14
Sei $(K, |\cdot|)$ ein vollständiger, nicht-archimedischer Körper. Seien ferner $K \subseteq L \subseteq \overline{K}$, $\alpha \in \overline{K}$ separabel über L und $m \in L[X]$ sein Minimalpolynom über L. Es gibt eine nur von α abhängige reelle Konstante $\epsilon > 0$, sodass jedes normierte Polynom $f \in L[X]$ vom Grad $n := \deg(m)$ mit $||f - m|| < \epsilon$ eine Nullstelle $\beta \in L(\alpha)$ besitzt mit $L(\beta) = L(\alpha)$, wobei $|| \cdot ||$ die Gauß-Norm ist.

Beweis: Seien $f(X) = \prod_{j=1}^n (X - \beta_j) = \sum_{i=0}^n b_i X^i$ und $m(X) = \prod_{i=1}^n (X - \alpha_i) = \sum_{i=0}^n a_i X^i$ mit $\beta_j, \alpha_i \in \overline{K} = \overline{L}$. Dann ist

$$\prod_{j=1}^{n} (\alpha - \beta_j) = f(\alpha) = f(\alpha) - m(\alpha). \tag{4}$$

Offenbar ist $M := \max\{|\alpha|^i : 0 \leqslant i \leqslant n\} = \max\{1, |\alpha|^n\}$. Wegen (4) gilt

$$\prod_{j=1}^{n} |\alpha - \beta_j| = |\sum_{i=0}^{n} (b_i - a_i)\alpha^i| \leqslant ||f - m||M.$$

Sei $j_0 \in \{1, \ldots, n\}$ mit $|\alpha - \beta_{j_0}| \leqslant |\alpha - \beta_j|$ für alle $j \in \{1, \ldots, n\}$. Dann ist $|\alpha - \beta_{j_0}|^n \leqslant \prod_{j=1}^n |\alpha - \beta_j| \leqslant ||f - m||M$ und somit $|\alpha - \beta_{j_0}| \leqslant ||f - m||^{\frac{1}{n}} M^{\frac{1}{n}}$. Für f mit $||f - m|| < M^{-1}(\min\{|\alpha - \alpha_i| : 2 \leqslant i \leqslant n\})^n = \epsilon$ gilt nach 1.4.13 $L(\alpha) \subseteq L(\beta_{j_0})$. Da $[L(\beta_{j_0}) : L] \leqslant \deg(f) = n = [L(\alpha) : L]$ ist, gilt sogar Gleichheit. □

Lemma 1.4.15
Sei $(F, |\cdot|)$ ein nicht-archimedischer Körper. Ist F separabel abgeschlossen, so ist $\widehat{F}$ algebraisch abgeschlossen.

Beweis: Sei F separabel abgeschlossen. Zunächst wird gezeigt, dass F dicht in $\overline{F}$ liegt und anschließend, dass $\widehat{F}$ separabel abgeschlossen ist. In Charakteristik 0 ist $F^{sep} = \overline{F}$, also $F = \overline{F}$. Sei also $char(F) = p > 0$ und $\alpha \in \overline{F}$. Da F separabel abgeschlossen ist, ist die Körpererweiterung $\overline{F}|F$ rein-inseparabel. Damit existiert ein $m \geqslant 0$ mit $a = \alpha^{p^m} \in F$ und $X^{p^m} - a$ ist das Minimalpolynom von α über F. Im Fall $m = 0$ ist $\alpha \in F$. Sei also $m \geqslant 1$ und $\epsilon \in \mathbb{R}_{\geqslant 0}$. Sei ferner $a_1 \in F$ mit $0 < |a_1| < \frac{\epsilon^{p^m}}{|\alpha|}$

und $f(X) := X^{p^m} + a_1X - a$. Da $a_1 \neq 0$ ist, gilt $\gcd(f(X), f'(X)) = \gcd(X^{p^m} + a_1X - a, a_1) = 1$. Das Polynom f ist also separabel. Mit F' wird der Zerfällungskörper von f bezeichnet. Da F separabel abgeschlossen und $K'|K$ eine separable Körpererweiterung ist, ist $F' = F$. Damit gibt es $\beta_j \in F$ mit $f(X) = \prod_{j=1}^{p^m}(X - \beta_j)$. Insbesondere ist $\prod_{j=1}^{p^m}(\alpha - \beta_j) = f(\alpha) = a_1\alpha$ und somit ist $\prod_{j=1}^{p^m}|\alpha - \beta_j| = |a_1\alpha| < \epsilon^{p^m}$. Dies impliziert die Existenz eines $j \in \{1, \ldots, p^m\}$ mit $|\alpha - \beta_j| < \epsilon$. Der Körper F liegt demnach dicht in seinem algebraischen Abschluss. Nun wird gezeigt, dass $\widehat{F}$ separabel abgeschlossen ist. Sei $E|\widehat{F}$ eine endliche separable Körpererweiterung und o.B.d.A. eine Galoiserweiterung. Für $x \in E$ sei $m(X) = X^d + \alpha_{d-1}X^{d-1} + \ldots + \alpha_0$ sein Minimalpolynom über $\widehat{F}$. Angenommen x liegt nicht in $\widehat{F}$. Dann ist $d > 1$. Seien $x = x_1, x_2, \ldots, x_d$ die Nullstellen von m. Da F in $\overline{F}$ dicht liegt sind nach 1.3.10 die Körper $\widehat{F}$ und $\widehat{\overline{F}}$ ismorph, also ist $\overline{F} \subseteq \widehat{F}$. Damit gibt es $\beta_i \in \overline{F}$ mit

$$|\alpha_i - \beta_i|^\wedge < \frac{\min\limits_{2 \leqslant j \leqslant d}\{|x - x_j|^\wedge\}^d}{\max\limits_{0 \leqslant j \leqslant d-1}\{(|x|^\wedge)^j\}} \tag{5}$$

für alle $0 \leqslant i \leqslant d-1$, da wegen der Separabilität von m alle Nullstellen x_i verschieden sind und somit $\min_{2 \leqslant j \leqslant d}\{|x - x_j|^\wedge\} \neq 0$ ist. Seien $b_1, \ldots, b_d$ die Nullstellen von $f(X) := X^d + \beta_{d-1}X^{d-1} + \ldots + \beta_0 \in \overline{F}[X]$. Da $\overline{F}$ algebraisch abgeschlossen ist, ist $f(X) = \prod_{i=1}^{d}(X - b_i) \in \overline{F}[X]$. Damit ist $\prod_{i=1}^{d}(x - b_i) = f(x) = f(x) - m(x) = \sum_{i=0}^{d-1}(\alpha_i - \beta_i)x^i$. Durch das Anwenden der starken Dreiecksungleichung folgt

$$\prod_{i=1}^{d}|x - b_i|^\wedge \leqslant \max_{0 \leqslant i \leqslant d-1}\{|\alpha_i - \beta_i|^\wedge\} \max_{0 \leqslant j \leqslant d-1}\{(|x|^\wedge)^j\} \overset{(5)}{<} \min_{2 \leqslant j \leqslant d}\{|x - x_j|^\wedge\}^d.$$

Daher gibt es ein $i \in \{1, \ldots, d\}$ mit $|x - b_i|^\wedge < \min_{2 \leqslant j \leqslant d-1}\{(|x - x_j|^\wedge\}$. Sei $j \in \{2, \ldots, d\}$. Dann gibt es ein $\sigma \in Gal(E|\widehat{F})$ mit $\sigma(x) = x_j$. Da $b_i \in \overline{F} \subseteq \widehat{F}$, ist $\sigma(b_i) = b_i$ und somit $\sigma(x - b_i) = x_j - b_i$. Nach 1.4.12 sind Elemente aus $Gal(E|\widehat{F})$ Isometrien und somit gilt

$$\begin{aligned} |x - x_j|^\wedge &= |x - b_i + b_i - x_j|^\wedge \leqslant \max\{|x - b_i|^\wedge, |\sigma(x - b_i)|^\wedge\} \\ &= |x - b_i|^\wedge < |x - x_j|^\wedge. \end{aligned}$$

Damit muss $d = 1$ sein, also $x \in E$. Also ist $\widehat{F}$ ist separabel abgeschlossen.
Im Folgenden wird gezeigt, dass $\widehat{F}$ algebraisch abgeschlossen ist. Ist $char(F) = 0$, so gilt auch $char(\widehat{F}) = 0$ und somit $\overline{\widehat{F}} = (\widehat{F})^{sep} = \widehat{F}$, da $\widehat{F}$ separabel abgeschlossen ist.
Sei also $char(F) = p > 0$. Da $(\widehat{F})^{sep}$ separabel abgeschlossen ist, liegt dieser Körper dicht in seinem algebraischen Abschluss $\overline{(\widehat{F})^{sep}} = \overline{\widehat{F}}$. Nach 1.3.10 sind ihre Vervollständigungen isomorph und es ergibt sich die Gleichung $\widehat{\overline{\widehat{F}}} = \widehat{(\widehat{F})^{sep}} = \widehat{\widehat{F}} = \widehat{F}$. Damit ist $\widehat{F} \subseteq \overline{\widehat{F}} \subseteq \widehat{\overline{\widehat{F}}} = \widehat{F}$ und somit $\widehat{F} = \overline{\widehat{F}}$. □

Lemma 1.4.16
Sei $(K, |\cdot|)$ ein vollständiger, nicht-archimedischer Körper und $K \subseteq L \subseteq \overline{K}$, sodass $\widehat{L}$ algebraisch abgeschlossen ist. Dann gilt $K^{sep} \subseteq L$ und L ist separabel abgeschlossen.

Beweis: Sei $\alpha \in K^{sep}$. Dann ist α auch separabel über L. Sei ferner $m \in L[X]$ sein Minimalpolynom über L. Da $\widehat{L}$ algebraisch abgeschlossen ist, gilt $m(X) = \prod_{i=1}^{n}(X - \alpha_i)$ mit $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n \in \widehat{L}$. Wegen der Separabilität von m gilt sogar $\alpha_1, \ldots, \alpha_n \in \widehat{L} \cap L^{sep}$. Sei $C_n := \max\{1, |\alpha_1|, \ldots, |\alpha_n|\}$. Es gibt $\beta_1, \ldots, \beta_n \in L$, sodass für alle $i \in \{1, \ldots, n\}$ die Abschätzung $|\alpha_i - \beta_i| < \frac{\epsilon}{C_n^n}$ mit ϵ wie in 1.4.14, da L dicht in $\widehat{L}$ liegt. Für $f(X) := \prod_{i=1}^{n}(X-\beta_i) \in L[X]$ wird nun induktiv nach $n \geqslant 1$ die Gültigkeit der Ungleichung

$$||f-m|| \leqslant C_n^n \max\{|\alpha_i - \beta_i| : 1 \leqslant i \leqslant n\} < \epsilon \tag{6}$$

gezeigt. Für $n = 1$ ist

$$\begin{aligned} ||(X-\beta_1)-(X-\alpha_1)|| &= |\alpha_1 - \beta_1| \leqslant \max\{1, |\alpha_1|\}|\alpha_1 - \beta_1| \\ &= C_1^1 \max\{|\alpha_i - \beta_i| : 1 \leqslant i \leqslant 1\}. \end{aligned}$$

Gelte nun (6) für alle natürlichen Zahlen $\leqslant n$. Für alle $i \in \{1, \ldots, n\}$ gilt die Ungleichung $|\alpha_i - \beta_i| < 1$. Per Konstruktion der β_i gilt nämlich $|\alpha_i - \beta_i| < \frac{\epsilon}{C_n^n}$. Im Beweis von 1.4.14 war zu sehen, dass $\epsilon = \frac{\min\{|\alpha-\alpha_i| : 2 \leqslant i \leqslant n\}^n}{\max\{1, |\alpha|^n\}}$ ist. Die starke Dreiecksungleichung und eine Fallunterscheidung liefert

$$\frac{\epsilon}{C_n^n} = \frac{\min\{|\alpha - \alpha_i| : 2 \leqslant i \leqslant n\}^n}{\max\{1, |\alpha|^n\} \max\{1, |\alpha_1|, \ldots, |\alpha_n|\}^n} \leqslant 1.$$

Damit ist $||(X-\alpha_i)-(X-\beta_i)|| = |\alpha_i - \beta_i| < 1 \leqslant ||X - \alpha_i||$. Mit der starken Dreiecksungleichung folgt

$$\begin{aligned} ||X - \beta_i|| &= ||(X-\beta_i)-(X-\alpha_i)+(X-\alpha_i)|| = ||X-\alpha_i|| \\ &= \max\{1, |\alpha_i|\} \leqslant C_{n+1}. \end{aligned}$$

Es gilt

$$\begin{aligned} \prod_{i=1}^{n+1}(X-\alpha_i) - \prod_{i=1}^{n+1}(X-\beta_i) &= (X-\alpha_1)(\prod_{i=2}^{n+1}(X-\alpha_i) - \prod_{i=2}^{n+1}(X-\beta_i)) \\ &\quad +(\beta_1 - \alpha_1)\prod_{i=2}^{n+1}(X-\beta_i). \end{aligned} \tag{7}$$

Sei $g := (X-\alpha_1)(\prod_{i=2}^{n+1}(X-\alpha_i) - \prod_{i=2}^{n+1}(X-\beta_i))$ und $h := (\beta_1 - \alpha_1)\prod_{i=2}^{n+1}(X-\beta_i)$. Für g gilt nach Induktionsvoraussetzung

$$\begin{aligned} ||g|| &\leqslant ||X-\alpha_1|| \max\{1, |\alpha_2|, \ldots, |\alpha_{n+1}|\}^n \max\{|\alpha_i - \beta_i| : 2 \leqslant i \leqslant n+1\} \\ &\leqslant C_{n+1}C_{n+1}^n \max\{|\alpha_i - \beta_i| : 2 \leqslant i \leqslant n+1\} \\ &= C_{n+1}^{n+1} \max\{|\alpha_i - \beta_i| : 2 \leqslant i \leqslant n+1\}. \end{aligned}$$

. Wegen (1.4) gilt für h

$$||h|| = |\beta_1 - \alpha_1| \prod_{i=2}^{n+1} ||X - \beta_i|| \leqslant |\beta_1 - \alpha_1| C_{n+1}^{n+1}.$$

Durch Anwenden von $||\cdot||$ auf (7) folgt

$$\begin{aligned} ||f-m|| &\leqslant \max\{||g||, ||h||\} \\ &\leqslant \max\{C_{n+1}^{n+1}\max\{|\alpha_i - \beta_i| : 2 \leqslant i \leqslant n+1\}, C_{n+1}^{n+1}|\beta_1 - \alpha_1|\} \\ &= C_{n+1}^{n+1} \max\{|\alpha_i - \beta_i| : 1 \leqslant i \leqslant n+1\}. \end{aligned}$$

Damit gilt (6). Nach 1.4.14 besitzt f eine Nullstelle $\beta \in L(\alpha)$ mit $L(\alpha) = L(\beta)$. Alle Nullstellen von f liegen aber in L und somit ist $L(\alpha) = L$, also liegt α in L. □

1.5 Projektiver Limes

Sei I eine Menge mit Halbordnung $\leqslant$, sodass für alle $i, j \in I$ ein $k \in I$ existiert mit $i \leqslant k$ und $j \leqslant k$. Ein **projektives System** $((M_i)_{i\in I}, (f_{ij})_{\substack{i,j\in I \\ i\leqslant j}})$ von Objekten desselben Typs (von Mengen, Gruppen, Ringen) über I ist eine Familie $(M_i)_{i\in I}$ von Objekten desselben Typs (Mengen, Gruppen, Ringen) M_i mit Morphismen (Abbildungen, Gruppenhomomorphismen, Ringhomomorphismen) $f_{ij} : M_j \to M_i$ für alle $i, j \in I$ mit $i \leqslant j$, sodass gilt:

i) $f_{ii} = id_{M_i}$ für alle $i \in I$

ii) für alle $i, j, k \in I$ mit $i \leqslant j \leqslant k$ gilt $f_{ik} = f_{ij} \circ f_{jk}$.

Sei $((M_i)_{i\in I}, (f_{ij})_{\substack{i,j\in I \\ i\leqslant j}})$ ein projektives System über I. Dann heißt

$$\varprojlim_{i\in I} M_i := \{(m_i)_{i\in I} \in \prod_{i\in I} M_i : f_{ij}(m_j) = m_i\}$$

projektiver Limes zum projektiven System $((M_i)_{i\in I}, (f_{ij})_{\substack{i,j\in I \\ i\leqslant j}})$.

Proposition 1.5.1

Sei $((M_i)_{i\in I}, (f_{ij})_{\substack{i,j\in I \\ i\leqslant j}})$ ein projektives System über I und N ein Objekt desselben Typs (Menge, Gruppe, Ring) mit Homomorphismen $g_j : N \to M_j$ für alle $j \in I$, sodass $f_{ij} \circ g_j = g_i$ für $i, j \in I$ mit $i \leqslant j$ gilt. Dann gibt es genau einen Homomorphismus g, sodass das Diagramm

$$\begin{tikzcd} N \arrow[r, "g"] \arrow[dr, "g_j"'] & \varprojlim_{i\in I} M_i \arrow[d, "pr_j"] \\ & M_j \end{tikzcd}$$

mit $pr_j((m_i)_{i\in I}) = m_j$ für alle $j \in I$ kommutiert.

Beweis: Sei $n \in N$ und

$$\begin{array}{rccl} g: & N & \to & \varprojlim_{i\in I} M_i \\ & n & \mapsto & (g_i(n))_{i\in I} \end{array}$$

Es gilt $g_i(n) = f_{ij} \circ g_j(n)$ für alle $i, j \in I$ mit $i \leqslant j$. Damit ist g wohldefiniert.
Angenommen es gibt $\tilde{g} \neq g$, sodass das Diagramm

$$\begin{tikzcd} N \arrow[r, "\tilde{g}"] \arrow[dr, "g_j"'] & \varprojlim_{i\in I} M_i \arrow[d, "pr_j"] \\ & M_j \end{tikzcd}$$

kommutiert. Dann gibt es $n \in N$ mit $(x_i)_{i\in I} = \tilde{g}(n) \neq g(n) = (y_i)_{i\in I}$, d.h. es gibt ein $i \in I$ mit $x_i \neq y_i$. Dann ist $pr_i \circ \tilde{g}(n) = x_i \neq y_i = pr_i \circ g(n) = g_i(n)$. Dies widerspricht der Kommutativität. □

Lemma 1.5.2
Der projektive Limes eines projektiven Systems von Ringen, Gruppen, etc ist bzgl. der komponentenweise Verknüpfung(en) ein Ring, Gruppe, etc.

Beweis: folgt unmittelbar. □

Lemma 1.5.3
Sei R ein Ring und $(M_j)_{j\in\mathbb{N}}$ eine Familie von $R-$Untermoduln von M, sodass $M_0 \supseteq M_1 \supseteq M_2 \supseteq ...$ und sei $x + M_j := \{x + y : y \in M_j\}$ die Nebenklasse von $x \in M$ für $j \in \mathbb{N}$. Dann definiert die Menge

$$\tau_M := \{U \subseteq M : \text{für alle } x \in U \text{ existiert ein } j \in \mathbb{N}, \text{ sodass } x + M_j \subseteq U \text{ ist } \}$$

eine Topologie auf M.

Beweis: Es gilt offensichtlich $\varnothing$, $M \in \tau_M$.
Seien $L \subseteq \tau_M$ und $x \in \bigcup_{U\in L} U$. Dann gibt es ein $U_0 \in L$ und ein $k \in \mathbb{N}$, sodass $x \in U_0$ und $x + M_k \subseteq U_0 \subseteq \bigcup_{U\in L} U$ ist.
Für $U_1, U_2 \in \tau_M$ ist auch $U_1 \cap U_2 \in \tau_M$, denn für $x \in U_1 \cap U_2 \in \tau_M$ gibt es $i, j \in \mathbb{N}$ mit $x + M_i \subseteq U_1$ und $x + M_j \subseteq U_2$. Dann gilt $x + M_{\min\{i,j\}} \subseteq U_1 \cap U_2$. □

Sei p eine Primzahl. Ist $M = R$ und sind die $M_j = p^j R$, so heißt τ_R **p-adische Topologie**. Die durch den p-adischen Absolutbetrag induzierte Topologie auf einem Bewertungsring $\mathcal{O}_K$ der Charakteristik Null ist die p-adische Topologie, da für $x \in \mathcal{O}_K = R$ und $\epsilon > 0$ ein $N \in \mathbb{N}$ mit $0 < |p^N| < \epsilon$ existiert und somit $B_{|\cdot|_p}(x, \epsilon) \supseteq B_{|\cdot|_p}(x, p^N) = \{y \in \mathcal{O}_K : x - y \in p^N \mathcal{O}_K\} = x + p^N \mathcal{O}_K$. Analog gilt:

Lemma 1.5.4
Sei $\mathcal{O}$ ein diskreter Bewertungsring, mit seinem maximalen Ideal $\mathfrak{m} = (\pi)$. Dann entspricht die in 1.5.3 definierte Topologie mit $\mathcal{O} \supseteq \mathfrak{m} \supseteq \mathfrak{m}^2 \supseteq \mathfrak{m}^3 \supseteq ...$ genau der durch den Absolutbetrag induzierten Topologie.

Beweis: Es genügt zu zeigen, dass für $x \in \mathcal{O}$ und $q \in \mathbb{N}\backslash\{0\}$ gilt $x + \mathfrak{m}^j = \{y \in \mathcal{O} : |x - y| < q^{-j+1}\} = B(x, q^{-j+1})$, wobei $|x| = q^{-\nu(x)}$. Dann ist

$$\begin{aligned} y \in B(x, q^{-j+1}) \quad &\Leftrightarrow \quad \nu(x-y) > j-1 \quad \Leftrightarrow \quad \nu(x-y) \geqslant j \\ &\Leftrightarrow \quad x - y \in \mathfrak{m}^j \quad \Leftrightarrow \quad y \in x + \mathfrak{m}^j. \end{aligned}$$

□

Lemma 1.5.5
Seien R und S Ringe und sei $\vartheta : R \to S$ ein Ringhomomorphismus. Dann ist ϑ bzgl. der p-adischen Topologie auf R und S stetig.

Beweis: Sei $V \subseteq S$ offen und sei $x \in \vartheta^{-1}(V) \subseteq R$. Das bedeutet $\vartheta(x) \in V$. Damit gibt es ein $n \in \mathbb{N}$ mit $\vartheta(x) + p^n y \in V$ für alle $y \in S$. Für alle $m \in R$ ist somit $\vartheta(x + p^n m) = \vartheta(x) + p^n \vartheta(m) \in V$. $\vartheta^{-1}(V)$ ist offen, da $x + p^n R \subseteq \vartheta^{-1}(V)$. □

Sei R ein Ring und $(M_j)_{j\in\mathbb{N}}$ eine Familie von $R-$Untermoduln von M wie in 1.5.3. Dann heißt eine Folge $(x_j)_{j\geqslant 0}$ mit $x_j \in M$ **Cauchyfolge**, wenn für alle $j \in \mathbb{N}$ ein $N \in \mathbb{N}$ existiert, sodass für alle

$m, n \geqslant N$ gilt $\mathrm{x}_n - x_m \in M_j$.
$(\mathrm{x}_j)_{j\geqslant 0}$ heißt **konvergent**, wenn ein $x \in M$ existiert, sodass für alle $j \in \mathbb{N}$ ein $N \in \mathbb{N}$ existiert, sodass für alle $n \geqslant N$ gilt $x - x_n \in M_j$.
M ist **vollständig**, wenn jede Cauchyfolge konvergiert.

Lemma 1.5.6
Seien R, M, $(M_j)_{j\in\mathbb{N}}$ wie oben und sei $f_{ij} : M/M_j \to M/M_i$, $m + M_j \mapsto m + M_i$. Dann ist $((M/M_i)_{i\in\mathbb{N}}, (f_{ij})_{\substack{i,j\in\mathbb{N}\\ i\leqslant j}})$ ein projektives System.

Beweis: Es gilt offensichtlich $f_{ii} = id_{M/M_i}$. Sei $i \leqslant j$, dann gilt $M_i \supseteq M_j$ und damit ist f_{ij} wohldefiniert und offenbar gilt $f_{ik} = f_{ij} \circ f_{jk}$ für $i \leqslant j \leqslant k$. □

Proposition 1.5.7
Sei $((M/M_i)_{i\in\mathbb{N}}, (f_{ij})_{\substack{i,j\in\mathbb{N}\\ i\leqslant j}})$ *das projektive System wie in 1.5.6 und sei*

$$\begin{aligned} g: \quad M &\to \varprojlim_{i\in\mathbb{N}} M/M_i \\ m &\mapsto (m + M_i)_{i\geqslant 0}. \end{aligned}$$

Dann gelten

i) g ist genau dann injektiv , wenn $\bigcap\limits_{i\in\mathbb{N}} M_i = 0$ ist.

ii) M ist genau dann bezüglich der Topologie in 1.5.3 vollständig, wenn g surjektiv ist.

Beweis: Offensichtlich ist g ein R-Modul Homomorphismus. Aussage i) gilt, da offenbar $\ker(g) = \bigcap_{j\in\mathbb{N}} M_j$ ist.
Sei g surjektiv und sei $(x_j)_{j\geqslant 0}$ eine Cauchyfolge in M. Sei $j \in \mathbb{N}$. Dann gibt es $N_j \in \mathbb{N}$, sodass für alle $n \geqslant N_j$ gilt $x_n - x_{N_j} \in M_j$. Damit wird die Folge $(x_m + M_j)_{m\geqslant 0}$ in M/M_j stationär. Die Folge $y = (x_{N_j} + M_j)_{j\geqslant 0}$ liegt in $\varprojlim\limits_{i\in\mathbb{N}} M/M_i$, da für $i \leqslant j$ und $n \geqslant \max\{N_i, N_j\}$ gilt

$$f_{ji}(x_{N_i} + M_i) = x_{N_i} + M_j = x_n + M_j = x_{N_j} + M_j.$$

Da g surjektiv ist, gibt es ein $x \in M$ mit $g(x) = y$. Somit ist $g(x) = (x + M_j)_{j\geqslant 0} = (x_{N_j} + M_j)_{j\geqslant 0}$, also liegt für alle $j \in \mathbb{N}$ die Differenz $x - x_{N_j}$ in M_j. Für alle $j \in \mathbb{N}$ und für alle $n \geqslant N_j$ gilt $x - x_n = x - x_{N_j} + x_{N_j} - x_n \in M_j$. Damit ist $x \in M$ der Grenzwert der Folge $(x_j)_{j\geqslant 0}$.
Sei nun M vollständig und sei $(x_j + M_j)_{j\geqslant 0} \in \varprojlim_{i\in\mathbb{N}} M/M_i$. Nach Definition des projektiven Limes ist $x_i - x_j \in M_i$ für alle $i \leqslant j$. Für $n, m \geqslant j$ gilt somit $x_n - x_m = x_n - x_j + x_j - x_m \in M_j$. Damit ist die Folge $(x_j)_{j\geqslant 0}$ eine Cauchyfolge in M und konvergiert in M. Sei x sein Grenzwert. Für $j \in \mathbb{N}$ wähle $n \geqslant j$ mit $x - x_n \in M_j$. Dann ist $x - x_n + x_n - x_j \in M_j$. Also ist $x + M_j = x_j + M_j$ für alle $j \in \mathbb{N}$ und somit ist $(x_j + M_j)_{j\geqslant 0} = (x + M_j)_{j\geqslant 0} = g(x)$. □

Korollar 1.5.8
Für einen vollständigen diskreten Bewertungsring $\mathcal{O}$ mit seinem maximalen Ideal $\mathfrak{m}$ ist der Ringhomomorphismus

$$\begin{array}{rcl} \mathcal{O} & \to & \varprojlim_{n\in\mathbb{N}} \mathcal{O}/\mathfrak{m}^n \\ r & \mapsto & (r+\mathfrak{m}^n)_{n\geqslant 0} \end{array}$$

ein Ringisomorphismus.

Beweis: Die Behauptung folgt unmittelbar aus 1.5.7 und 1.5.4. □

2 Tilting eines perfektoiden Körpers

In diesem Kapitel wird aus einem perfektoiden Körper K der Charakteristik 0 mit $char(\mathcal{O}/\mathfrak{m}) = p$ ein perfektoider Körper der Charakteristik p konstruiert, der sogenannte Tilt von K. Für eine Menge $S \subseteq K$ ist $|S| := \{|s| : s \in S\}$.
Die Grundlage für dieses Kapitel bildete die Vorlesung „p-adic Galois representations “ von Herrn Prof. Dr. Kohlhaase.

Sei $(K, |\cdot|)$ nicht-archimedischer Körper mit $char(\mathcal{O}_K/\mathfrak{m}) = p$. Er heißt **perfektoid**, falls folgende Bedingungen erfüllt sind:

i) K ist vollständig

ii) $|K^\times| \subseteq \mathbb{R}_{\geqslant 0}$ dicht

iii) $\mathcal{O}_K/p\mathcal{O}_K \to \mathcal{O}_K/p\mathcal{O}_K, \quad x \mapsto x^p$ ist surjektiv.

Beispiel 2.1

i) Sei μ_{p^n} die Gruppe aller p^n-ten Einheitswurzeln und μ_{p^∞} die Gruppe aller Einheitswurzeln, dessen Ordnung eine $p-$Potenz ist. Dann ist die Vervollständigung $K := \widehat{\mathbb{Q}_p[\mu_{p^\infty}]}$ ein perfektoider Körper.

Es ist $\mathbb{Q}_p[\mu_{p^\infty}] = \bigcup_{n \geqslant 1} \mathbb{Q}_p[\mu_{p^n}]$, wobei nach [4] Satz 7.13 gilt
$[\mathbb{Q}_p[\mu_{p^n}] : \mathbb{Q}_p] = (p-1)p^{n-1}$. Nach 1.4.10 ist für $x \in \mathbb{Q}_p[\mu_{p^n}]$ dann

$$|x|_{\mathbb{Q}_p[\mu_{p^n}]} = |N_{\mathbb{Q}_p[\mu_{p^n}]|\mathbb{Q}_p}(x)|^{\frac{1}{(p-1)p^{n-1}}}.$$

Also ist $|K^\times|_K \supseteq \bigcup_{n \geqslant 1} p^{-\frac{1}{(p-1)p^{n-1}}\mathbb{Z}} \supseteq p^{-\mathbb{Z}[\frac{1}{p}]}$, wobei $p^{\mathbb{Z}[\frac{1}{p}]} \subseteq \mathbb{R}_{\geqslant 0}$ dichte Teilmenge ist, denn $\log_p : \mathbb{R}_{\geqslant 0} \to \mathbb{R}$ ist ein Homöomorphismus und $\mathbb{Z}[\frac{1}{p}] \subseteq \mathbb{R}$ ist dicht. Der Beweis dazu ist analog zum Beweis der Dichtheit von $\mathbb{Q} \subseteq \mathbb{R}$. Damit ist nach [6] Lemma 1.3.6 (c) für $\log_p^{-1} : \mathbb{R} \to \mathbb{R}_{\geqslant 0}, \quad x \mapsto p^x$ die Menge $\log_p^{-1}(\mathbb{Z}[\frac{1}{p}]) = p^{\mathbb{Z}[\frac{1}{p}]}$ dicht in $\log_p^{-1}(\mathbb{R}) = \mathbb{R}_{\geqslant 0}$.
Nach 1.3.8 und [4] Satz 2.3 gilt

$$\mathcal{O}_K/p\mathcal{O}_K \cong \mathcal{O}_{\mathbb{Q}_p[\mu_{p^\infty}]}/p\mathcal{O}_{\mathbb{Q}_p[\mu_{p^\infty}]} = \mathbb{Z}_p[\mu_{p^\infty}]/p\mathbb{Z}_p[\mu_{p^\infty}],$$

welches eine $\mathbb{F}_p-$Algebra ist. Da der Frobenius auf $\mathbb{F}_p$ surjektiv ist, genügt es zu zeigen, dass die Erzeuger der $\mathbb{F}_p-$Algebra, also die Restklassen aller $\zeta \in \mu_{p^\infty}$ im Bild der Abbildung $\mathbb{Z}_p[\mu_{p^\infty}]/p\mathbb{Z}_p[\mu_{p^\infty}] \to \mathbb{Z}_p[\mu_{p^\infty}]/p\mathbb{Z}_p[\mu_{p^\infty}], \quad x \mapsto x^p$ liegen. Dies ist gewährleistet, da $\mu_{p^\infty} \to \mu_{p^\infty}, \quad \zeta \mapsto \zeta^p$ surjektiv ist.

ii) Die Vervollständigung des separablen Abschlusses $\mathbb{C}_p = \widehat{\mathbb{Q}_p^{sep}}$ ist ein perfektoider Körper.

Da $\mathbb{C}_p \supseteq \widehat{\mathbb{Q}_p[\mu_{p^\infty}]}$ ist $|\mathbb{C}_p|_{\mathbb{C}_p}$ dicht in $\mathbb{R}_{\geqslant 0}$. Nach 1.3.8 ist $\mathcal{O}_{\mathbb{C}_p}/p\mathcal{O}_{\mathbb{C}_p} \cong \mathcal{O}_{\mathbb{Q}_p^{sep}}/p\mathcal{O}_{\mathbb{Q}_p^{sep}}$. Wegen $char(\mathbb{Q}_p^{sep}) = 0$ gilt $\mathbb{Q}_p^{sep} = \overline{\mathbb{Q}_p}$, wobei $\overline{\mathbb{Q}_p}$ der algebraische Abschluss von $\mathbb{Q}_p$ ist.
Damit ist $\mathbb{Q}_p^{sep} \to \mathbb{Q}_p^{sep}, \quad x \mapsto x^p$ offensichtlich surjektiv, da für $y \in \mathbb{Q}_p^{sep}$ eine Nullstelle des

Polynoms $f(t) := t^p - y$ in $\mathbb{Q}_p^{sep}$ als Urbild gewählt werden kann. Aufgrund der Multiplikativität des Absolutbetrags gilt die Surjektivität der Abbildung $\mathcal{O}_{\mathbb{Q}_p^{sep}} \to \mathcal{O}_{\mathbb{Q}_p^{sep}},\quad x \mapsto x^p$, und diese induziert einen surjektiven Ringhomomorphismus $\mathcal{O}_{\mathbb{Q}_p^{sep}}/p\mathcal{O}_{\mathbb{Q}_p^{sep}} \to \mathcal{O}_{\mathbb{Q}_p^{sep}}/p\mathcal{O}_{\mathbb{Q}_p^{sep}},\quad x \mapsto x^p$.

Sei K ein perfektoider Körper. Dann definiert man

$$\mathcal{O}_{\mathbf{K}^\flat} := \varprojlim_{x \mapsto x^p} \mathcal{O}_K/p\mathcal{O}_K := \{(a_n)_{n \geqslant 0} \in \prod_{n \geqslant 0} \mathcal{O}_K/p\mathcal{O}_K : a_{n+1}^p = a_n\}.$$

Für die komponentenweise Operation ist dies ein Ring der Charakteristik p.

Proposition 2.2
Sei K ein perfektoider Körper.

i) Sei $a = (a_n)_{n \geqslant 0} \in \mathcal{O}_{K^\flat}$ mit $a_n = \alpha_n + p\mathcal{O}_K$. Dann existiert der Grenzwert der Folge $(\alpha_n^{p^n})_{n \geqslant 0}$ in $\mathcal{O}_K$ und ist unabhängig von der Wahl der α_n. Im Folgenden gilt die Notation $a^\# := \lim_{n \to \infty} \alpha_n^{p^n}$.

ii) Die Abbildung

$$\begin{aligned} \# : \quad \mathcal{O}_{K^\flat} &\to \mathcal{O}_K \\ a &\mapsto a^\# \end{aligned}$$

ist multiplikativ und erfüllt $a^\# + p\mathcal{O}_K = a_0$ für alle $a \in \mathcal{O}_{K^\flat}$.

iii) Die Abbildung

$$\begin{array}{ccc} \mathcal{O}_{K^\flat} & \to & \mathcal{O}_{K^\flat} \\ x & \mapsto & x^p \end{array}$$

ist bijektiv, d.h. $\mathcal{O}_{K^\flat}$ ist perfekt.

iv) Sei $\varprojlim_{x \mapsto x^p} \mathcal{O}_K := \{(\alpha_n)_{n \geqslant 0} \in \prod_{n \geqslant 0} \mathcal{O}_K : \alpha_{n+1}^p = \alpha_n\}$. Die Abbildung

$$\begin{array}{ccc} \varprojlim_{x \mapsto x^p} \mathcal{O}_K & \to & \mathcal{O}_{K^\flat} \\ (\alpha_n)_{n \geqslant 0} & \mapsto & (\alpha_n + p\mathcal{O}_K)_{n \geqslant 0} \end{array}$$

ist eine multiplikative Bijektion mit der inversen Abbildung $a = (a_n)_{n \geqslant 0} \mapsto ((a^{\frac{1}{p^n}})^\#)_{n \geqslant 0}$.

Beweis: i) Seien $(a_n)_{n \geqslant 0}, (b_n)_{n \geqslant 0} \in \mathcal{O}_{K^\flat}$ mit $a_n = b_n$ und $\alpha_n + p\mathcal{O}_K = a_n,\ \beta_n + p\mathcal{O}_K = b_n$. Dann ist $\alpha_{n+1}^p \equiv \alpha_n \mod p\mathcal{O}_K$ und $\beta_{n+1}^p \equiv \beta_n \mod p\mathcal{O}_K$. Mit 1.1.2 folgt $(\alpha_{n+1}^p)^{p^n} \equiv \alpha_n^{p^n} \mod p^{n+1}\mathcal{O}_K$. Für β_n gilt dies analog. Da $char(\mathcal{O}_K/\mathfrak{m}) = p$ ist $p \in \mathfrak{m}$ und somit $|p| < 1$. Damit sind $(\alpha_n^{p^n})_{n \geqslant 0}$ und $(\beta_n^{p^n})_{n \geqslant 0}$ Cauchyfolgen und somit konvergent. Da $\alpha_n - \beta_n \in p\mathcal{O}_K$ gilt mit 1.1.2, dass $\alpha_n^{p^n} \equiv \beta_n^{p^n} \mod p^{n+1}\mathcal{O}_K$ ist und es folgt die Gleichheit der Grenzwerte.
ii) Sei $ab = (a_n b_n)_{n \geqslant 0} \in \mathcal{O}_{K^\flat}$. Dann ist $(ab)^\# = \lim_{n \to \infty} \alpha_n^{p^n} \beta_n^{p^n} = a^\# b^\#$, da $(\alpha_n^{p^n})_{n \geqslant 0}$ und $(\beta_n^{p^n})_{n \geqslant 0}$ konvergieren.
Nach Definition ist $a_n^{p^n} = a_0$ für alle $n \in \mathbb{N}$, also $\alpha_n^{p^n} - \alpha_0 \in p\mathcal{O}_K$ für alle $n \in \mathbb{N}$. Damit ist $(\alpha_n^{p^n} - \alpha_0 + p\mathcal{O}_K)_{n \geqslant 0}$ konstante Nullfolge in $\mathcal{O}_{K^\flat}$ und somit ist $\lim_{n \to \infty} \alpha_n^{p^n} - \alpha_0 \in p\mathcal{O}_K$.
iii) Da $char(\mathcal{O}_{K^\flat}) = p$ ist $x \mapsto x^p$ ein Ringhomomorphismus. Sei $a = (a_n)_{n \geqslant 0} \in \mathcal{O}_{K^\flat}$ mit $0 = a^p = (a_0^p, a_1^p, \ldots) = (a_0^p, a_0, a_1, \ldots)$. Damit ist $a = 0$.
Sei $b = (a_1, a_2, \ldots) \in \mathcal{O}_{K^\flat}$. Dann ist $b^p = a$.

iv) Sei $a = (a_n)_{n\geqslant 0} \in \mathcal{O}_{K^\flat}$ und $a_n = \alpha_n + p\mathcal{O}_K$. Dann ist $a^{\frac{1}{p^n}} = (a_n, a_{n+1}, \ldots)$. Es ist zu überprüfen, ob $((a^{\frac{1}{p^n}})^\#)_{n\geqslant 0} \in \varprojlim_{x\mapsto x^p} \mathcal{O}_K$ ist. Es gilt

$$((a^{\frac{1}{p^{n+1}}})^\#)^p = (\lim_{m\to\infty} \alpha_{n+1+m}^{p^m})^p = \lim_{n\to\infty} \alpha_{n+1+m}^{p^{m+1}} = (a^{\frac{1}{p^n}})^\#$$

also $((a^{\frac{1}{p^n}})^\#)_{n\geqslant 0} \in \varprojlim_{x\mapsto x^p} \mathcal{O}_K$. Die Hintereinanderausführung

$$\begin{array}{ccccc} \mathcal{O}_{K^\flat} & \to & \varprojlim_{x\mapsto x^p} \mathcal{O}_K & \to & \mathcal{O}_{K^\flat} \\ (a_n)_{n\geqslant 0} & \mapsto & ((a^{\frac{1}{p^n}})^\#)_{n\geqslant 0} & \mapsto & ((a^{\frac{1}{p^n}})^\# + p\mathcal{O}_K)_{n\geqslant 0}, \end{array}$$

ist die Identität, da wegen ii) $((a^{\frac{1}{p^n}})^\# + p\mathcal{O}_K)_{n\geqslant 0} = (a_n)_{n\geqslant 0}$ ist. Damit ist die Abbildung surjektiv. Seien $\alpha, \beta \in \varprojlim_{x\mapsto x^p} \mathcal{O}_K$ mit $\alpha_m + p\mathcal{O}_K = \beta_m + p\mathcal{O}_K$ für alle $m \geqslant 0$. Mit 1.1.2 folgt $\alpha_m = \alpha_{m+n}^{p^n} \equiv \beta_{m+n}^{p^n} = \beta_m \mod p^{n+1}\mathcal{O}_K$ für alle $m, n \geqslant 0$. Damit ist $\alpha_m = \beta_m$ für alle $m \geqslant 0$, da $\bigcap_{n\geqslant 0} p^n\mathcal{O}_K = 0$. □

Proposition 2.3

Sei K ein perfektoider Körper.

i) Die Abbildung

$$\begin{array}{rll} |\cdot|_\flat : & \mathcal{O}_{K_\flat} & \to \mathbb{R}_{\geqslant 0} \\ & a & \mapsto |a^\#| \end{array}$$

ist ein nicht-archimedischer Absolutbetrag.

ii) Es gilt $|\mathcal{O}_K| = |\mathcal{O}_{K^\flat}|_\flat$.

iii) Für $a, b \in \mathcal{O}_{K^\flat}$ ist genau dann $|a|_\flat \leqslant |b|_\flat$, wenn $a\mathcal{O}_{K^\flat} \subseteq b\mathcal{O}_{K^\flat}$.

iv) Erfüllt $p^\flat \in \mathcal{O}_{K^\flat}$ die Gleichung $|p^\flat|_\flat = |p|$, dann ist die Abbildung

$$\begin{array}{rl} \mathcal{O}_{K^\flat}/p^\flat\mathcal{O}_{K^\flat} & \to \mathcal{O}_K/p\mathcal{O}_K \\ (a_n)_{n\geqslant 0} + p^\flat\mathcal{O}_{K^\flat} & \mapsto a_0 \end{array}$$

ein Ringisomorphismus.

Beweis: i) Man wähle für jedes Folgenglied des Nullelements $0 \in \mathcal{O}_{K^\flat}$ den Repräsentanten $0 \in K$. Dann sieht man leicht, dass $|0|_\flat = |0^\#| = |0| = 0$ ist. Sei nun andererseits $a \in \mathcal{O}_{K^\flat}$ mit $|a|_\flat = |a^\#| = 0$. Da $|\cdot|$ ein Absolutbetrag ist, ist $a^\# = 0$. Für alle $n \geqslant 0$ gilt nach 2.2 ii), dass $((a^{\frac{1}{p^n}})^\#)^{p^n} = a^\# = 0$. Der Ring $\mathcal{O}_K$ ist ein Integritätsbereich. Also folgt für alle $n \geqslant 0$, dass $(a^{\frac{1}{p^n}})^\# = 0$ iist. Aufgrund der Bijektivität der Abbildung in 2.2 iv), ist $a = 0$.
Die zweite Eigenschaft eines Absolutbetrags ist wegen der Multiplikativität der Abbildungen # und $|\cdot|$ erfüllt.
Seien $a = (a_n)_{n\geqslant 0} = (\alpha_n + p\mathcal{O}_K)_{n\geqslant 0}$, $b = (b_n)_{n\geqslant 0} = (\beta_n + p\mathcal{O}_K)_{n\geqslant 0} \in \mathcal{O}_{K^\flat}$. Dann ist $|a+b|_\flat = |(a+b)^\#| = |\lim_{n\to\infty}(\alpha_n + \beta_n)^{p^n}| = \lim_{n\to\infty} |\alpha_n + \beta_n|^{p^n} \leqslant \lim_{n\to\infty} \max\{|\alpha_n|^{p^n}, |\beta_n|^{p^n}\} = \max\{|a|_\flat, |b|_\flat\}$.
ii) Die Inklusion $|\mathcal{O}_{K^\flat}|_\flat \subseteq |\mathcal{O}_K|$ gilt offensichtlich.
Sei $\alpha \in \mathcal{O}_K\backslash\{0\}$. Da K perfektoid ist, liegt $|K^\times|$ dicht in $\mathbb{R}_{>0}$. Daher gibt es $\lambda \in \mathcal{O}_K$, sodass $|p| <$

$|\lambda| < 1$. Sei $m \in \mathbb{N}$ mit $|\lambda^{m+1}| < |\alpha| \leqslant |\lambda^m|$. Da $|\lambda| < 1$ ist, ist offensichtlich $|\lambda| < |\lambda^{-m}|$ und wegen $|\alpha| \leqslant |\lambda^{-m}|$ ist $|\lambda^{-m}\alpha| \leqslant 1$. Nach Voraussetzung ist die Abbildung $\mathcal{O}_K/p\mathcal{O}_K \to \mathcal{O}_K/p\mathcal{O}_K, \quad x \mapsto x^p$ surjektiv und damit gibt es $\gamma, \delta \in \mathcal{O}_K$, sodass $\lambda^{-m}\alpha - \delta^p, \lambda - \gamma^p \in p\mathcal{O}_K$ ist. Somit ist $|\lambda - \gamma^p| \leqslant |p|$. Darüberhinaus ist $|\gamma^p| > |p|$, denn angenommen es gelte $|\gamma^p| \leqslant |p|$. Dann ist $|\lambda| = |\lambda - \gamma^p + \gamma^p| \leqslant \max\{|\lambda - \gamma^p|, |\gamma^p|\} \leqslant |p|$. Dies widerspricht aber der Ungleichung $|p| < |\lambda|$. Mit 1.2.5 folgt somit insgesamt $|\lambda| = |\lambda - \gamma^p + \gamma^p| = |\gamma^p| = |\gamma|^p$.
Auf dieselbe Art erhält man $|\lambda^{-m}\alpha| = |\delta|^p$.
Mit diesen beiden Gleichungen folgt $|\alpha| = |\gamma^m\delta|^p$. Dies lässt sich induktiv fortsetzen, sodass nach $n-$maliger Ausführung β konstruiert wird, mit $|\alpha| = |\beta|^{p^n}$. Wähle $n \in \mathbb{N}$ groß genug, sodass $|p| < |\beta|$ ist. Dies ist möglich, da $|\beta| = \sqrt[p^n]{|\alpha|}$ und $\lim_{n\to\infty} \sqrt[p^n]{|\alpha|} = 1$ ist. Es genügt nun zu zeigen, dass $|\beta| \in |\mathcal{O}_{K^\flat}|_\flat$ ist. Im Folgenden wird $b \in \mathcal{O}_{K^\flat}$ konstruiert mit $|b|_\flat = |\beta|$. Setze $\beta_0 := \beta$ und $b_0 := \beta_0 + p\mathcal{O}_K$. Wegen der Surjektivität von $\mathcal{O}_K/p\mathcal{O}_K \to \mathcal{O}_K/p\mathcal{O}_K, \quad x \mapsto x^p$ erhält man eine Folge $b = (b_n)_{n\geqslant 0} = (\beta_n + p\mathcal{O}_K)_{n\geqslant 0}$ mit $b_{n+1}^p = b_n$. Also ist $b \in \mathcal{O}_{K^\flat}$. Da für alle $n \in \mathbb{N}$ gilt $\beta_n^{p^n} \equiv \beta = \beta_0 \mod p\mathcal{O}_K$, ist $|b^\# - \beta| = |\lim_{n\to\infty} \beta_n^{p^n} - \beta| = \lim_{n\to\infty} |\beta_n^{p^n} - \beta| \leqslant |p|$. Insgesamt ist also $|b|_\flat = |b^\#| = |b^\# - \beta + \beta| = \max\{|b^\# - \beta|, |\beta|\} = |\beta| \in |\mathcal{O}_{K^\flat}|$.
iii) Seien $a, b \in \mathcal{O}_{K^\flat}$ mit $a\mathcal{O}_{K^\flat} \subseteq b\mathcal{O}_{K^\flat}$. Für den Fall, dass $a = 0$ ist, gilt die Behauptung offensichtlich. Dieser wird im Folgenden ausgeschlossen.
Es existiert $c \in \mathcal{O}_{K^\flat}$ mit $a = bc$. Mit i) folgt, dass $|a|_\flat = |bc|_\flat \leqslant |b|_\flat|c|_\flat \leqslant |b|_\flat$, da wegen ii) $|c|_\flat \leqslant 1$ ist.
Seien nun $a, b \in \mathcal{O}_{K^\flat}$ mit $|a|_\flat \leqslant |b|_\flat$ und $\alpha_n := (a^{\frac{1}{p^n}})^\#, \beta_n := (b^{\frac{1}{p^n}})^\#$ für alle $n \in \mathbb{N}$. Mit 2.2 ii) folgt, dass $|\alpha_0| = |a|_\flat \leqslant |b|_\flat = |\beta_0|$. Die Folgen $(\alpha_n)_{n\geqslant 0}$ und $(\beta_n)_{n\geqslant 0}$ liegen nach 2.2 iv) in $\varprojlim_{x\mapsto x^p} \mathcal{O}_K$. Da die Funktion $f(x) := x^{\frac{1}{p^n}}$ auf $\mathbb{R}_{\geqslant 0}$ monoton wachsend ist, folgt für alle $n \in \mathbb{N}$, dass $|\alpha_n| = |\alpha_0|^{\frac{1}{p^n}} \leqslant |\beta_0|^{\frac{1}{p^n}} = |\beta_n|$ ist. Mit 1.2.12 folgt, dass für alle $n \in \mathbb{N}$ ein $\gamma_n \in \mathcal{O}_K$ existiert, sodass $\alpha_n = \gamma_n\beta_n$ ist. Darüberhinaus ist $\gamma_n\beta_n = \alpha_n = \alpha_{n+1}^p = \gamma_{n+1}^p\beta_{n+1}^p = \gamma_{n+1}^p\beta_n$. Folglich gilt für alle $n \in \mathbb{N}$ die Gleichung $\gamma_n = \gamma_{n+1}^p$, da $\mathcal{O}_K$ ein Integritätsbereich ist. Für $\gamma := (\gamma_n)_{n\geqslant 0}$ und $c := (\gamma_n + p\mathcal{O}_K)_{n\geqslant 0}$ folgt aus $\alpha = \beta\gamma$ aufgrund der Multiplikativität der Abbildung aus 2.2 iv), dass $a = bc$ und somit $a\mathcal{O}_{K^\flat} \subseteq b\mathcal{O}_{K^\flat}$ ist.
iv) Sei $p^\flat \in \mathcal{O}_{K^\flat}$ mit $|p^\flat|_\flat = |p|$. Da $\mathcal{O}_K/p\mathcal{O}_K \to \mathcal{O}_K/p\mathcal{O}_K, \quad x \mapsto x^p$ surjektiv ist, ist es möglich, jedes $a_0 \in \mathcal{O}_K/p\mathcal{O}_K$ fortzusetzen, sodass $(a_n)_{n\geqslant 0}$ in $\mathcal{O}_{K^\flat}$ liegt. Daher ist $\mathcal{O}_{K^\flat} \to \mathcal{O}_K/p\mathcal{O}_K, \quad (a_n)_{n\geqslant 0} \mapsto a_0$ ein surjektiver Ringhomomorphismus. Der Kern dieser Abbildung ist

$$\begin{aligned} \{a \in \mathcal{O}_{K^\flat} : a_0 = 0\} &\overset{2.2}{\underset{\text{ii)}}{=}} \{a \in \mathcal{O}_{K^\flat} : a^\# \in p\mathcal{O}_K\} \\ &= \{a \in \mathcal{O}_{K^\flat} : |a|_\flat = |a^\#| \leqslant |p| = |p^\flat|_\flat\} \\ &\overset{\text{iii)}}{=} p^\flat\mathcal{O}_{K^\flat}. \end{aligned}$$

Also gilt die Isomorphie. □

Korollar 2.4
$\mathcal{O}_{K^\flat}$ ist ein Integritätsbereich und $|\cdot|_\flat : \mathcal{O}_{K^\flat} \to \mathbb{R}_{\geqslant 0}$ ist zu einem nicht-archimedischen Absolutbetrag auf $K^\flat := Quot(\mathcal{O}_{K^\flat})$ fortsetzbar. Darüberhinaus ist $|K^\flat|_\flat = |K|$ und $\mathcal{O}_{K^\flat} = \{x \in K^\flat : |x|_\flat \leqslant 1\}$.

Beweis: Seien $a, b \in \mathcal{O}_{K^\flat}$ mit $ab = 0$. Dann ist $|ab|_\flat = |a|_\flat|b|_\flat = 0$ in $\mathbb{R}_{\geqslant 0}$. Somit ist entweder $|a|_\flat = 0$ oder $|b|_\flat = 0$ und folglich $a = 0$ oder $b = 0$. Offensichtlich definiert $|\frac{x}{y}|_\flat := \frac{|x|_\flat}{|y|_\flat}$ einen nicht-archimedischen Absolutbetrag auf $K^\flat$.

Es gilt

$$\begin{array}{rcl} |K^\flat|_\flat & = & \{|x|_\flat |y|_\flat^{-1} : x \in \mathcal{O}_{K^\flat}, y \in \mathcal{O}_{K^\flat}\backslash\{0\}\} \\ & = & \{r_1 r_2 : r_1 \in |\mathcal{O}_{K^\flat}|_\flat, r_2 \in |\mathcal{O}_{K^\flat}\backslash\{0\}|_\flat^{-1}\} \\ & \underset{\text{ii)}}{\overset{2.3}{=}} & \{r_1 r_2 : r_1 \in |\mathcal{O}_K|, r_2 \in |\mathcal{O}_K\backslash\{0\}|^{-1}\} = |K|, \end{array}$$

wobei für eine Teilmenge A von $\mathbb{R}_{>0}$ bedeutet $A^{-1} := \{x \in \mathbb{R}_{>0} : x^{-1} \in A\}$.
Offensichtlich gilt die Inklusion $\mathcal{O}_{K^\flat} \subseteq \{x \in K^\flat : |x|_\flat \leqslant 1\}$. Sei $x \in K^\flat$ mit $|x|_\flat \leqslant 1$. Es gibt $y, z \in \mathcal{O}_{K^\flat}$, sodass $x = yz^{-1}$ ist. Folglich ist wegen 2.3 iii) $y \in z\mathcal{O}_{K^\flat}$. Daher ist $x \in \mathcal{O}_{K^\flat}$. □

Proposition 2.5
$K^\flat$ ist ein perfekter Körper mit $char(K^\flat) = p$. Bezüglich $|\cdot|_\flat$ ist er vollständig. Wegen 2.4 ist $(K^\flat, |\cdot|_\flat)$ daher ein perfektoider Körper.

Beweis: Da $\mathcal{O}_{K^\flat}$ perfekt ist und $char(\mathcal{O}_{K^\flat}) = p$, gilt dies ebenfalls für seinen Quotientenkörper. Nach 1.3.9 genügt nun noch zu zeigen, dass $\mathcal{O}_{K^\flat}$ vollständig ist. Dazu werden zwei Fälle unterschieden. Zunächst wird die Behauptung für den Fall $char(K) = p \neq 0$ und im Anschluss für den Fall $char(K) = 0$.
Sei $char(K) = p \neq 0$. Dann ist die Charakteristik des Restklassenkörpers ebenfalls p und es gilt $\mathcal{O}_K/p\mathcal{O}_K \cong \mathcal{O}_K$. Nach Voraussetzung ist die Abbildung $\mathcal{O}_K/p\mathcal{O}_K \cong \mathcal{O}_K \to \mathcal{O}_K \cong \mathcal{O}_K/p\mathcal{O}_K,\ \ x \mapsto x^p$ surjektiv. Damit ist $\mathcal{O}_K$ perfekt und somit ist auch K perfekt. Damit ist der Ringhomomorphismus $\mathcal{O}_{K^\flat} \to \mathcal{O}_K/p\mathcal{O}_K \cong \mathcal{O}_K,\ \ (a_n)_{n\geqslant 0} \to a_0$ surjektiv. Darüberhinaus ist er injektiv und eine Isometrie. Für $(a_n)_{n\geqslant 0} \in \mathcal{O}_{K^\flat}$ mit $(a_n)_{n\geqslant 0} \mapsto 0$ gilt für alle $n \in \mathbb{N}$, dass $0 = a_0 = a_n^{p^n}$ und somit $a_n = 0$ für alle $n \in \mathbb{N}$ ist.
Wegen 2.2 ii) gilt $|(a_n)_{n\geqslant 0}|_\flat = |(a_n)_{n\geqslant 0}^\#| = |a_0|$.
Setzt man die Abbildung $\mathcal{O}_{K^\flat} \to \mathcal{O}_K/p\mathcal{O}_K \cong \mathcal{O}_K,\ \ (a_n)_{n\geqslant 0} \to a_0$ auf K fort, so erhält man einen isometrischen Isomorphismus $(K^\flat, |\cdot|_\flat) \to (K, |\cdot|)$. Da K perfektoid ist, ist $K^\flat$ bzgl. $|\cdot|_\flat$ vollständig.

Sei nun $char(K) = 0$ und sei $a^{(m)} := (a_n^{(m)})_{n\geqslant 0} \in \mathcal{O}_{K^\flat}$ für alle $m \in \mathbb{N}$, wobei $(a^{(m)})_{m\geqslant 0}$ eine Cauchyfolge ist. Sei $n \in \mathbb{N}$ beliebig. Dann gibt es ein $N \in \mathbb{N}$, sodass für alle $m, m' \geqslant N$ gilt $|a^{(m)} - a^{(m')}|_\flat < |p|^{p^n}$ ist.
Für $b = (b_n)_{n\geqslant 0} \in \{x \in \mathcal{O}_{K^\flat} : |x|_\flat \leqslant |p|^{p^n}\}$ gilt $|p| \geqslant |b^{\frac{1}{p^n}}|_\flat = |(b^{\frac{1}{p^n}})^\#|$. Es gilt also $(b^{\frac{1}{p^n}})^\# \in p\mathcal{O}_K$ und wegen 2.2 iv) ist $b_n = (b^{\frac{1}{p^n}})^\# + p\mathcal{O}_K = (b_n, b_{n+1}, \ldots)^\# + p\mathcal{O}_{K^\flat} = 0$. Damit ist auch $b_k = b_n^{p^{n-k}} = 0$ für alle $k \in \mathbb{N}$ mit $0 \leqslant k \leqslant n$.
Für die $k-$ten Folgenglieder von $a^{(m)} - a^{(m')}$ mit $0 \leqslant k \leqslant n$ gilt demnach für alle $m, m' \geqslant N$, dass $(a^{(m)} - a^{(m')})_k = a_k^{(m)} - a_k^{(m')} = 0$ ist, also gilt $a_k^{(m)} = a_k^{(m')}$. Da n beliebig ist, wird $(a_k^{(m)})_{m\geqslant 0}$ stationär für alle $k \in \mathbb{N}$. Sei $a_k := \lim_{m\to\infty} a_k^{(m)} \in \mathcal{O}_K/p\mathcal{O}_K$. Man wähle m groß genug, sodass $a_k = a_k^{(m)}$ und $a_{k+1} = a_{k+1}^{(m)}$ ist. Dann ist $a_{k+1}^p = (a_{k+1}^{(m)})^p = a_k^{(m)} = a_k$, weil $a^{(m)} \in \mathcal{O}_{K^\flat}$. Damit ist $a := (a_k)_{k\geqslant 0} \in \mathcal{O}_{K^\flat}$ der Grenzwert der Folge $(a^{(m)})_{m\geqslant 0}$. Denn sei dazu $\epsilon > 0$ und $n \in \mathbb{N}$ mit $|p|^{p^n} < \epsilon$. Dann gibt es ein $N > 0$, sodass für alle $m \geqslant N$ gilt $a_n^{(m)} = a_n$. Mit 2.2 ii) folgt $0 = a_n^{(m)} - a_n = ((a^{(m)} - a)^{\frac{1}{p^n}})^\# + p\mathcal{O}_K$ und somit $((a^{(m)} - a)^{\frac{1}{p^n}})^\# \in p\mathcal{O}_K$, also $|((a^{(m)} - a)^{\frac{1}{p^n}})^\#| = |(a^{(m)} - a)^{\frac{1}{p^n}}|_\flat \leqslant |p|$. Dies impliziert $|a^{(m)} - a|_\flat \leqslant |p|^{p^n} < \epsilon$. □

Definition 2.6
Ist $(K, |\cdot|)$ ein perfektoider Körper, so heißt $(K^\flat, |\cdot|_\flat)$ der **Tilt von** K.

Ist $char(K) = p \neq 0$, so sind $(K, |\cdot|)$ und $(K^\flat, |\cdot|_\flat)$ isometrisch isomorph. Im Beweis von 2.5 ist dieser Isomorphismus angegeben.

Lemma 2.7
Seien K und L perfektoide Körper der Charakteristik 0 und sei $\sigma : K \to L$ ein stetiger Körperhomomorphismus. Dann ist

$$\begin{array}{rccc} \sigma^\flat & : & \mathcal{O}_{K^\flat} & \to & \mathcal{O}_{L^\flat} \\ & & (\alpha_n + p\mathcal{O})_{n\geqslant 0} & & (\sigma(\alpha_n) + p\mathcal{O})_{n\geqslant 0} \end{array}$$

ein stetiger und injektiver Ringhomomorphismus. Ist σ eine Isometrie, so ist auch $\sigma^\flat$ eine Isometrie.

Beweis: Damit $\sigma^\flat$ wohldefiniert ist, muss zunächst gewährleistet sein, dass $\sigma(\mathcal{O}_K)$ in $\mathcal{O}_L$ liegt. Sei $x \in \mathcal{O}_K$ mit $|x| < 1$. Dann gilt wegen der Stetigkeit von σ

$$\lim_{n\to\infty} \sigma(x^n) = \sigma(\lim_{n\to\infty} x^n) = \sigma(0) = 0.$$

Damit ist $(\sigma(x)^n)_{n\geqslant 0}$ eine Nullfolge und somit ist $|\sigma(x)| < 1$.
Sei $x \in \mathcal{O}_K^\times$, also $|x| = 1$. Angenommen es gilt $|\sigma(x)| \neq 1$. Dann ist $(\sigma(x^n))_{n\geqslant 0}$ oder $(\sigma(x^{-1})^n)_{n\geqslant 0}$ eine Nullfolge. Die Folgen $(x^n)_{n\geqslant 0}$ und $(x^{-n})_{n\geqslant 0}$ sind keine Nullfolgen. Dies widerspricht der Stetigkeit von σ.
Damit ist die Einschränkung $\sigma : \mathcal{O}_K \to \mathcal{O}_L$ ein Ringhomomorphismus und somit ist $\sigma^\flat$ wohldefiniert und offenbar ein Ringhomomorphismus. Das Diagramm

$$\begin{tikzcd} (\alpha_n)_{n\geqslant 0} \arrow[d, mapsto] & \varprojlim_{x\mapsto x^p} \mathcal{O}_K \arrow[r, "2.2iv)"] \arrow[d] & \mathcal{O}_{K^\flat} \arrow[d] \\ (\sigma(\alpha_n))_{n\geqslant 0} & \varprojlim_{x\mapsto x^p} \mathcal{O}_L \arrow[r, "2.2iv)"] & \mathcal{O}_{L^\flat} \end{tikzcd}$$

kommutiert, wobei die Abbildungen $\varprojlim_{x\mapsto x^p} \mathcal{O}_K \to \varprojlim_{x\mapsto x^p} \mathcal{O}_L$ und $\varprojlim_{x\mapsto x^p} \mathcal{O}_K \to \mathcal{O}_{K^\flat}$ injektiv bzw. bijektiv sind. Damit ist auch $\sigma^\flat$ ein injektiver Ringhomomorphismus.
Sei nun $\sigma : K \to L$ eine Isometrie und sei $(\alpha_n + p\mathcal{O}_K)_{n\geqslant 0} \in \mathcal{O}_{K^\flat}$. Dann ist

$$\begin{aligned} |\sigma^\flat((\alpha_n + p\mathcal{O}_K)_{n\geqslant 0})|_\flat &= |(\sigma(\alpha_n) + p\mathcal{O}_K)_{n\geqslant 0}|_\flat = |(\sigma(\alpha_n) + p\mathcal{O}_K)_{n\geqslant 0})^\#| = |\lim_{n\to\infty} \sigma(\alpha_n)^{p^n}| \\ &= |\sigma(\lim_{n\to\infty} \alpha_n^{p^n})| = |\lim_{n\to\infty} \alpha_n^{p^n}| = |(\alpha_n + p\mathcal{O}_K)_{n\geqslant 0}|_\flat. \end{aligned}$$

Der Ringhomomorphismus $\sigma^\flat$ ist also ebenfalls eine Isometrie. □

Da $\sigma^\flat : \mathcal{O}_{K^\flat} \to \mathcal{O}_{L^\flat}$ ein injektiver Ringhomomorphismus ist, lässt sich dieser zu einem Körperhomomorphismus $\sigma^\flat : K^\flat \to L^\flat$ fortsetzen. Dieser heißt der **Tilt von σ**.

Lemma 2.8
Die Zuordnung

$$\begin{array}{ccc} K & \mapsto & K^\flat \\ \\ \sigma & \mapsto & \sigma^\flat \end{array}$$

für perfektoide Körper K ist funktoriell.

Beweis: Offensichtlich gilt die Gleichheit $(id_K)^\flat = id_{K^\flat}$. Seien f und g isometrische Körperhomomorphismen, sodass die Verknüpfung $f \circ g$ sinnvoll ist. Dann ist offensichtlich $(f \circ g)^\flat = f^\flat \circ g^\flat$. $\square$

Lemma 2.9
Ist K ein perfektoider Körper, so ist $\widehat{K^\flat}$ ein perfektoider Körper.

Beweis: Der Körper $\widehat{K^\flat}$ ist vollständig. Da $K^\flat$ perfektoid ist, ist $|(K^\flat)^\times|_\flat$ dicht in $\mathbb{R}_{\geqslant 0}$ und somit liegt nach Definition von $|\cdot|^\wedge$ die Menge $|(\widehat{K^\flat})^\times|^\wedge$ dicht in $\mathbb{R}_{\geqslant 0}$. Es ist also noch zu zeigen, dass die Abbildung

$$\begin{array}{ccc} \mathcal{O}_{\widehat{K^\flat}}/p\mathcal{O}_{\widehat{K^\flat}} \cong \mathcal{O}_{\widehat{K^\flat}} & \to & \mathcal{O}_{\widehat{K^\flat}} \cong \mathcal{O}_{\widehat{K^\flat}}/p\mathcal{O}_{\widehat{K^\flat}} \\ x & \mapsto & x^p \end{array}$$

surjektiv ist. Das zeigt man wie in 2.1 ii). $\square$

Theorem 2.10
Sei K ein perfektoider Körper. K ist genau dann algebraisch abgeschlossen, wenn $K^\flat$ algebraisch abgeschlossen ist.

Beweis: Sei K algebraisch abgeschlossen und $E|K^\flat$ eine endliche Körpererweiterung. Da $K^\flat$ nach 2.5 perfekt ist, ist die Körpererweiterung separabel. Es kann o.B.d.A angenommen werden, dass $E|K^\flat$ eine endliche Galoiserweiterung ist, da sich endliche Körpererweiterungen zu einer normalen Körpererweiterung erweitern lassen. Sei $x \in E$. Es wird nun gezeigt, dass x in $K^\flat$ liegt, denn dann besitzt $K^\flat$ keine echte algebraische Erweiterung und ist somit algebraisch abgeschlossen. Falls x nicht in $\mathcal{O}_E$ liegt, wird es mit y^{-1} multipliziert, wobei $y \in K^\flat \backslash \{0\}$ und $|x|_\flat \leqslant |y|_\flat$ ist. Sei also o.B.d.A, $x \in \mathcal{O}_E$ und $m(X) = X^d + a^{(d-1)}X^{d-1} + \ldots + a^{(0)}$ das Minimalpolynom von x in $K^\flat$. Das Polynom m zerfällt in E in Linearfaktoren und seine Nullstellen sind Galoiskonjugierte von x. Nach 1.4.12 sind Elemente der Galoisgruppe Isometrien und somit liegen die Galoiskonjugierten ebenfalls im Bewertungsring $\mathcal{O}_E$ und folglich auch die Koeffizienten $a^{(0)}, \ldots, a^{(d-1)}$. Da sie Elemente in $K^\flat$ sind, liegen sie in $\mathcal{O}_{K^\flat}$. Sei $a^{(j)} = (a_n^{(j)})_{n\geqslant 0} \in \mathcal{O}_{K^\flat} = \varprojlim_{y \mapsto y^p} \mathcal{O}_K/p\mathcal{O}_K$ und $m_n := X^d + a_n^{(d-1)}X^{d-1} + \ldots + a_n^{(0)} \in \mathcal{O}_K/p\mathcal{O}_K[X]$. Sei ferner $B_n := \{z \in \mathcal{O}_K/p\mathcal{O}_K : m_n(z) = 0\}$. Da nach Definition $(a_{n+1}^{(j)})^p = (a_n^{(j)})$ für alle $j \in \{0, \ldots, d-1\}$ gilt, ist $B_{n+1}^p := \{b_{n+1}^p : b_{n+1} \in B_{n+1}\} \subseteq B_n$ für alle $n \in \mathbb{N}$. Dadurch ist

$$B := \varprojlim_{y \mapsto y^p} B_n = \{(b_n)_{n\geqslant 0} : b_n \in B_n \text{ und } b_{n+1}^p = b_n \text{ für alle } n \in \mathbb{N}\} \subseteq \mathcal{O}_{K^\flat},$$

wobei $((B_n)_{n\in\mathbb{N}}, (f_{ij})_{i\leqslant j\in\mathbb{N}})$ mit $f_{mn} : B_m \to B_n, \quad b_m \mapsto b_m^{p^{m-n}} = b_n$ offensichtlich ein projektives System ist. B ist die Menge der Nullstellen von m. Wenn nun gezeigt werden kann, dass B nicht leer ist, so muss aufgrund der Irreduzibilität des Minimalpolynoms m dieses vom Grad 1 sein und folglich

ist $x \in \mathcal{O}_{K^\flat}$. Damit wäre $K^\flat$ algebraisch abgeschlossen, da keine echte algebraische Erweiterung existiert.
Sei für $n \in \mathbb{N}$ das Polynom $\widetilde{m}_n(X) = X^d + (\alpha_n^{(d-1)})X^{d-1} + \ldots + (\alpha_n^{(0)}) \in \mathcal{O}_K[X]$ mit $\alpha_n^{(j)} + p\mathcal{O}_K = a_n^{(j)}$ und definiere $C_n := \{z \in K : \widetilde{m}_n(z) = 0\}$. Diese Menge ist endlich. Da K algebraisch abgeschlossen ist, zerfällt $\widetilde{m}_n$ in Linearfaktoren. Im Folgenden wird gezeigt, dass diese in $\mathcal{O}_K[X]$ liegen, also

$$C_n \subseteq \mathcal{O}_K. \tag{8}$$

Sei im Folgenden $||\cdot||$ die Gauß-Norm aus Kapitel 1. Da $\widetilde{m}_n$ ein normiertes Polynom in $\mathcal{O}_K[X]$ ist, ist $||\widetilde{m}_n|| = 1$ und da $||X - \beta|| \geqslant 1$ für alle $\beta \in K$ ist, gilt

$$1 = ||\widetilde{m}_n|| = |\prod_j (X - \beta_j)|| \overset{1.4.2}{=} \prod_j ||(X - \beta_j)||$$

und somit $||X - \beta_j|| \leqslant 1$ für alle β_j. Damit gilt (8).
Sei $A_n := \{\alpha^{p^{d-1}} + p\mathcal{O}_K : \alpha \in C_{n+d-1}\} \subseteq \mathcal{O}_K/p\mathcal{O}_K$. Dann ist $A_n \subseteq B_n$ für alle $n \in \mathbb{N}$. Denn sei α Nullstelle des Polynoms $\widetilde{m}_{n+d-1}$. Es gilt

$$\begin{aligned}
m_n(\alpha^{p^{d-1}} + p\mathcal{O}_K) &= (\alpha^{p^{d-1}})^d + (\alpha_n^{(d-1)})(\alpha^{p^{d-1}})^{d-1} + \ldots + (\alpha_n^{(0)}) + p\mathcal{O}_K \\
&= (\alpha^{p^{d-1}})^d + (\alpha_{n+d-1}^{(d-1)})^{p^{d-1}}(\alpha^{p^{d-1}})^{d-1} + \ldots + (\alpha_{n+d-1}^{(0)})^{p^{d-1}} + p\mathcal{O}_K \\
&= (\alpha^d)^{p^{d-1}} + (\alpha_{n+d-1}^{(d-1)}\alpha^{d-1})^{p^{d-1}} + \ldots + (\alpha_{n+d-1}^{(0)})^{p^{d-1}} + p\mathcal{O}_K \\
&= (\alpha^d + \alpha_{n+d-1}^{(d-1)}\alpha^{d-1} + \ldots + \alpha_{n+d-1}^{(0)})^{p^{d-1}} + p\mathcal{O}_K \\
&= (\widetilde{m}_{n+d-1}(\alpha))^{p^{d-1}} + p\mathcal{O}_K = 0.
\end{aligned}$$

Damit ist A_n eine endliche nicht-leere Teilmenge von B_n. Darüberhinaus ist

$$A_{n+1}^p \subseteq A_n. \tag{9}$$

Sei dazu $\alpha^{p^{d-1}} + p\mathcal{O}_K \in A_{n+1}$ mit $\alpha \in C_{n+d}$. Dann ist

$$\begin{aligned}
\widetilde{m}_{n+d-1}(\alpha^p) + p\mathcal{O}_K &= m_{n+d-1}(\alpha^p + \mathcal{O}_K) \\
&= (\alpha^p)^d + \alpha_{n+d-1}^{(d-1)}(\alpha^p)^{d-1} + \ldots + \alpha_{n+d-1}^{(0)} + p\mathcal{O}_K \\
&= (\alpha^d)^p + (\alpha_{n+d}^{(d-1)})^p(\alpha^{d-1})^p + \ldots + (\alpha_{n+d}^{(0)})^p + p\mathcal{O}_K \\
&= (\alpha^d + \alpha_{n+d}^{(d-1)}\alpha^{d-1} + \ldots + \alpha_{n+d}^{(0)})^p + p\mathcal{O}_K \\
&= (\widetilde{m}_{n+d}(\alpha))^p + p\mathcal{O}_K = 0.
\end{aligned}$$

Das Element $\widetilde{m}_{n+d-1}(\alpha^p)$ liegt also in $p\mathcal{O}_K$. Sei $\widetilde{m}_{n+d-1}(X) = \prod_{\beta \in C_{n+d-1}}(X - \beta)^{t_\beta}$ mit geeigneten positiven ganzen Zahlen t_β. Dann ist $\sum_{\beta \in C_{n+d-1}} t_\beta = d$ und $\prod_{\beta \in C_{n+d-1}}(\alpha^p - \beta)^{t_\beta} \in p\mathcal{O}_K$. Sei $\tilde{\beta} \in C_{n+d-1}$ mit $|\alpha^p - \tilde{\beta}| \leqslant |\alpha^p - \beta|$ für alle $\beta \in C_{n+d-1}$. Dann ist

$$|\alpha^p - \tilde{\beta}|^d \leqslant \prod_{\beta \in C_{n+d-1}} |\alpha^p - \beta|^{t_\beta} \leqslant |p|,$$

und somit gilt $|\alpha^p - \tilde{\beta}| \leqslant |p|^{\frac{1}{d}}$, also ist $\alpha^p - \tilde{\beta} \in \zeta\mathcal{O}_K$, wobei ζ eine Nullstelle von $X^d - p$ ist. Das Polynom $X^d - p$ zerfällt in $K[X]$, da K algebraisch abgeschlossen ist. Darüberhinaus liegt ζ in $\mathcal{O}_K$, da p in $\mathcal{O}_K$ liegt. Mit dem Ring $\mathcal{O}_K$ und dem Ideal $\zeta\mathcal{O}_K$ folgt mit 1.1.2 $\alpha^{p^d} - \tilde{\beta}^{p^{d-1}} \in p\mathcal{O}_K$ und somit ist

$$(\alpha^{p^{d-1}} + p\mathcal{O}_K)^p = \alpha^{p^d} + p\mathcal{O}_K = \tilde{\beta}^{p^{d-1}} + p\mathcal{O}_K \in A_n,$$

da $\tilde{\beta} \in C_{n+d-1}$. Damit gilt (9).
Sei $A'_n := \bigcap_{m\geqslant 0} A_{n+m}^{p^m}$. Da $A_n \supseteq A_{n+1}^p \supseteq A_{n+2}^{p^2}$.. eine Kette endlicher nicht-leerer Mengen ist, so ist auch A'_n eine endliche nicht-leere Menge. Es gibt eine natürliche Zahl $j(n)$ mit $A_n = A_{n+m}^{p^m}$ für alle $m \geqslant j(n)$. Da für alle $m \geqslant 0$ die Inklusion $A_{n+1+m}^{p^{m+1}} \subseteq A_n^{p^n}$ gilt, ist $(A'_{n+1})^p \subseteq A'_n$. Es gilt sogar Gleichheit, denn für $m \geqslant \max\{j(n), j(n+1)\}$ gilt $A'_n = A_{n+m}^{p^m} = A_{n+m+1}^{p^{m+1}} = (A_{n+m+1}^{p^m})^p = (A'_{n+1})^p$. Insgesamt gelten die Inklusionen

$$A' := \varprojlim_{y\mapsto y^p} A'_n \subseteq \varprojlim_{y\mapsto y^p} A_n \subseteq \varprojlim_{y\mapsto y^p} B_n = B,$$

bzgl. der projektiven Systeme $((A_n)_{n\in\mathbb{N}}, (f_{ij})_{i\leqslant j\in\mathbb{N}})$ und $((A'_n)_{n\in\mathbb{N}}, (f_{ij})_{i\leqslant j\in\mathbb{N}})$ mit f_{mn} wie bei B. Es genügt also zu zeigen, dass A' eine nicht leere Menge ist. Da die Abbildungen f_{mn} wegen $A'_n = (A'_m)^{p^{m-n}}$ surjektiv ist, lässt sich ein Element in A' konstruieren. Für $x_n \in A'_n$ wird $x_{n+1} \in A'_{n+1}$ gewählt mit $x_{n+1}^p = x_n$. Damit liegt $(x_n)_{n\geqslant 0}$ in A' und somit in B.

Sei nun $K^\flat$ algebraisch abgeschlossen. Angenommen es gibt eine endliche Körpererweiterung $E|K$ mit $[E:K] = d \geqslant 2$. Gilt $char(K) = p > 0$, so ist $K \cong K^\flat$, und es ist nichts zu zeigen. Wir nehmen daher ohne Einschränkung $char(K) = 0$ an. Damit ist $E|K$ eine separable Körpererweiterung und somit gibt es ein $y \in E$ mit $E = K(y)$. Durch Multiplikation mit einem geeigneten Element aus $K\backslash\{0\}$ kann man $y \in \mathcal{O}_E$ wählen. Wie oben sei o.B.d.A. $E|K$ eine Galoiserweiterung. Dann liegt das Minimalpolynom $m(X)$ von y in $\mathcal{O}_K[X]$. Im Folgenden wird ein Element konstruiert, das sowohl in $\mathcal{O}_K$ liegt, als auch eine Nullstelle von m ist. Das wird der Irreduzibilität von m widersprechen.
Nach 2.3 ii) gibt es ein $p^\flat \in \mathcal{O}_{K^\flat}$ mit $|p^\flat|_\flat = |p| = p^{-1}$. Wegen $\mathcal{O}_{K^\flat}/p^\flat\mathcal{O}_{K^\flat} \cong \mathcal{O}_K/p\mathcal{O}_K$ in 2.3 iv) gibt es ein normiertes Polynom $f(X) \in \mathcal{O}_{K^\flat}[X]$, sodass das Bild von $f(x) + p^\flat\mathcal{O}_{K^\flat}$ unter dem durch $\mathcal{O}_{K^\flat}/p^\flat\mathcal{O}_{K^\flat} \cong \mathcal{O}_K/p\mathcal{O}_K$ induzierten Ringhomomorphismus zwischen den entsprechenden Polynomringen das Polynom $m(X) + p\mathcal{O}_K$ ist. Da $K^\flat$ algebraisch abgeschlossen ist, zerfällt das Polynom $f(X)$ in Linearfaktoren, es gibt also $b_1, \ldots, b_d \in K^\flat$ mit $f(X) = \prod_{i=1}^d (X - b_i)$. Unter den Nullstellen gibt es ein $b_{i_0} \in \mathcal{O}_{K^\flat}$, denn aus der Annahme, dass alle Nullstellen nicht in $\mathcal{O}_{K^\flat}$ liegen, folgt aus Absolutbetragseigenschaften, dass $f(0) = \pm\prod_{i=0}^d b_i \notin \mathcal{O}_{K^\flat}$ ist. Dies widerspricht aber $f(X) \in \mathcal{O}_{K^\flat}[X]$.
Sei $y_1 := b_{i_0}^\# \in \mathcal{O}_K$. Da $m(X)$ in $K[x]$ irreduzibel ist, ist $m(y_1) \neq 0$. Das Bild unter dem obigen Ringhomomorphismus von $b_{i_0} + p^\flat\mathcal{O}_{K^\flat}$ ist $b_{i_0}^\# + p\mathcal{O}_K = y_1 + p\mathcal{O}_K$. Da $f(b_{i_0}) + p^\flat\mathcal{O}_{K^\flat} = 0$ ist, ist sein Bild $m(y_1) + p\mathcal{O}_K$ ebenfalls 0 und somit ist $m(y_1) \in p\mathcal{O}_K$. Damit gilt wegen $m(y_1) \neq 0$ die Ungleichung $0 < |m(y_1)| \leqslant |p|$. Wegen $|K| = |K^\flat|_\flat$ gibt es ein $a_1 \in K^\flat$ mit $|a_1|_\flat = |m(y_1)|$. Da $K^\flat$ algebraisch abgeschlossen ist, zerfällt das Polynom $X^d - a_1$ in Linearfaktoren und somit gibt es ein $b_1 \in K^\flat$ mit $b_1^d = a_1$. Wegen $|K^\flat|_\flat = |K|$ gibt es ein $c_1 \in K$ mit $|c_1| = |b_1|_\flat$ und somit ist $|c_1|^d = |m(y_1)| \neq 0$. Insbesondere ist $c_1 \neq 0$. Sei $m_1 := c_1^{-d} m(c_1X + y_1)$. Dieses Polynom ist offensichtlich normiert und vom Grad d und ist irreduzibel, denn angenommen es gibt ein Polynom $f(X)$, dessen Grad größer ist als 0 und $m(c_1X + y_1)$ teilt. Dann teilt $f(c_1^{-1}(X - y_1))$ das Polynom $m(c_1^{-1}(c_1X + y_1 - y_1)) = m(X)$, was aber der Irreduzibilität von $m(X)$ widerspricht. Darüberhinaus gilt $|m_1(0)| = |c_1|^{-d}|m(y_1)| = 1$. Damit ist $m_1(0)$ eine Einheit in $\mathcal{O}_K$. Seien $\lambda_1, \ldots, \lambda_d$ die Nullstellen von $m_1(X)$ in $\overline{K}$ und $K' := K(\lambda_1, \ldots, \lambda_d)$. Da m_1 irreduzibel ist, gibt es $\sigma_i \in Gal(K'|K)$ mit $\sigma_i(\lambda_i) = \lambda_1$. Elemente der Galoisgruppe sind nach 1.4.12 Isometrien und somit haben alle

Nullstellen den gleichen Absolutbetrag. Es gilt $1 = |m(0)| = \prod_{i=0}^{j} |\lambda_i|$ und somit haben alle Nullstellen Absolutbetrag 1. Das Polynom $m_1(X)$ liegt in $\mathcal{O}_K[X]$. Induktiv fortschreitend konstruiert man$(y_n)_{n\geqslant 1}, (c_n)_{n\geqslant 1}$ in $\mathcal{O}_K$ und eine Folge $(m_n)_{n\geqslant 0}$ normierter, irreduzibler Polynome $m_n \in \mathcal{O}_K[X]$ vom Grad d mit $m_0(X) = m(X), 0 < |c_n|^d = |m_{n-1}(y_n)| \leqslant |p|$ und $m_n(X) = c_n^{-d} m_{n-1}(c_n X + y_n)$ für alle $n \geqslant 1$. Es gilt $z := \sum_{n=1}^{\infty} (\prod_{i=0}^{n-1} c_i) y_n \in \mathcal{O}_K$, denn die Folge $(\sum_{n=1}^{s} (\prod_{i=0}^{n-1} c_i) y_n)_{s\geqslant 1}$ konvergiert in $\mathcal{O}_K$, da $\mathcal{O}_K$ vollständig ist und sie offensichtlich eine Cauchyfolge ist, da $|c_1..c_n| \leqslant |p|^{\frac{n}{d}}$ und y_n in $\mathcal{O}_K$ liegt. Es wird gezeigt, dass z eine Nullstelle von $m(X)$ ist. Dabei wird die Gleichheit

$$m(c_1..c_n X + c_1..c_{n-1} y_n + \ldots + c_1 y_2 + y_1) = c_1^d..c_n^d m_n(X) \tag{10}$$

hilfreich sein, welche per Induktion gezeigt wird. Für $n = 1$ ist $m(c_1 X + y_1) = c_1^d c_1^{-d} m(c_1 X + y_1) = c_1^d m_1(X)$. Es gilt

$$\begin{aligned} c_1^d..c_n^d m_n(X) &= c_1^d..c_n^d c_n^{-d} m_{n-1}(c_n X + y_n) \\ &= c_1^d..c_{n-1}^d m_{n-1}(c_n X + y_n) \\ &\overset{\text{IV}}{=} m(c_1..c_{n-1}(c_n X + y_n) + c_1..c_{n-2} y_{n-1} + \ldots + c_1 y_2 + y_1) \\ &= m(c_1..c_n X + c_1..c_{n-1} y_n + \ldots + c_1 y_2 + y_1). \end{aligned}$$

Mit (10) folgt nun

$$|m(c_1..c_n y_{n+1} + c_1..c_{n-1} y_n + \ldots + c_1 y_2 + y_1)| = |c_1^d..c_n^d m_n(y_{n+1})| \leqslant |p|^{n+1}.$$

Wegen der Stetigkeit von $\mathcal{O}_K \to \mathcal{O}_K, \quad x \mapsto m(x)$ gilt

$$m(z) = \lim_{n\to\infty} m(c_1..c_n y_{n+1} + \ldots + c_1 y_2 + y_1) = 0.$$

□

3 Ring der Wittvektoren

Im vorherigen Kapitel wurde aus einem perfektoiden Körper ein perfektoider Körper der Charakteristik p konstruiert. Das nächste Ziel ist die Konstruktion eines perfektoiden Körpers der Charakteristik 0 aus einem perfektoiden Körper der Charakteristik p. Dafür wird im folgenden Kapitel der sogenannte Ring der Wittvektoren eingeführt, der bei dieser Konstruktion eine große Rolle spielt.
Auch hier bildete die Vorlesung „p-adic Galois representations " von Herrn Prof. Dr. Kohlhaase die Grundlage.

Das Polynom $\Phi_n(X_0, \ldots, X_n) := \sum_{i=0}^{n} p^i X_i^{p^{n-i}} \in \mathbb{Z}[X_0, X_1, \ldots]$ heißt das **n−te Wittpolynom**.

Bemerkung 3.1
Es gelten $\Phi_0(X_0) = X_0$ und

$$\Phi_{n+1}(X_0, \ldots, X_{n+1}) = \Phi_n(X_0^p, \ldots, X_n^p) + p^{n+1} X_{n+1} = X_0 p^{n+1} + p\Phi_n(X_1, \ldots, X_{n+1}).$$

Lemma 3.2
Sei A ein kommutativer Ring, $m, n \in \mathbb{N}$ und $a_0, \ldots, a_n, b_0, \ldots, b_n \in A$. Dann gelten:

i) Für alle $i \in \{0, \ldots, n\}$ mit $a_i \equiv b_i \mod p^m A$ ist $\Phi_i(a_0, \ldots, a_i) \equiv \Phi_i(b_0, \ldots, b_i) \mod p^{m+i} A$.

ii) Die Umkehrung von i) gilt, falls $p \cdot 1$ kein Nullteiler in A ist, d.h. $A \to A,\ a \mapsto pa$ ist injektiv.

Beweis: i) Dies wird induktiv über n gezeigt. Sei $n = 0$ und $a_0 \equiv b_0 \mod p^m A$. Dann ist $\Phi_0(a_0) = a_0 \equiv b_0 = \Phi_0(b_0) \mod p^m A$.
Gelte nun die Aussage für n und für alle $i \in \{0, \ldots, n+1\}$ sei $a_i \equiv b_i \mod p^m A$. Dann gilt nach Induktionsvoraussetzung

$$\Phi_n(a_0^p, \ldots, a_n^p) \equiv \Phi_n(b_0^p, \ldots, b_n^p) \mod p^{m+n+1} A,$$

da nach 1.1.2 die Kongruenz $a_i^p \equiv b_i^p \mod p^{m+1} A$ gilt. Insgesamt ergibt sich also mit 3.1

$$\begin{aligned} \Phi_{n+1}(a_0, \ldots, a_{n+1}) &= \Phi_n(a_0^p, \ldots, a_n^p) + p^{n+1} a_{n+1} \equiv \Phi_n(b_0^p, \ldots, b_n^p) + p^{n+1} b_{n+1} \\ &= \Phi_{n+1}(b_0, \ldots, b_{n+1}) \mod p^{m+n+1} A, \end{aligned}$$

da $p^{n+1} a_{n+1} \equiv p^{n+1} b_{n+1} \mod p^{m+n+1} A$.
ii) Auch hier wird die Behauptung induktiv über n gezeigt. Sei $n = 0$ und $\Phi_0(a_0) \equiv \Phi_0(b_0) \mod p^m A$. Dann ist offensichtlich $a_0 \equiv b_0 \mod p^m A$. Gelte nun die Aussage für und sei $p \cdot 1$ kein Nullteiler. Da nach Induktionsvoraussetzung für alle $i \in \{0, \ldots, n\}$ die Kongruenz $a_i \equiv b_i \mod p^m A$ gilt, folgt mit (1.1.2) für alle $i \in \{0, \ldots, n\}$, dass $a_i^p \equiv b_i^p \mod p^{m+1} A$. Mit i) folgt

$$\Phi_n(a_0^p, \ldots, a_n^p) \equiv \Phi_n(b_0^p, \ldots, b_n^p) \mod p^{m+1+n} A. \tag{11}$$

Nach Voraussetzung gilt $\Phi_{n+1}(a_0, \ldots, a_{n+1}) \equiv \Phi_{n+1}(b_0, \ldots, b_{n+1}) \mod p^{m+n+1} A$ und somit ist wegen 3.1

$$\Phi_n(a_0^p, \ldots, a_n^p) + p^{n+1} a_{n+1} - \Phi_n(b_0^p, \ldots, b_n^p) - p^{n+1} b_{n+1} \in p^{m+n+1} A.$$

Insgesamt ergibt sich mit (11), dass $p^{n+1}(a_{n+1} - b_{n+1}) \in p^{m+n+1}$ ist. Da $p \cdot 1$ kein Nullteiler ist, ist $a_{n+1} - b_{n+1} \in p^m A$, also $a_{n+1} \equiv b_{n+1} \mod p^m A$. □

Sei A ein kommutativer Ring. Dann ist $\mathbf{A}^{\mathbb{N}} := \prod_{n \in \mathbb{N}} = \{(a_0, a_1, \ldots) : a_i \in A\}$ bzgl. der komponentenweise Addition und Multiplikation ein Ring. Ferner werden folgende Abbildungen definiert:

$$\begin{array}{llll} f_A & : & A^{\mathbb{N}} \to A^{\mathbb{N}} & ,(a_0, a_1, a_2, \ldots) \mapsto (a_1, a_2, \ldots) \\ v_A & : & A^{\mathbb{N}} \to A^{\mathbb{N}} & ,(a_0, a_1, a_2, \ldots) \mapsto (0, pa_0, pa_1, \ldots) \\ \Phi_n & : & A^{\mathbb{N}} \to A & ,(a_0, a_1, a_2, \ldots) \mapsto \Phi_n(a_0, \ldots, a_n) \\ \Phi_A & : & A^{\mathbb{N}} \to A^{\mathbb{N}} & ,(a_0, a_1, a_2, \ldots) \mapsto (\Phi_n(a_0, \ldots, a_n))_{n \geqslant 0} \end{array}$$

Lemma 3.3
Sei A ein kommutativer Ring.

i) Ist $p \cdot 1$ kein Nullteiler, so ist Φ_A injektiv.

ii) Φ_A ist bijektiv, wenn $p \cdot 1 \in A^\times$.

Beweis: i) Induktiv wird gezeigt, dass aus $(\Phi_n(a_0, \ldots, a_n))_{n \geqslant 0} = (\Phi_n(b_0, \ldots, b_n))_{n \geqslant 0}$ die Gleichheit $a_i = b_i$ für alle $i \geqslant 0$ folgt. Für $n = 0$ gilt $\Phi_0(a_0) = \Phi_0(b_0)$ und somit $a_0 = b_0$. Gelte nun $a_i = b_i$ für alle $i < n$. Nach 3.1 ist

$$\begin{aligned} \Phi_n(a_0, \ldots, a_n) &= \Phi_{n-1}(a_0^p, \ldots, a_{n-1}^p) + p^n a_n \quad \text{und} \\ \Phi_n(b_0, \ldots, b_n) &= \Phi_{n-1}(b_0^p, \ldots, b_{n-1}^p) + p^n b_n \end{aligned}$$

Nach Induktionsvoraussetzung ist $\Phi_{n-1}(a_0^p, \ldots, a_{n-1}^p) = \Phi_{n-1}(b_0^p, \ldots, b_{n-1}^p)$ und somit $p^n a_n = p^n b_n$. Es gilt $a_n = b_n$, da $p \cdot 1$ kein Nullteiler ist.
ii) Sei nun darüberhinaus $p \cdot 1$ invertierbar und $u = (u_n)_{n \geqslant 0} \in A^{\mathbb{N}}$. Definiere induktiv

$$\begin{aligned} a_0 &= u_0 \\ a_n &= (u_n - \Phi_{n-1}(a_0^p, \ldots, a_{n-1}^p))p^{-n}, \ n \geqslant 1 \end{aligned}$$

Dann ist $\Phi_A((a_n)_{n \geqslant 0}) = u$, da

$$\begin{aligned} \Phi_n(a_0, \ldots, a_n) &= \Phi_{n-1}(a_0^p, \ldots, a_{n-1}^p) + p^n a_n \\ &= \Phi_{n-1}(a_0^p, \ldots, a_{n-1}^p) + p^n(u_n - \Phi_{n-1}(a_0^p, \ldots, a_{n-1}^p)p^{-n} \\ &= u_n \ . \end{aligned}$$

□

Proposition 3.4
Seien A ein kommutativer Ring und $B \subseteq A$ ein Unterring von A, $\Phi_A((a_n)_{n \geqslant 0}) = (u_n)_{n \geqslant 0}$ und sei die Abbildung $A/B \to A/B$, $a' + B \mapsto pa' + B$ injektiv. Für $m \geqslant 0$ sind dann $u_0, \ldots, u_m \in B$, genau dann, wenn $a_0, \ldots, a_m \in B$.

Beweis: Eine Implikation wird induktiv über m bewiesen. Für $m = 0$ ist $a_0 = u_0$ und die Behauptung ist klar.
Gelte nun $u_0, \ldots, u_m \in B$. Nach Induktionsvoraussetzung gilt dann $a_0, \ldots, a_{m-1} \in B$. Ferner ist

$a_m p^m = u_m - \Phi_{m-1}(a_0^p, \ldots, a_{m-1}^p) \in B$ und da $a + B \mapsto pa + B$ injektiv ist, folgt $a_m \in B$.
Seien nun $a_0, \ldots, a_m \in B$. Es folgt $u_n = \Phi_n(a_0, \ldots, a_n) \in B$ für alle $n \in \{0, \ldots, m\}$, da Φ_n ein ganzzahliges Polynom ist. □

Proposition 3.5
Sei $\varphi : A \to A$ ein Ringendomorphismus mit $\varphi(a) \equiv a^p \mod pA$ für alle $a \in A$.

i) Seien $a_0, \ldots, a_{n-1} \in A$, $u_i = \Phi_i(a_0, \ldots, a_i)$ für alle $i \in \{0, \ldots, n-1\}$ und $u_n \in A$. Dann existiert genau dann ein $a_n \in A$ mit $u_n = \Phi_n(a_0, \ldots, a_n)$, wenn $\varphi(u_{n-1}) \equiv u_n \mod p^n A$ ist.

ii) $A' := \Phi_A(A^{\mathbb{N}})$ ist ein Unterring von $A^{\mathbb{N}}$, welcher sowohl f_A, als auch v_A invariant ist. Insbesondere gilt $A' = \{(u_n)_{n \geqslant 0} \in A^{\mathbb{N}} : \varphi(u_n) \equiv u_{n+1} \mod p^{n+1}A \text{ für alle } n \geqslant 0\}$.

Beweis: i) Es gilt

$$\begin{aligned} \varphi(u_{n-1}) &= \varphi(\Phi_{n-1}(a_0, \ldots, a_{n-1})) = \Phi_{n-1}(\varphi(a_0), \ldots, \varphi(a_{n-1})) \\ &\underset{\text{i)}}{\overset{3.2}{\equiv}} \Phi_{n-1}(a_0^p, \ldots, a_{n-1}^p) \mod p^n A. \end{aligned}$$

Die Gleichung

$$u_n = \Phi_n(a_0, \ldots, a_n) = \Phi_{n-1}(a_o^p, \ldots, a_{n-1}^p) + a_n p^n$$

ist äquivalent zur Kongruenz $u_n \equiv \varphi(u_{n-1}) \mod p^n A$.
ii) Seien $a := (a_n)_{n \geqslant 0} \in A^{\mathbb{N}}, b := (b_n)_{n \geqslant 0} \in A'$ mit $\Phi_A(a) = b$. Damit ist $b_n = \Phi_n(a_0, \ldots, a_n)$ für alle $n \geqslant 0$. Wegen i) ist dies äquivalent zu $\varphi(b_{n-1}) \equiv b_n \mod p^n A$. Demnach folgt die die Gleichheit

$$A' = \{(u_n)_{n \geqslant 0} \in A^{\mathbb{N}} : \varphi(u_n) \equiv u_{n+1} \mod p^{n+1}A \text{ für alle } n \geqslant 0\}.$$

A' ist offensichtlich multiplikativ und additiv abgeschlossen und ist somit ein Unterring von $A^{\mathbb{N}}$.
Seien $a \in A'$ und $b := f_A(a)$. Dann gilt für alle $n \in \mathbb{N}$, dass $\varphi(a_n) \equiv a_{n+1} \mod p^{n+1}A$ ist. Dies impliziert

$$\begin{aligned} \varphi(b_n) &= \varphi((f_A(a))_n) = \varphi(a_{n+1}) \equiv a_{n+2} \\ &= b_{n+1} \mod p^{n+2}A. \end{aligned}$$

Damit ist $\varphi(b_n) \equiv b_{n+1} \mod p^{n+1}A$ und somit ist $b \in A'$.
Seien $a \in A'$ und $b := v_A(a) = (0, pa_0, pa_1, \ldots)$. Dann gilt wieder für alle $n \geqslant 1$, dass $\varphi(a_n) \equiv a_{n+1} \mod p^{n+1}A$ ist. Es folgt

$$\begin{aligned} \varphi(b_n) - b_{n+1} &= \varphi((v_A(a))_n) - (v_A(a))_{n+1} = \varphi(pa_{n-1}) - pa_n \\ &= p\varphi(a_{n-1}) - a_n) \in pp^n A = p^{n+1}A. \end{aligned}$$

□

Mit der gewöhnlichen Ringstruktur auf $A^{\mathbb{N}}$ ist Φ_A kein Ringhomomorphismus, denn für $A = \mathbb{Z}$ ist $\Phi_A((1, 1, \ldots)) + \Phi_A((1, 0, \ldots)) = (2, 2 + p, \ldots) \neq (2, 2^p + p, \ldots) = \Phi_A((2, 1, \ldots))$. Im Folgenden wird eine Ringstruktur auf $A^{\mathbb{N}}$ konstruiert, sodass $\Phi_A : (A^{\mathbb{N}}, neu) \to (A^{\mathbb{N}}, alt)$ ein Ringhomomorphismus ist.

Proposition 3.6
Sei $A = \mathbb{Z}[X_0, X_1, \ldots, Y_0, Y_1, \ldots]$ *und* $X := (X_0, X_1, \ldots), Y := (Y_0, Y_1, \ldots) \in A^{\mathbb{N}}$.

i) Dann gibt es eindeutige Elemente $S = (S_n)_{n \geqslant 0}, P = (P_n)_{n \geqslant 0}, I = (I_n)_{n \geqslant 0}, F = (F_n)_{n \geqslant 0} \in A^{\mathbb{N}}$, *sodass gilt*

$$\begin{aligned} \Phi_A(S) &= \Phi_A(X) + \Phi_A(Y), \\ \Phi_A(P) &= \Phi_A(X) \cdot \Phi_A(Y), \\ \Phi_A(I) &= -\Phi_A(X), \\ \Phi_A(F) &= f_A(\Phi_A(X)). \end{aligned}$$

ii) Es gilt $S_n, P_n \in \mathbb{Z}[X_0, \ldots, X_n, Y_0, \ldots, Y_n]$, $I_n \in \mathbb{Z}[X_0, \ldots, X_n]$ *und* $F_n \in \mathbb{Z}[X_0, \ldots, X_{n+1}]$.

iii) Für alle $n \geqslant 0$ *ist* $F_n \equiv X_n^p \mod pA$.

iv) Es gelten

$$\begin{aligned} P_0(X_0, Y_0) &= X_0 Y_0, \\ P_1(X_0, X_1, Y_0, Y_1) &= X_0^p Y_1 + X_1 Y_0^p + p X_1 Y_1, \\ S_0(X_0, Y_0) &= X_0 + Y_0, \\ S_1(X_0, X_1, Y_0, Y_1) &= X_1 + Y_1 + \tfrac{1}{p}(X_0^p + Y_0^p - (X_0 + Y_0)^p). \end{aligned}$$

Beweis: i) Nach 3.5 ii) ist $\Phi_A(A^{\mathbb{N}})$ ein Unterring von $A^{\mathbb{N}}$, und somit sind $\Phi_A(X) + \Phi_A(Y)$, $\Phi_A(X) \cdot \Phi_A(Y)$ und $-\Phi_A(X)$ Elemente in $\Phi_A(A^{\mathbb{N}})$. Außerdem ist $f_A(\Phi_A(X))$ ein Element in $\Phi_A(A^{\mathbb{N}})$. Damit existieren S, P, I und $F \in A^{\mathbb{N}}$. Da p in A kein Nullteiler ist, ist wegen 3.3 Φ_A injektiv und somit sind S, P, I und F eindeutig bestimmt.
ii) Es gelten

$$\begin{aligned} u_n^S &:= \Phi_n(S_0, \ldots, S_n) = \Phi_n(X_0, \ldots, X_n) + \Phi_n(Y_0, \ldots, Y_n) \in \mathbb{Z}[X_0, \ldots, X_n, Y_0, \ldots, Y_n] \\ u_n^P &:= \Phi_n(P_0, \ldots, P_n) = \Phi_n(X_0, \ldots, X_n) \cdot \Phi_n(Y_0, \ldots, Y_n) \in \mathbb{Z}[X_0, \ldots, X_n, Y_0, \ldots, Y_n] \\ u_n^I &:= \Phi_n(I_0, \ldots, I_n) = -\Phi_n(X_0, \ldots, X_n) \in \mathbb{Z}[X_0, \ldots, X_n] \\ u_n^F &:= \Phi_n(F_0, \ldots, F_n) = (f_A(\Phi_A(X_0, X_1, \ldots))_n \\ &= \Phi_{n+1}(X_0, \ldots, X_{n+1}) \in \mathbb{Z}[X_0, \ldots, X_{n+1}] \end{aligned}$$

Da die Abbildung $A/B \to A/B, \quad a + B \mapsto ap + B$ mit $B = \mathbb{Z}[X_0, \ldots, X_n, Y_0, \ldots, Y_n]$ injektiv ist, folgt mit 3.4, dass $S_n, P_n \in \mathbb{Z}[X_0, \ldots, X_n, Y_0, \ldots, Y_n]$, $I_n \in \mathbb{Z}[X_0, \ldots, X_n]$ und $F_n \in \mathbb{Z}[X_0, \ldots, X_{n+1}]$ sind.
iii) Da $\Phi_n(F_0, \ldots, F_n) = \Phi_{n+1}(X_0, \ldots, X_{n+1}) = \Phi_n(X_0^p, \ldots, X_n^p) + p^{n+1} X_{n+1}$ ist, gilt $\Phi_n(F_0, \ldots, F_n) \equiv \Phi_n(X_0^p, \ldots, X_n^p) \mod p^{n+1}A$. Wegen 3.2 folgt, dass $F_n \equiv X_n^p \mod pA$ ist.
iv) Es gilt $P_0(X_0, Y_0) = X_0 Y_0$, denn

$$\begin{aligned} & \Phi_0(P_0(X_0, Y_0)) = \Phi_0((X_0))\Phi_0((Y_0)) \\ \Leftrightarrow\ & P_0(X_0, Y_0) = X_0 Y_0. \end{aligned}$$

Ebenso ist

$$\begin{aligned} & \Phi_0(S_0(X_0, Y_0) = \Phi_0(X_0) + \Phi_0(Y_0) \\ \Leftrightarrow\ & S(X_0, Y_0) = X_0 + Y_0. \end{aligned}$$

Für das zweite Folgenglied des Produkts gilt

$$\begin{aligned}
& \Phi_1(P_1(X_0,X_1,Y_0,Y_1)) = \Phi_1((X_0,X_1))\Phi_1(Y_0,Y_1) \\
\Leftrightarrow\ & P_0(X_0,Y_0)^p + pP_1(X_0X_1Y_0,Y_1) = (X_0^p+pX_1)(Y_0^p+pY_1) \\
\Leftrightarrow\ & pP_1(X_0,X_1,Y_0,Y_1) = -X_0^pY_0^p + X_0^pY_0^p + pX_0^pY_1 + pX_1Y_0^p + p^2X_1Y_1 \\
\Leftrightarrow\ & P_1(X_0,X_1,Y_0,Y_1) = X_0^pY_1 + X_1Y_0^p + pX_1Y_1.
\end{aligned}$$

Die Berechnung für $S_1(X_0,X_1,Y_0,Y_1)$ verläuft ähnlich. □

Lemma 3.7

i) Für alle $n \in \mathbb{N}$ ist $S_n(X_0,X_1^p,\dots,X_n^{p^n},Y_0,Y_1^p..,Y_n^{p^n}) \in \mathbb{Z}[X,Y]$ homogen vom Grad p^n.

ii) Für alle $n \in \mathbb{N}$ ist $P_n(X_0,X_1^p,\dots,X_n^{p^n},Y_0,Y_1^p..,Y_n^{p^n}) \in \mathbb{Z}[X,Y]$ eine Summe von Monomen $X^mY^{m'} = X_0^{m_0}..X_n^{m_n}Y_0^{m'_0}..Y_n^{m'_n}$ mit $m_0+\ldots+m_n = p^n = m'_0+\ldots+m'_n$, d.h. $P_n(X_0,X_1^p,\dots,X_n^{p^n},Y_0,\dots,Y_n^{p^n})$ ist homogen vom Grad p^n, sowohl als Polynom in X, als auch als Polynom in Y.

Beweis: i) Das Polynom $S_0(X_0,Y_0) = X_0+Y_0$ ist homogen und vom Grad $p^0 = 1$. Aufgrund der Definition der Addition und einer Eigenschaft von Φ_n gilt

$$\begin{aligned}
& p^nS_n(X_0,X_1^p,\dots,X_n^{p^n},Y_0,\dots,Y_n^{p^n}) \\
+\ & \Phi_{n-1}(S_0(X_0,Y_0)^p,\dots,S_{n-1}(X_0,\dots,X_{n-1}^{p^{n-1}},Y_0,\dots,Y_n^{p^{n-1}})^p) \\
=\ & \Phi_n(X_0,\dots,X_n^{p^n}) + \Phi_n(Y_0,\dots,Y_n^{p^n}).
\end{aligned}$$

Die Summe $\Phi_n(X_0,\dots,X_n^{p^n}) = \sum_{i=0}^n p^i(X_i^{p^i})^{p^{n-i}} = \sum_{i=0}^n p^iX_i^{p^n}$ ist homogen vom Grad p^n. Dies gilt analog für $\Phi_n(Y_0,\dots,Y_n^{p^n})$.
Nach Induktionsvoraussetzung ist $S_i := S_i(X_0,\dots,X_i^{p^i},Y_0,\dots,Y_i^{p^i})$ homogen und $\deg(S_i) = p^i$ für alle $i \leqslant n-1$. Nun ist $\Phi_{n-1}(S_0,\dots,S_{n-1}^p) = \sum_{i=0}^{n-1} p^i(S_i^p)^{p^{n-1-i}} = \sum_{i=0}^{n-1} p^iS_i^{p^{n-i}}$. Da $\deg(S_i^{p^{n-i}}) = p^n$ und $S_i^{p^{n-i}}$ homogen ist, ist $\Phi_{n-1}(S_0^p,\dots,S_{n-1}^p)$ homogen vom Grad p^n und somit ist $p^nS_n(X_0,\dots,X_n^{p^n},Y_0,\dots,Y_n^{p^n})$ vom Grad p^n, da das Monom $p^nX_n^{p^n}$ ein Summand der Summe $\Phi_n(X_0,\dots,X_n^{p^n})$ ist, aber kein Summand der Summe $\Phi_{n-1}(S_0^p,\dots,S_{n-1}^p) \in \mathbb{Z}[X_0,\dots,X_{n-1},Y_0,\dots,Y_{n-1}]$. Darüberhinaus ist es homogen, da Summen homogener Polynome gleichen Grades homogen sind.
ii) Aufgrund der Definition von P_n und einer Eigenschaft von Φ_n gilt

$$\begin{aligned}
& p^nP_n(X_0,X_1^p,\dots,X_n^{p^n},Y_0,\dots,Y_n^{p^n}) \\
+\ & \Phi_{n-1}(P_0(X_0,Y_0)^p,\dots,P_{n-1}(X_0,\dots,X_{n-1}^{p^{n-1}},Y_0,\dots,Y_n^{p^{n-1}})^p) \\
=\ & \Phi_n(X_0,\dots,X_n^{p^n}) \cdot \Phi_n(Y_0,\dots,Y_n^{p^n}).
\end{aligned}$$

Wie in i) sind auch hier die Summen $\Phi_n(X_0,\dots,X_n^{p^n})$ und $\Phi_n(Y_0,\dots,Y_n^{p^n})$ homogen vom Grad p^n. Das Produkt dieser Summen ist eine Summe von Monomen mit $\alpha_{ij}X_i^{p^n}Y_j^{p^n}$ mit $i,j \leqslant n$ und $\alpha_{ij} \in \mathbb{Z}$.
Nach Induktionsvoraussetzung ist $P_i := P_i(X_0,\dots,X_i^{p^i},Y_0,\dots,Y_i^{p^i})$ eine Summe von Monomen $X_0^{m_0}..X_i^{m_i}Y_0^{m'_0}..Y_i^{m'_i}$ mit $m_0+\ldots+m_i = p^n = m'_0+\ldots+m'_i$ für alle $i < n$.
Damit ist $\Phi_n(P_0,\dots,P_{n-1}^p) = \sum_{i=0}^{n-1} p^iP_i^{p^{n-i}}$ eine Summe von Monomen mit $\deg(P_i^{p^{n-i}}) = p^{i+n-i} = p^n$ sowohl in $X_0,\dots,X_{n-1}$, als auch in $Y_0,\dots,Y_{n-1}$. Damit folgt die Behauptung. □

Sei B ein kommutativer Ring mit 1. Im Folgenden wird gezeigt, dass die Abbildungen

$$\begin{array}{rccl} \oplus_B & : & B^{\mathbb{N}} \times B^{\mathbb{N}} & \to & B^{\mathbb{N}} \\ & & ((a_n)_{n\geqslant 0}, (b_n)_{n\geqslant 0}) & \mapsto & (S_n(a_0, \ldots, a_n, b_0, \ldots, b_n))_{n\geqslant 0} \end{array}$$

$$\begin{array}{rccl} \odot_B & : & B^{\mathbb{N}} \times B^{\mathbb{N}} & \to & B^{\mathbb{N}} \\ & & ((a_n)_{n\geqslant 0}, (b_n)_{n\geqslant 0}) & \mapsto & (P_n(a_0, \ldots, a_n, b_0, \ldots, b_n))_{n\geqslant 0} \end{array}$$

Ringoperationen auf $B^{\mathbb{N}}$ definieren. $B^{\mathbb{N}}$ mit diesen Verknüpfungen wird mit $W(B)$ bezeichnet.

Theorem 3.8

Sei B ein kommutativer Ring mit 1.

i) $(W(B), \oplus_B, \odot_B)$ *ist ein kommutativer Ring mit dem Nullelement* $0_{W(B)} := (0, 0, \ldots)$ *und dem Einselement* $1_{W(B)} := (1, 0, 0..)$. *Das inverse Element zu* $(b_n)_{n\geqslant 0}$ *ist* $(I_n(b_0, \ldots, b_n))_{n\geqslant 0}$.

ii) Die Abbildung $\Phi_B : W(B) \to B^{\mathbb{N}}$ *ist ein Ringhomomorphismus, insbesondere auch die Abbildung* $\Phi_m : W(B) \to B, \quad (b_n)_{n\geqslant 0} \mapsto \Phi_m(b_0, \ldots, b_m)$ *mit* $m \geqslant 0$.

iii) Ist $\rho : B_1 \to B_2$ *ein Ringhomomorphismus kommutativer Ringe, dann gilt dies auch für die Abbildung*
$W(\rho) : W(B_1) \to W(B_2), \quad (b_n)_{n\geqslant 0} \mapsto (\rho(b_n))_{n\geqslant 0}$.

Beweis: i) Zunächst überprüft man, ob $W(\rho)$ für einen Ringhomorphismus $\rho : B_1 \to B_2$ bzgl beider Abbildungen additiv bzw. multiplikativ ist. Sei dazu $f \in \mathbb{Z}[X_0, \ldots, X_m]$ und $b_0, \ldots, b_m \in B_1$. Dann gilt aufgrund der Homomorphieigenschaft von ρ, dass $\rho(f(b_0, \ldots, b_m)) = f(\rho(b_0), \ldots, \rho(b_m))$ ist. Damit ist also

$$\begin{aligned} W(\rho)((a_n)_{n\geqslant 0} \oplus (b_n)_{n\geqslant 0})) &= W(\rho)((S_n(a_0, \ldots, a_n, b_0, \ldots, b_n)_{n\geqslant 0}) \\ &= (S_n(\rho(a_0), \ldots, \rho(a_n), \rho(b_0), \ldots, \rho(b_n))_{n\geqslant 0} \\ &= W(\rho)(a_n)_{n\geqslant 0} \oplus W(\rho)(b_n)_{n\geqslant 0}. \end{aligned} \tag{12}$$

Bezüglich $\odot$ gilt dies analog.
Darüberhinaus ist $W(\rho)(1_{W(B_1)}) = (\rho(1_{B_1}), \rho(0_{B_1}), \ldots) = (1_{B_1}, 0_{B_1}, \ldots)$. Nach Definition von $\oplus_B$ und $\odot_B$ gelten

$$\begin{aligned} \Phi_B((a_n)_{n\geqslant 0} \oplus_B (b_n)_{n\geqslant 0}) = \Phi_B((a_n)_{n\geqslant 0}) + \Phi_B((b_n)_{n\geqslant 0})) \\ \Phi_B((a_n)_{n\geqslant 0} \odot_B (b_n)_{n\geqslant 0}) = \Phi_B((a_n)_{n\geqslant 0}) \cdot \Phi_B((b_n)_{n\geqslant 0})). \end{aligned} \tag{13}$$

Sei $B_1 := \mathbb{Z}[(X_b)_{b\in B}]$. Da B_1 ein freier $\mathbb{Z}-$Modul ist, d.h. B_1 ist torsionsfrei, ist p kein Nullteiler und somit ist die Abbildung $\Phi_{B_1} : W(B_1) \to B_1^{\mathbb{N}}$ nach 3.3 i) injektiv. Damit ist

$$(a_n)_{n\geqslant 0} \odot_{B_1} ((b_n)_{n\geqslant 0} \oplus_{B_1} (c_n)_{n\geqslant 0}) = ((a_n)_{n\geqslant 0} \odot_{B_1} (b_n)_{n\geqslant 0}) \oplus_{B_1} ((a_n)_{n\geqslant 0} \odot_{B_1} (c_n)_{n\geqslant 0}),$$

da wegen (13) und der Ringaxiome in $B_1^{\mathbb{N}}$ gilt:

$$\begin{aligned} &\Phi_{B_1}((a_n)_{n\geqslant 0} \odot_{B_1} ((b_n)_{n\geqslant 0} \oplus_{B_1} (c_n)_{n\geqslant 0})) \\ &= \Phi_{B_1}((a_n)_{n\geqslant 0} \odot_{B_1} (b_n)_{n\geqslant 0} \oplus_{B_1} (a_n)_{n\geqslant 0} \odot_{B_1} (c_n)_{n\geqslant 0}). \end{aligned}$$

Außerdem gelten offensichtlich wegen der Injektivität von Φ_{B_1}, dass $(a_n)_{n\geqslant 0} \oplus_{B_1} (0_{B_1})_{n\geqslant 0} = (a_n)_{n\geqslant 0}$ und $(a_n)_{n\geqslant 0} \odot_{B_1} (1_{B_1})_{n\geqslant 0} = (a_n)_{n\geqslant 0}$ sind, wobei zu beachten ist, dass nach Definition von Φ_A stets

$\Phi_A((0)_{n\geqslant 0}) = (0)_{n\geqslant 0}$ und $\Phi_A((1,0,0,\ldots)) = (1,1,1,\ldots)$ gilt. Ebenso veerbt sich die Assoziativität auf $W(B_1)$.
Das inverse Element der Addition für ein $(b_n)_{n\geqslant 0}$ ist $(I_n(b_0,\ldots,b_n))_{n\geqslant 0}$, da

$$\begin{aligned}
\Phi_{B_1}((b_n)_{n\geqslant 0} \oplus_{B_1} (I_n(b_0,\ldots,b_n))_{n\geqslant 0}) &= \Phi_{B_1}((b_n)_{n\geqslant 0}) + (\Phi_{B_1}(I_n(b_0,\ldots,b_n))_{n\geqslant 0}) \\
&= \Phi_{B_1}((b_n)_{n\geqslant 0}) - \Phi_{B_1}((b_n)_{n\geqslant 0}) = (0_{B_1})_{n\geqslant 0} \\
&= \Phi_{B_1}((0_{B_1})_{n\geqslant 0}).
\end{aligned}$$

Damit ist $(W(B_1), \oplus_{B_1}, \odot_{B_1})$ ein kommutativer Ring mit 1.
Da $\rho : B_1 = \mathbb{Z}[(X_b)_{b\in B}] \to B,\ X_b \mapsto b$ ein surjektiver Ringhomorphismus ist, ist auch $W(\rho)$ surjektiv.
Wegen (12) und $W(\rho)(1_{W(B_1)}) = 1_{W(B)}$, ist $(W(B), \oplus_B, \odot_B)$ ein kommutativer Ring mit 1.
ii) Wegen (13) und $\Phi_n(1,0,\ldots,0) = 1^{p^n} + \sum_{i=1}^{n} p^i 0^{p^{n-i}}$ für alle $n \geqslant 0$ folgt die Behauptung.
iii) Dies gilt wegen (12). □

Definition 3.9
Der Ring $(W(B), \oplus_B, \odot_B)$ heißt **Ring der Wittvektoren mit Koeffizienten in B**.
Die Subtraktion wird mit
$\ominus_B : W(B) \times W(B) \to W(B),\quad ((a_n)_{n\geqslant 0}, (b_n)_{n\geqslant 0}) \mapsto (a_n)_{n\geqslant 0} \oplus (I_n(b_0,\ldots,b_n))_{n\geqslant 0}$ bezeichnet.
Falls keine Verwechselung möglich ist, wird $\oplus_B, \odot_B, \ominus_B$ mit $\oplus, \odot, \ominus$ bezeichnet. Ist $b = (b_0, b_1, \ldots) \in W(B)$, dann heißt $\Phi_n(b_0,\ldots,b_n)$ die **n−te Phantomkomponente von** b.
Die Abbildung $F_B : W(B) \to W(B),\quad (b_n)_{n\geqslant 0} \mapsto (F_n(b_0,\ldots,b_n))_{n\geqslant 0}$ heißt **Frobenius**.
Die Abbildung $V_B : W(B) \to W(B),\quad (b_n)_{n\geqslant 0} \mapsto (0, b_0, b_1, \ldots)$ heißt **Verschiebung**.

Lemma 3.10
Seien B_1, B_2 kommutative Ringe mit Eins und sei $\rho : B_1 \to B_2$ ein Ringhomomorphismus. Dann kommutieren die folgenden Diagramme

$$\begin{tikzcd}
W(B) \arrow[r, "\Phi_B"] \arrow[d, "F_B"'] & B^{\mathbb{N}} \arrow[d, "f_B"] \\
W(B) \arrow[r, "\Phi_B"'] & B^{\mathbb{N}}
\end{tikzcd}
\qquad
\begin{tikzcd}
W(B) \arrow[r, "\Phi_B"] \arrow[d, "V_B"'] & B^{\mathbb{N}} \arrow[d, "v_B"] \\
W(B) \arrow[r, "\Phi_B"'] & B^{\mathbb{N}}
\end{tikzcd}$$

$$\begin{tikzcd}
W(B_1) \arrow[r, "F_{B_1}"] \arrow[d, "W(\rho)"'] & W(B_1) \arrow[d, "W(\rho)"] \\
W(B_2) \arrow[r, "F_{B_2}"'] & W(B_2)
\end{tikzcd}
\qquad
\begin{tikzcd}
W(B_1) \arrow[r, "V_{B_1}"] \arrow[d, "W(\rho)"'] & W(B_1) \arrow[d, "W(\rho)"] \\
W(B_2) \arrow[r, "V_{B_2}"'] & W(B_2).
\end{tikzcd}$$

Beweis: Das erste Diagramm kommutiert aufgrund der Konstruktion der Polynome F_n.

Sei $(a_n)_{n\geqslant 0} \in W(B)$. Dann ist

$$\begin{aligned}
v_B \circ \Phi_B((a_n)_{n\geqslant 0}) &= v_B((\Phi_n(a_0,\dots,a_n))_{n\geqslant 0}) \\
&= \left(\begin{cases} p\Phi_{n-1}(a_0,\dots,a_{n-1}), & n>0 \\ 0, & n=0 \end{cases}\right)_{n\geqslant 0} \\
&= \left(\begin{cases} p\Phi_{n-1}(a_0,\dots,a_{n-1}) + 0p^n, & n>0 \\ 0, & n=0 \end{cases}\right)_{n\geqslant 0} \\
&\overset{3.1}{=} (\Phi_n(0,a_0,a_1,\dots))_{n\geqslant 0} \\
&= \Phi_B((0,a_0,a_1,\dots)) = \Phi_B \circ V((a_n)_{n\geqslant 0}).
\end{aligned}$$

Damit ist das zweite Diagramm kommutativ.
Für die Kommutativität des darauffolgenden Diagramms sei $(a_n)_{n\geqslant 0} \in W(B_1)$. Dann gilt wegen der Ganzzahligkeit der Polynome F_n in 3.6, dass

$$\begin{aligned}
W(\rho) \circ F_{B_1}((a_n)_{n\geqslant 0} &= W(\rho)((F_n(a_0,\dots,a_n))_{n\geqslant 0}) = (F_n(\rho(a_0),\dots,\rho(a_n)))_{n\geqslant 0} \\
&= F_{B_2} \circ W(\rho)((a_n)_{n\geqslant 0}).
\end{aligned}$$

Nun wird gezeigt, dass das letzte Diagramm kommutiert. Sei dazu $(a_n)_{n\geqslant 0} \in W(B_1)$. Dann ist

$$\begin{aligned}
W(\rho) \circ V_{B_1}((a_n)_{n\geqslant 0}) &= W(\rho)(0,a_0,a_1,\dots) = (\rho(0),\rho(a_0),\rho(a_1),\dots) \\
&= V_{B_2} \circ W(\rho)((a_n)_{n\geqslant 0}).
\end{aligned}$$

□

Proposition 3.11
Sei B ein kommutativer Ring mit Eins. Dann gelten:

i) F_B ist ein Ringendomorphismus von $W(B)$.

ii) V_B ist bzgl. der Addition in $W(B)$ ein Gruppenhomomorphismus.

iii) Für alle $b \in W(B)$ gilt $(F_B \circ V_B)(b) = pb := \bigoplus_{i=1}^n b$.

iv) Für alle $a, b \in W(B)$ ist $V_B(a \odot F_B(b)) = V_B(a) \odot b$.

v) Für alle $b \in W(B)$ gilt $F_B(b) \equiv b^p := \bigodot_{i=1}^p b \mod pW(B)$.

Beweis: i) Sei wieder $B_1 = \mathbb{Z}[(X_b)_{b\in B}]$ und $\rho : B_1 \to B,\quad X_b \mapsto b$. Dann ist $\Phi_{B_1} : W(B_1) \to B_1^{\mathbb{N}}$ injektiv. Außerdem gilt wegen der Homomorphieeigenschaft von $\Phi_{B_1} : W(B_1) \to B_1^{\mathbb{N}}$ und $f_{B_1} : B_1^{\mathbb{N}} \to B_1^{\mathbb{N}}$, dass

$$\begin{aligned}
\Phi_{B_1} \circ F_{B_1}(x \oplus y) &\overset{3.10}{=} f_{B_1} \circ \Phi_{B_1}(x \oplus y) = f_{B_1} \circ \Phi_{B_1}(x) + f_{B_1} \circ \Phi_{B_1}(y) \\
&\overset{3.10}{=} \Phi_{B_1} \circ F_{B_1}(x) + \Phi_{B_1} \circ F_{B_1}(y) = \Phi_{B_1}(F_{B_1}(x) \oplus F_{B_1}(y))
\end{aligned}$$

ist. Also gilt $F_{B_1}(x \oplus y) = F_{B_1}(x) \oplus F_{B_1}(y)$. Analog zeigt man, dass F_{B_1} und $\odot$ kommutieren. Darüberhinaus ist $F_{B_1}(1_{W(B_1)}) = 1_{W(B_1)}$, wegen

$$\Phi_{B_1} \circ F_{B_1}(1_{W(B_1)}) = f_{B_1} \circ \Phi_{B_1}(1_{W(B_1)}) = f_{B_1}(1_{B_1^{\mathbb{N}}}) = 1_{B_1^{\mathbb{N}}} = \Phi_{B_1}(1_{W(B_1)}).$$

Daher ist F_{B_1} ein Ringhomomorphismus. Da nach 3.10 die Gleichung $F_B \circ W(\rho) = W(\rho) \circ F_{B_1}$ gilt und $W(\rho)$ surjektiv ist, ist auch F_B ein Ringhomomorphismus.
ii) Auch hier gilt wie in i) die Gleichung $\Phi_{B_1} \circ V_{B_1}(x \oplus y) = \Phi_{B_1}(V_{B_1}(x) \oplus V_{B_1}(y))$. Aufgrund der Injektivität von Φ_{B_1} ist V_{B_1} bzgl. der Addition auf $W(B_1)$ ein Gruppenhomomorphismus. Die Gültigkeit der Gleichung $V_B \circ W(\rho) = W(\rho) \circ V_{B_1}$ gilt wegen 3.10 und die Surjektivität von $W(\rho)$ impliziert, dass V_B bzgl. der Addition auf $W(B)$ ein Gruppenhomomorphismus ist.
iii) Sei $b = (b_n)_{n\geqslant 0} \in W(B_1)$. Wegen 3.10 gilt dann:

$$\begin{aligned}
\Phi_{B_1}(F_{B_1} \circ V_{B_1}(b)) &= f_{B_1} \circ \Phi_{B_1} \circ V_{B_1}(b) = f_{B_1} \circ v_{B_1} \circ \Phi_{B_1}(b) \\
&= f_{B_1}((0, \Phi_0(b_0), \Phi_1(b_0, b_1), \ldots)) = (p\Phi_0(b_0), p\Phi_1(b_0, b_1), \ldots) \\
&= p(\Phi_{B_1}(b)) = \Phi_{B_1}(pb).
\end{aligned}$$

Es folgt somit $F_{B_1} \circ V_{B_1} = pb$ für alle $b \in W(B_1)$. Sei $a = (a_n)_{n\geqslant 0} \in W(B)$. Dann gibt es ein $b \in W(B_1)$ mit $W(\rho)(b) = a$. Insgesamt ergibt sich wieder mit 3.10

$$\begin{aligned}
F_B \circ V_B(a) &= F_B \circ V_B \circ W(\rho)(b) = F_B \circ W(\rho) \circ V_{B_1}(b) \\
&= W(\rho) \circ F_{B_1} \circ V_{B_1}(b) = W(\rho)(pb) = pW(\rho)(b) = pa.
\end{aligned}$$

iv) Für $a = (a_n)_{n\geqslant 0}, b = (b_n)_{n\geqslant 0} \in B^{\mathbb{N}}$ gilt

$$\begin{aligned}
v_B(af_B(b)) &= v_B((a_n)_{n\geqslant 0}(b_1, b_2, b_3, \ldots)) = v_B((a_0b_1, a_1b_2, a_2b_3, \ldots)) \\
&= (0, pa_0b_1, pa_1b_2, pa_2b_3, \ldots) \\
&= (0, pa_0, pa_1, pa_2, \ldots)(b_0, b_1, b_2, \ldots) \\
&= v_B(a)b.
\end{aligned} \tag{14}$$

Diese Gleichheit impliziert aufgrund der Multiplikativitätvon v_{B_1}

$$\begin{aligned}
\Phi_{B_1}(V_{B_1}(a \odot F_{b_1}(b))) &= \Phi_{B_1}(V_{B_1}(a)) \odot \Phi_{B_1}(V_{B_1} \circ F_{B_1}(b)) \\
&= v_{B_1}(\Phi_{B_1}(a)) \odot v_{B_1}(f_{B_1} \circ \Phi_{B_1}(b)) \\
&\overset{(14)}{=} v_{B_1}(\Phi_{B_1}(a)) \odot \Phi_{B_1}(b) = \Phi_{B_1}(V_{B_1}(a) \odot b).
\end{aligned}$$

Aufgrund der Injektivität von Φ_{B_1} ist $V_{B_1}(a \odot F_{B_1}(b)) = V_{B_1}(a) \odot b$ für alle $a, b \in W(B_1)$.
Seien $x, y \in W(B)$ und $a, b \in W(B_1)$ mit $W(\rho)(a) = x$ und $W(\rho)(b) = y$. Dann ist

$$\begin{aligned}
V_B(x \odot_B F_B(y)) &= V_B(W(\rho)(a) \odot_B F_B \circ W(\rho)(y)) \\
&= V_B(W(\rho)(a) \odot_B W(\rho) \circ F_{B_1}(b)) = V_B \circ W(\rho)(a \odot_{B_1} F_{B_1}(b)) \\
&= W(\rho) \circ V_{B_1}(a \odot_{B_1} F_{B_1}(b)) = W(\rho)(V_{B_1}(a) \odot_{B_1} b) \\
&= V_B \circ W(\rho)(a) \odot W(\rho)(b) = V_B(x) \odot_B y.
\end{aligned}$$

v) Der Ringhomomorphismus $\varphi : B_1 \to B_1, \quad \sum_{b\in B} a_b X_b \to \sum_{b\in B} a_b X_b^p$, wobei alle, bis auf endlich viele Koeffizienten a_b null sind, erfüllt die Kongruenz $\varphi(a) \equiv a^p \mod pB_1$ für alle $a \in B_1$. Diese folgt aus dem binomischen Lehrsatz, dem Kleinen Fermatschen Satz und der Tatsache, dass p den Binomialkoeffizienten $\binom{p}{k}$ für alle $k \in \{1, \ldots, p-1\}$ teilt.
Mit 3.5 ii) folgt

$$\Phi_{B_1}(W(B)) = \{(u_n)_{n\geqslant 0} \in B_1^{\mathbb{N}} : \varphi(u_n) \equiv u_{n+1} \mod p^{n+1}B_1\}$$

Sei $\tilde{b} \in B_1$ und $a = (a_n)_{n\geqslant 0} = \Phi_{B_1}(\tilde{b})$. Mit 3.10 folgt

$$\Phi_{B_1}(F(\tilde{b}) \ominus \tilde{b}^p) = f_{B_1} \circ \Phi_{B_1}(\tilde{b}) - \Phi_{B_1}(\tilde{b})^p = f_{B_1}(a) - a^p = (a_{n+1} - a_n^p)_{n\geqslant 0}.$$

Damit sind $(a_n)_{n\geqslant 0}$ und $f_{B_1}(a) - a^p$ Elemente in $\Phi_{B_1}(W(B))$ und somit gelten

$$\begin{aligned} \varphi(a_n) &\equiv a_n^p \mod pB_1, \\ \varphi(a_n) &\equiv a_{n+1} \mod p^{n+1}B_1. \end{aligned}$$

Dies impliziert $a_{n+1} - a_n^p \equiv \varphi(a_n) - \varphi(a_n) \equiv 0 \mod pB_1$ für alle $n \geqslant 0$. Sei $c_n \in B_1$ mit $a_{n+1} - a_n^p = pc_n$. Dann ist

$$pc_{n+1} - p\varphi(c_n) = a_{n+2} - \varphi(a_{n+1}) - (a_{n+1}^p - \varphi(a_n)^p).$$

Dabei gilt $a_{n+2} - \varphi(a_{n+1}) \in p^{n+2}B_1$. Wegen 1.1.2 und $a_{n+1} - \varphi(a_n) \in p^{n+1}B_1$ ist $a_{n+1}^p - \varphi(a_n)^p$ ein Element in $p^{n+2}B_1$. Dann ist auch $pc_{n+1} - p\varphi(c_n) \in p^{n+2}B$. Da p kein Nullteiler ist, ist $c_{n+1} - \varphi(c_n) \in p^{n+1}B$.

Damit ist $c = (c_n)_{n\geqslant 0} \in \Phi_{B_1}(W(B_1))$, d.h. es gibt $d \in W(B_1)$ mit $\Phi_{B_1}(d) = c$. Dann ist

$$\Phi_{B_1}(F(\tilde{b}) \ominus \tilde{b}^p) = p\Phi_{B_1}(d) = \Phi_{B_1}(pd).$$

Aufgrund der Injektivität von Φ_{B_1} gilt $F(\tilde{b}) \ominus \tilde{b}^p = pd \in pW(B_1)$. Da $W(\rho)$ surjektiv ist, gibt es ein $b \in W(B)$ mit $W(\rho)(b) = \tilde{b}$. Dann folgt

$$\begin{aligned} F_B(b) \ominus b^p &= F_B \circ W(\rho)(\tilde{b}) \ominus W(\rho)(\tilde{b})^p \\ &\overset{3.10}{=} W(\rho) \circ F_{B_1}(\tilde{b}) \ominus W(\rho)(\tilde{b})^p = W(\rho)(F_{B_1}(\tilde{b}) \ominus (\tilde{b})^p) \\ &= W(\rho)(pd) = pW(\rho d) \in pW(B). \end{aligned}$$

□

Sei B ein kommutativer Ring mit 1 und V die Verschiebung auf $W(B)$. Für $m \geqslant 0$ wird die Menge $Im(V^m) = \{(b_n)_{n\geqslant 0} \in W(B) : b_0 = .., b_{m-1} = 0\}$ mit $V_m(B)$ bezeichnet.

Es gilt $W(B) = V_0(B) \supsetneq V_1(B) \supsetneq ...$ und $\bigcap_{n\geqslant 0} V_m(B) = 0$. Wegen 3.11 ii) und iv) sind für alle $m \geqslant 0$ die Mengen $V_m(B)$ Ideale.

Der Ring $W(B)/V_m(B)$ heißt **Ring der Wittvektoren der Länge m** und wird mit $W_m(B)$ bezeichnet.

Lemma 3.12

Sei B ein kommutativer Ring mit Eins und $m \geqslant 1$.

i) Für $(b_n)_{n\geqslant 0} \in W(B)$ ist $(b_n)_{n\geqslant 0} = (b_0, \ldots, b_{m-1}, 0, 0, \ldots) \oplus (0, \ldots, 0, b_m, b_{m+1}, \ldots)$.

ii) Die Abbildung

$$\begin{aligned} B^m &\to W_m(B) \\ (b_0, \ldots, b_{m-1}) &\mapsto (b_0, \ldots, b_{m-1}, 0, 0, \ldots) \oplus V_m(B) \end{aligned}$$

ist bijektiv.

Beweis: i) Es gilt für alle $k \in \mathbb{N}$

$$\Phi_k(b_0, \ldots, b_{m-1}, 0, \ldots, 0) + \Phi_k(0, \ldots, 0, b_m, \ldots, b_k) = \Phi_k(b_0, \ldots, b_k),$$

da

$$\begin{aligned} \Phi_k(b_0, \ldots, b_{m-1}, 0, \ldots, 0) &= \begin{cases} \Phi_k(b_0, \ldots, b_k), & 0 \leqslant k < m \\ \sum\limits_{i=0}^{m-1} p^i b_i^{p^{k-i}}, & 0 \leqslant m \leqslant k \end{cases} \\ \Phi_k(0, \ldots, 0, b_m, \ldots, b_k) &= \begin{cases} 0, & 0 \leqslant k < m \\ \sum\limits_{i=m}^{k} p^i b_i^{p^{k-i}}, & m \leqslant k \end{cases} . \end{aligned}$$

Damit ist

$$\begin{aligned} & \Phi_B((b_0, \ldots, b_{m-1}, 0, 0, \ldots) \oplus (0, \ldots, 0, b_m, b_{m+1}, \ldots)) \\ = \; & \Phi_B((b_0, \ldots, b_{m-1}, 0, 0, \ldots)) + \Phi_B((0, \ldots, 0, b_m, b_{m+1}, \ldots)) \\ = \; & (\Phi_k(b_0, \ldots, b_{m-1}, 0, \ldots, 0))_{k \geqslant 0} + (\Phi_k(0, \ldots, 0, b_m, \ldots, b_k))_{k \geqslant 0} \\ = \; & \Phi_B((b_0, \ldots, b_{m-1}, b_m, b_{m+1}, \ldots)). \end{aligned}$$

Die Behauptung gilt somit für $B_1 = \mathbb{Z}[(X_b)_{b \in B}]$, da die Abbildung Φ_{B_1} nach nach 3.3 i) injektiv ist. Sei wieder $\rho : B_1 \mapsto B, \quad X_b \mapsto b$ und $\widehat{b} = (b_0, \ldots, b_{m-1}, 0, \ldots), \tilde{b} = (0, \ldots, 0, b_m, b_{m+1}, \ldots) \in W(B)$. Wegen der Surjektivität von $W(\rho)$ gibt es $\widehat{x} = (x_0, \ldots, x_{m-1}, 0, \ldots), \tilde{x} = (0, \ldots, 0, x_m, x_{m+1}, \ldots) \in W(B_1)$, sodass $W(\rho)(\widehat{x}) = \widehat{b}$ und $W(\rho)(\tilde{x}) = (\tilde{b})$. Folglich ist

$$\begin{aligned} \widehat{b} \oplus_B \tilde{b} &= W(\rho)(\widehat{x}) \oplus_B W(\rho)(\tilde{x}) = W(\rho)(\widehat{x} \oplus_{B_1} \tilde{x}) \\ &= W(\rho)((x_0, \ldots, x_{m-1}, x_m, x_{m+1}, \ldots)) = (b_0, \ldots, b_{m-1}, b_m, b_{m+1}, \ldots). \end{aligned}$$

ii) Die Abbildung ist surjektiv, da mit i)

$$\begin{aligned} (b_0, b_1, b_2, \ldots) \oplus V_m(B) &= (b_0, \ldots b_{m-1}, 0, \ldots) \oplus (0, \ldots, 0, b_m, b_{m+1}, \ldots) \oplus V_m(B) \\ &= (b_0, \ldots, b_{m-1}, 0, \ldots) \oplus V_m(B) \end{aligned}$$

gilt und somit $(b_0, \ldots, b_{m-1})$ im Urbild von $(b_0, b_1, \ldots) \oplus V_m(B)$ liegt.
Sei $(b_0, \ldots, b_{m-1}, 0, \ldots) \oplus V_m(B) = (c_0, \ldots, c_{m-1}, 0, \ldots) \oplus V_m(B)$. Dann gibt es $(0, \ldots, 0, b_m, b_{m+1}, \ldots) \in V_m(B)$, sodass

$$\begin{aligned} & (b_0, \ldots, b_{m-1}, 0, \ldots) \oplus (0, \ldots, 0, b_m, b_{m+1}) \\ \overset{\text{i)}}{=} \; & (b_0, \ldots, b_{m-1}, b_m, b_{m+1}, \ldots) = (c_0, \ldots, c_{m-1}, 0, \ldots). \end{aligned}$$

Somit ist $b_i = c_i$ für alle $i < m$. Die Abbildung ist also injektiv. □

Korollar 3.13
Für einen kommutativen Ring B mit Eins gilt $B \cong W_1(B)$.

Beweis: Mit 3.12 ii) und 3.8 ii) induziert $\Phi_0 : W(B) \to B$ einen Ringisomorphismus $W_1(B) \to B$. □

Lemma 3.14
Die Abbildung $\tau : B \to W(B), \quad b \mapsto (b, 0, 0, \ldots)$ *ist multiplikativ.*

Beweis: Für das erste Folgenglied des Produktes

$$(b, 0, \ldots) \odot (c, 0, \ldots) = (P_0(b, c), P_1(b, 0, c, 0), \ldots),$$

gilt $P_0(b, c) = bc$. Es ist also zu zeigen, dass für alle $n \geqslant 1$ alle übrigen Folgenglieder gleich 0 sind, also

$$\tilde{P}_n(X_0, Y_0) := P_n(X_0, 0, \ldots, 0, Y_0, 0, \ldots, 0) = 0.$$

Es gilt

$$\begin{aligned} X_0^{p^n} Y_0^{p^n} &= \Phi_n(X_0, 0, \ldots, 0)\Phi_n(Y_0, 0, \ldots, 0) \\ &= \Phi_n(\tilde{P}_0(X_0, Y_0), \tilde{P}_1(X_0, Y_0), \ldots, \tilde{P}_n(X_0, Y_0)) \\ &= \sum_{i=0}^{n} p^i(\tilde{P}_i(X_0, Y_0))^{p^{n-i}} = (\tilde{P}_0(X_0, Y_0))^{p^n} + \sum_{i=1}^{n} p^i(\tilde{P}(X_0, Y_0))^{p^{n-i}} \\ &= X_0^{p^n} Y_0^{p^n} + \sum_{i=1}^{n} p^i(\tilde{P}(X_0, Y_0))^{p^{n-i}}. \end{aligned}$$

Somit ist $\sum_{i=1}^{n} p^i(\tilde{P}(X_0, Y_0))^{p^{n-i}} = 0$. Nach 3.6 iv) gilt $\tilde{P}_1(X_0, Y_0) = 0$.
Wegen $\sum_{i=0}^{n} p^i(\tilde{P}_n(X_0, Y_0))^{p^{n-i}} = 0$ folgt nach Induktion $\tilde{P}_n(X_0, Y_0) = 0$. □

Das Element $\tau(b)$ heißt **Teichmüllerrepräsentant von b** $\in B \cong W(B)/V_1(B)$. Er wird auch mit $\tau(b) = [b]$ bezeichnet.

Lemma 3.15
$\Big((W(B)/V_i(B))_{i \geqslant 0}, (\alpha_{ji})_{\substack{i,j \in I \\ i \leqslant j}}\Big)$ *mit*

$$\begin{aligned} \alpha_{ji} : \quad W(B)/V_i(B) &\to W(B)/V_j(B) \\ b \oplus V_i(B) &\mapsto b \oplus V_j(B) \end{aligned}$$

mit $j \leqslant i$ *ist ein projektives System.*

Beweis: Es gilt $V_j(B) \supseteq V_i(B)$ für $j \leqslant i$. Damit ist α_{ji} ein wohldefinierter Ringhomomorphismus. □

Lemma 3.16
Die Zuordnung

$$\begin{aligned} W(B) &\to \varprojlim_{m \in \mathbb{N}} W_m(B) \\ b &\mapsto (b \oplus V_m(B))_{m \geqslant 0} \end{aligned}$$

ist ein Ringisomorphismus.

Beweis: Da $\alpha_{ji}(b \oplus V_i(B)) = b \oplus V_j(B)$ ist für $i \geqslant j$, gilt $(b \oplus V_m(B))_{m \geqslant 0} \in \varprojlim_{m \in \mathbb{N}} W_m(B)$. Aufgrund der komponentenweise Addition und Multiplikation in $\varprojlim_{m \in \mathbb{N}} W_m(B)$ ist die Abbildung offensichtlich ein Ringhomomorphismus.
Der Kern des Homomorphismus ist $\bigcap_{m \geqslant 0} V_m(B) = 0$.

Sei $(x_n)_{n\geqslant 0} \in \varprojlim_{m\in\mathbb{N}} W_m(B)$ und $\tilde{x}_n = (x_{0,n}, \ldots, x_{n,n}, 0, \ldots) \in W(B)$ mit $\tilde{x}_n \oplus V_n(B) = x_n$ für alle $n \in \mathbb{N}$. Nach Definition des projektiven Limes und da nach 3.12 ii) Elemente in $W_m(B)$ eindeutig durch die ersten $m-1$ Folgenglieder des Repräsentanten bestimmt sind gilt für alle $m \leqslant n$ die Gleichheit $x_{i,n} = x_{i,m}$ für alle $i \leqslant m$. Bezeichne also $x_{i,n}$ mit y_i für alle $n \in \mathbb{N}$. Offenbar ist das Bild von $(y_n)_{n\geqslant 0}$ unter dem obigen Homomorphismus $(x_n)_{n\geqslant 0}$. □

Lemma 3.17
Für alle $k \geqslant 1$ ist $V_1(B)^k = p^{k-1}V_1(B)$.

Beweis: Die Behauptung wird mit vollständiger Induktion nach k gezeigt. Für $k=1$ gilt die Behauptung offensichtlich. Seien $a_1, \ldots, a_k \in B$. Dann gibt es nach Induktionsvoraussetzung ein $a \in W(B)$ mit

$$\begin{aligned} V(a_1) \odot \ldots \odot V(a_k) &= p^{k-2}V(a) \odot V(a_k) = V(p^{k-2}a) \odot V(a_k) \\ &\overset{3.11}{=} V(p^{k-2}a \odot F \circ V(a_k)) \overset{3.11}{=} V(p^{k-1}a \odot a_k) \\ &= p^{k-1}V(a \odot a_k). \end{aligned}$$

□

Theorem 3.18
Sei $char(B) = p$.

i) Ist $b = (b_n)_{n\geqslant 0} \in W(B)$, so ist $F(b) = (b_n^p)_{n\geqslant 0}$ und $pb = V \circ F(b) = (0, b_0^p, b_1^p, \ldots)$.

ii) Für alle $m, n \geqslant 0$ ist $V_m(B) \odot V_n(B) \subseteq V_{m+n}(B)$.

iii) Für alle $k \geqslant 1$ ist $p^kW(B) \subseteq V_1(B)^k \subseteq p^{k-1}W(B)$.

iv) Die Abbildung

$$\begin{aligned} W(B) &\to \varprojlim_{k\in\mathbb{N}} W(B)/p^kW(B) \\ b &\mapsto (b \oplus p^kW(B))_{k\geqslant 0} \end{aligned}$$

ist ein Ringisomorphismus.

Beweis: i) Nach 3.6 iii) erfüllte die n-te Komponente von $F(b)$ die Kongruenz $F_n(b) \equiv b_n^p \mod pB$. Da $char(B) = p$ ist, gilt $F(b) = (b_n^p)_{n\geqslant 0}$. Die Aussage 3.11 iii) impliziert $pb = F \circ V(b) =$
$F(0, b_0, b_1, \ldots) = (0, b_0^p, b_1^p, \ldots) = V(b_0^p, b_1^p, \ldots) = V \circ F(b)$.
ii) Nach 3.11 iv) gilt $V^m(a) \odot V^n(b) = V^m(a \odot F^m \circ V^n(b))$. Aus i) folgt $F^n \circ V^m = V^m \circ F^n$. Insgesamt ergibt sich

$$\begin{aligned} V^m(a) \odot V^n(b) &= V^m(a \odot F^m \circ V^n(b)) = V^m(a \odot V^n \circ F^m(b)) \\ &= V^m \circ V^n(F^m(b) \odot F^n(a)) \\ &= V^{m+n}(F^m(b) \odot F^n(a)) \in V^{m+n}(B). \end{aligned}$$

iii) In i) wurde gezeigt, dass $pW(B) = V \circ F((W(B)) \subseteq V_1(B)$ ist. Damit ist $p^kW(B) \subseteq V_1(B)^k$. Mit 3.17 folgt nun $p^kW(B) \subseteq V_1(B)^k = p^{k-1}V_1(B) \subseteq p^{k-1}W(B)$.

iv) Nach i) ist

$$p^k W(B) = \{p^k b : b \in W(B)\} = \{(\underbrace{0, \ldots, 0}_{k-\text{mal}}, b_0^{p^k}, b_1^{p^k}, \ldots) : (b_0, b_1, \ldots) \in W(B)\},$$

und daher ist $\bigcap_{k \geqslant 0} p^k W(B) = 0$. Das ist aber genau der Kern des Homomorphismus.
Sei $(b^{(k)} \oplus p^k W(B))_{k \geqslant 0} \in \varprojlim_{k \in \mathbb{N}} W(B)/p^k W(B)$. Für alle $k \geqslant 1$ gilt

$$p^k W(B) \overset{\text{iii)}}{\subseteq} V_1(B)^k = V_1(B) \odot .. \odot V_1(B) \overset{\text{ii)}}{\subseteq} V_k(B)$$

und somit ist $W(B)/p^k W(B) \to W(B)/V_k(B), \quad a \oplus p^k W(B) \mapsto a \oplus V_k(B)$ eine wohldefinierte Abbildung und folglich auch

$$\begin{array}{ccc} \varprojlim_{k \in \mathbb{N}} W(B)/p^k W(B) & \to & \varprojlim_{k \in \mathbb{N}} W_k(B) \\ (a^{(k)} \oplus p^k W(B))_{k \geqslant 0} & \mapsto & (a^{(k)} \oplus V_k)_{k \geqslant 0}. \end{array}$$

Da $W(B) \to \varprojlim_{k \in \mathbb{N}} W_k(B)$ wie in 3.16 ein Isomorphismus ist, gibt es ein $b \in W(B)$ mit $(b \oplus V_k(B))_{k \geqslant 0} = (b^{(k)} \oplus V_k(B))_{k \geqslant 0}$, also gilt für alle $k \geqslant 1$ die Kongruenz $b \equiv b^{(k)} \mod V_k(B)$.
In dem Ring $W(B)/V_j(B) \oplus p^k W(B)$ mit $j \geqslant k$ gilt

$$b \oplus V_j(B) \oplus p^k W(B) \quad = \quad b^{(j)} \oplus V_j(B) \oplus p^k W(B) = b^{(k)} \oplus V_j(B) \oplus p^k W(B)$$

Damit ist also $b \equiv b^{(k)} \mod \bigcap_{j \geqslant k}(V_j(B) \oplus p^k W(B))$ für alle $k \geqslant 1$. Es genügt also zu zeigen, dass $\bigcap_{j \geqslant k}(V_j(B) \oplus p^k W(B)) = p^k W(B)$ ist, denn dann ist $b \mapsto (b^{(k)} \oplus p^k W(B))_{k \geqslant 0}$. Sei also $c = c^{(j)} \oplus (0, \ldots, 0, a_k^{(j)}, a_{k+1}^{(j)}, \ldots) \in \bigcap_{j \geqslant k}(V_j(B) \oplus p^k W(B))$ mit $c^{(j)} \in V_j(B)$ und $a_k^{(j)} \in B^{p^k}$ für alle $j \geqslant k$. Da $j \geqslant k$, gilt $c \in V_j(B) \oplus p^k W(B) \subseteq V_k(B)$, d.h. $c = (0, \ldots, 0, c_k, c_{k+1}, \ldots)$. Für alle $n \in \{k, \ldots, j-1\}$ gilt $c_n = a_n^{(j)} \in B^{p^k}$ nach 3.12 i) . Da j beliebig gewählt werden kann, gilt für alle $n \geqslant k$, dass $c_n \in B^{p^k}$ ist. Mit i) folgt $c \in p^k W(B)$. □

Proposition 3.19
Sei $char(B) = p$ und sei B perfekt.

i) Ist $b = (b_n)_{n \geqslant 0} \in W(B)$ und $m \geqslant 1$, so gilt $b \oplus V_m(B) = \sum_{i=0}^{m-1} p^i [b_i^{p^{-i}}] \oplus V_m(B)$.

ii) Für alle $m \geqslant 0$ gilt $V_m(B) = p^m W(B) = V_1(B)^m$.

Beweis: i) Es gilt

$$\begin{aligned} \textstyle\sum_{i=0}^{m-1} p^i [b_i^{p^{-i}}] &\underset{\text{i)}}{\overset{3.18}{=}} (b_0, 0, \ldots) \oplus (0, b_1, 0, \ldots) \oplus .. \oplus (0, \ldots, 0, b_{m-1}, 0, \ldots) \\ &\underset{i)}{\overset{3.12}{=}} (b_0, b_1, \ldots, b_{m-1}, 0, \ldots) \underset{ii)}{\overset{3.12}{\equiv}} b \mod V_m(B). \end{aligned}$$

ii) Nach 3.18 i) ist die Abbildung $F : W(B) \to W(B), \quad (b_n)_{n \geqslant 0} \mapsto (b_n^p)_{n \geqslant 0}$ ein Automorphismus, da $B \to B, \quad b \mapsto b^p$ bijektiv ist. Wieder mit 3.18 i) folgt

$$p^m W(B) = (V \circ F)^m (W(B)) = V^m \circ F^m (W(B)) = V^m (W(B)) = V_m(B).$$

Damit ist $(V_1(B))^m = (pW(B))^m = p^m W(B)$. □

Lemma 3.20
Sei $char(B) = p$.

i) Die Folge $(\sum_{i=0}^{n}(\ominus 1)^i \odot c^i)_{n\geqslant 0}$ mit $c \in V_1(B)$ ist eine Cauchyfolge in $W(B)$ bzgl. der Topologie, wie in 1.5.3 mit $W(B) = V_0(B) \supseteq V_1(B) \supseteq ..$ als entsprechende Kette von $W(B)-$Moduln.

ii) Für $a \in V_1(b)$ ist $(a^n)_{n\geqslant 0}$ eine Nullfolge in $W(B)$, bzgl. der oben beschriebenen Toplogie.

iii) Für $c \in V_1(B)$ ist $\sum_{i=0}^{\infty}(\ominus c)^i$ inverses Element von $1 \oplus c$ in $W(B)$.

Beweis: i) Für $j \in \mathbb{N}$ sei $N_j := j$. Dann gilt für alle $m \geqslant n \geqslant N_j$:

$$\sum_{i=0}^{m}(\ominus c)^i \ominus \sum_{i=0}^{n}(\ominus c)^i = (\ominus c)^m \oplus .. \oplus (\ominus c)^{n+1} \in V(B)^{N_j} = V(B)^j \underset{ii)}{\overset{3.19}{=}} V_j(B),$$

da für $s \geqslant j$ die Inklusion $V(B)^s = V_s(B) \subseteq V_j(B) = V(B)^j$ gilt.
ii) Sei $j \in \mathbb{N}$ und $N_j := j$. Dann gilt für alle $n \geqslant N_j$, dass $a^n \in V(B)^n = V_n(B) \subseteq V_{N_j}(B) = V(B)^{N_j}$ ist. Wegen $\bigcap_{l\in\mathbb{N}} V_l(B) = \{0\}$ folgt die Behauptung.
iii) $W(B)$ ist nach 1.5.7 vollständig, da die Abbildung
$W(B) \to \lim_{\underset{m\in\mathbb{N}}{\longleftarrow}} W_m(B), \quad b \mapsto (b \oplus V_m)_{m\geqslant 0}$ wegen 3.16 surjektiv ist. Damit konvergiert die Folge $(\sum_{i=0}^{n}(\ominus 1)^i \odot c^i)_{n\geqslant 0}$. Darüberhinaus ist

$$(1 \oplus c) \odot \sum_{i=0}^{n}(\ominus c)^i = 1 \ominus (\ominus c)^{n+1}$$

Da die Folge $((\ominus c)^n)_{n\geqslant 0}$ nach ii) eine Nullfolge ist, folgt $(1 \oplus c) \odot \sum_{i=0}^{\infty}(\ominus c)^i = 1$. □

Theorem 3.21
Sei B ein Körper mit $char(B) = p$.

i) $W(B)$ ist ein Integritätsbereich mit genau einem maximalen Ideal $V_1(B)$.

ii) Die Zuordnung

$$\begin{array}{rcl} W(B) & \to & \lim\limits_{\underset{k\in\mathbb{N}}{\longleftarrow}} W(B)/V_1(B)^k \\ b & \mapsto & (b \oplus V_1(B)^k)_{k\geqslant 0} \end{array}$$

ist ein Ringisomorphismus.

iii) Ist B perfekt, so ist $W(B)$ ein vollständiger, diskreter Bewertungsring, wobei p ein uniformisierendes Element ist. Für $(b_n)_{n\geqslant 0}$ gilt die Darstellung $(b_n)_{n\geqslant 0} = \sum_{n=0}^{\infty} p^n[b_n^{p^{-n}}]$.

Beweis: Es gilt $W(B)/V_1(B) \cong B$. Damit ist $V_1(B)$ ein maximales Ideal.
Sei $b = (b_n)_{n\geqslant 0} \in W(B)\backslash V_1(B)$. Dann ist $b_0 \neq 0$. Für $a := [b_0^{-1}] = (b_0^{-1}, 0, \ldots)$ ist $a \odot b = (b_0 b_0^{-1}, c_1, c_2, \ldots) = 1 \oplus c$ mit $c = (0, c_1, c_2, \ldots) \in V_1(B)$ nach 3.6 iv) und 3.12 i). Nach 3.20 iii) ist $1 \oplus c \in W(B)^\times$. Da a ebenfalls eine Einheit ist, ist auch b eine Einheit. Dies impliziert, dass $V_1(B)$ das einzige maximale Ideal ist.
Seien $a = (0, \ldots, 0, a_i, a_{i+1}, \ldots), b = (0, \ldots, 0, b_j, b_{j+1}, \ldots) \in W(B)$ mit $a_i \neq 0 \neq b_j$. Dann ist

$$a \odot b = V^i((a_i, \ldots)) \odot V^j((b_j, \ldots)).$$

Im Beweis von 3.18 ii) wurde die Gleichheit $V^i((a_i,\ldots))\odot V^j((b_j,\ldots)) = V^{i+j}(F^j(a_i,\ldots)\odot F^i(b_j,\ldots))$ gezeigt. Damit gilt insgesamt

$$\begin{aligned} a\odot b &= V^i((a_i,\ldots))\odot V^j((b_j,\ldots)) = V^{i+j}(F^j(a_i,\ldots)\odot F^i(b_j,\ldots)) \\ &\overset{3.18}{\underset{\text{i)}}{=}} V^{i+j}((a_i^{p^j},\ldots)\odot(b_j^{p^i},\ldots)) = V^{i+j}((a_i^{p^j}b_j^{p^i},\ldots)) = (0,\ldots,0,a_i^{p^j}b_j^{p^i},\ldots)\neq 0. \end{aligned}$$

Somit ist $W(B)$ ein Integritätsbereich.
ii) Das folgende Diagramm

$$\begin{tikzcd}
 & \varprojlim_{k\in\mathbb{N}} W(B)/p^{k-1}W(B) \\
W(B) \arrow[ur, "\lambda_1"] \arrow[r, "\lambda_2"] \arrow[dr, "\lambda_3"'] & \varprojlim_{k\in\mathbb{N}} W(B)/V_1(B)^k \arrow[u, "\lambda_5"'] \\
 & \varprojlim_{k\in\mathbb{N}} W(B)/p^kW(B), \arrow[u, "\lambda_4"']
\end{tikzcd}$$

ist kommutativ, wobei $\lambda_1,\lambda_2,\lambda_3$ wie in 1.5.6 sind und λ_4 und λ_5 wegen 3.18 iii) durch $p^kW(B)\subseteq V_1(B)^k\subseteq p^{k-1}W(B)$ induziert werden. Nach 3.18 iv) sind λ_1 und λ_3 bijektiv. Damit ist $\lambda_5\circ\lambda_4$ bijektiv und somit ist λ_5 surjektiv. Sei $(w_k\oplus V_1(B)^k)_{k\geqslant 0}\in\ker(\lambda_5)$. Dann ist $0=(w_k\oplus p^{k-1}W(B))_{k\geqslant 0}$. Dies impliziert $w_k\in p^{k-1}W(B)$ für alle $k\geqslant 0$. Nach Definition des projektiven Limes und da $w_{k+1}\in p^kW(B)\subseteq V_1(B)^k$ nach 3.18 ii) ist, gilt für alle $k\geqslant 0$ die Gleichheit $w_k\oplus V_1(B)^k = w_{k+1}\oplus V_1(B)^k = V_1(B)^k$. Damit ist $w=0$ und somit ist λ_5 injektiv. Aus der Bijektivität von λ_5 folgt die Bijektivität von λ_2.
iii) Sei B ein perfekter Ring. Dann gilt nach 3.19 ii), dass $V_1(B)=pW(B)$ ist. Dies ist nicht das Nullideal, da $p1_{W(B)}\overset{3.18}{=}(0,1,0,\ldots)\neq 0$ ist. In i) wurde gezeigt, dass dies das einzige maximale Ideal ist. Da λ_2 injektiv ist, folgt mit 1.5.7 i), dass $\bigcap_{k\geqslant 0}V_1(B)^k=0$ ist. Nach 1.1.3 ist damit $W(B)$ ein Hauptidealring und somit ein diskreter Bewertungsring, wobei p uniformisierendes Element ist.
Nach 3.19 i) gilt für $b=(b_n)_{n\geqslant 0}$ und $m\geqslant 1$, dass $b\oplus V_m = \sum_{i=0}^{m-1}[b_i^{p^{-i}}]\oplus V_m(B)$. Damit ist $b=\sum_{i=0}^{\infty}p^i[b_i^{p^{-i}}]$. □

Der obige Beweis von i) zeigt allgemein: Ist B ein Integritätsbereich der Charakteristik p, so ist auch $W(B)$ ein Integritätsbereich.

Lemma 3.22
Sei B ein Körper mit $char(B)=p$. Dann ist $char(Quot(W(B)))=0$.

Beweis: Angenommen es gibt eine Primzahl $l\in\mathbb{N}$ mit $l\odot W(B)=0$. Dann ist $lB=0$, da $B\cong W(B)/V_1(B)$ ist. Damit ist $l=p$, aber es gilt $l\odot 1_{W(B)}=p\odot 1_{W(B)}=(0,1,0,\ldots)\neq 0$. Dies steht im Widerspruch zur Annahme. □

Theorem 3.23
Sei R ein vollständiger, diskreter Bewertungsring mit dem maximalen Ideal $\mathfrak{m}$ und perfektem Restklassenkörper k der Charakteristik p.

i) Es gibt einen eindeutigen Ringhomomorphismus $\gamma : W(k) \to R$, sodass $\gamma(x) \equiv x_0 \mod \mathfrak{m}$ für alle $x = (x_n)_{n\geqslant 0} \in W(k)$ ist.

ii) γ ist stetig und es gilt $\gamma((x_n)_{n\geqslant 0}) = \sum_{n=0}^{\infty} p^n s(x_n^{-p^n})$ mit $s : k \to R$ wie in 1.2.14.

iii) Ist $p1_R \neq 0$, so ist γ injektiv.

iv) Ist $pR = \mathfrak{m}$, so ist γ bijektiv.

Beweis: i) und ii) Zunächst wird die Existenz einer solchen Abbildung γ gezeigt.
Sei $\alpha : R \to R/\mathfrak{m},\ \ r \mapsto r + \mathfrak{m}$. Dann ist $W(\alpha) : W(R) \to W(k)$ ein surjektiver Ringhomomorphismus. Sei $b := (b_n)_{n\geqslant 0} \in W(R)$. Das Element b ist genau dann in $\ker(W(\alpha))$, wenn alle Folgenglieder b_n in $\ker(\alpha) = \mathfrak{m}$ liegen. Damit ist $\Phi_m(b_0, \ldots , b_m) = b_0^{p^m} + pb_1^{p m-1} + p^2 b_2^{p^{m-2}} + \ldots + p^m b_m \in \mathfrak{m}^{m+1}$, da $p \in \mathfrak{m}$ ist. Für $\alpha_{m+1} : R \to R/\mathfrak{m}^{m+1},\ \ r \mapsto r + \mathfrak{m}^{m+1}$ ist $\alpha_{m+1} \circ \Phi_m((b_n)_{n\geqslant 0}) = 0$.
Dies impliziert die Inklusion $\ker(W(\alpha)) \subseteq \ker(\alpha_{m+1} \circ \Phi_m)$. Nach dem Homomorphiesatz gibt es einen eindeutigen Homomorphismus $\gamma'_m : W(R)/\ker(W(\alpha)) \to R/\mathfrak{m}^{m+1}$, sodass

$$\begin{tikzcd}
W(R) \arrow[r, "\Phi_m"] \arrow[d, "q_{W(R),\ker(W(\alpha))}"'] & R \arrow[r, "\alpha_{m+1}"] & R/\mathfrak{m}^{m+1} \\
W(R)/\ker(W(\alpha)) \arrow[urr, "\gamma'_m"'] & &
\end{tikzcd}$$

kommutiert.
Da $W(\alpha) : W(R) \to W(k)$ ein surjektiver Ringhomomorphismus ist, gibt es einen Isomorphismus $\delta : W(R)/ker(W(\alpha)) \to Im(W(\alpha)) = W(k)$. Dieser ist gegeben durch $(b_n)_{n\geqslant 0} \oplus \ker(W(\alpha)) \mapsto (b_n + \mathfrak{m})_{n\geqslant 0}$. Darüberhinaus ist

$$\begin{aligned}
\delta \circ q_{W(R),\ker(W(\alpha))}((b_n)_{n\geqslant 0}) &= \delta((b_n)_{n\geqslant 0} \oplus \ker(W(\alpha))) = (b_n + \mathfrak{m})_{n\geqslant 0} \\
&= (\alpha(b_n))_{n\geqslant 0} = W(\alpha)((b_n)_{n\geqslant 0}))
\end{aligned}$$

Es gibt also einen eindeutigen Homomorphismus $\gamma_m : W(k) \to R/\mathfrak{m}^{m+1}$, sodass das Diagramm

$$\begin{tikzcd}
W(R) \arrow[r, "\Phi_m"] \arrow[d, "q_{W(R),\ker(W(\alpha))}"] \arrow[dd, bend right, "W(\alpha)"'] & R \arrow[r, "\alpha_{m+1}"] & R/\mathfrak{m}^{m+1} \\
W(R)/\ker(W(\alpha)) \arrow[urr, "\gamma'_m"'] \arrow[d, "\delta"'] & & \\
W(k) \arrow[uurr, "\gamma_m"'] & &
\end{tikzcd} \tag{15}$$

kommutiert.
Da $\Phi_R \circ F_{W(R)} = f_R \circ \Phi_R$ ist, folgt $\Phi_m \circ F_{W(R)}(b) = \Phi_{m+1}(b)$.

Für $\alpha_{n,m} : R/\mathfrak{m}^m \to R/\mathfrak{m}^n, \quad r + \mathfrak{m}^m \mapsto r + \mathfrak{m}^n$ mit $m \geqslant n$ ist

$$\begin{aligned}
\gamma_m \circ F_{W(k)} \circ W(\alpha) &\overset{3.10}{=} \gamma_m \circ W(\alpha) \circ F_{W(R)} = \alpha_{m+1} \circ \Phi_m \circ F_{W(R)} \\
&= \alpha_{m+1} \circ \Phi_{m+1} = \alpha_{m+1,m+2} \circ \alpha_{m+2} \circ \Phi_{m+1} \\
&= \alpha_{m+1,m+2} \circ \gamma_{m+1} \circ W(\alpha)
\end{aligned}$$

Da $W(\alpha)$ surjektiv ist, gilt $\gamma_m \circ F_{W(k)} = \alpha_{m+1,m+2} \circ \gamma_{m+1}$.
Der Frobenius $F_{W(k)} : W(k) \to W(k), \quad (b_n)_{n \geqslant 0} \overset{3.18i)}{\longmapsto} (b_n^p)_{n \geqslant 0}$ bijektiv, da k perfekt ist. Damit ergibt sich

$$\alpha_{m+1,m+2} \circ \gamma_{m+1} \circ F_{W(k)}^{-(m+1)} = \gamma_m \circ F_{W(k)}^{-m}.$$

Also erfüllen die Abbildungen $\gamma_n \circ F_{W(k)}^{-n}$ die Kommutativität des Diagramms

$$\begin{tikzcd}
W(k) \arrow[r, "\gamma_{m-1} \circ F_{W(k)}^{-(m-1)}"] \arrow[dr, "\gamma_{n-1} \circ F_{W(k)}^{-(n-1)}"'] & R/\mathfrak{m}^m \arrow[d, "\alpha_{mn}"] \\
& R/\mathfrak{m}^n
\end{tikzcd}$$

für alle $n, m \in \mathbb{N}$ mit $m \geqslant n$. Aufgrund der universellen Eigenschaft des projektiven Limes in 1.5.1 gibt es einen eindeutigen Homomorphismus $\tilde{\gamma} : W(k) \to \varprojlim_{m \in \mathbb{N}} R/\mathfrak{m}^m$, sodass das Diagramm

$$\begin{tikzcd}
W(k) \arrow[r, "\tilde{\gamma}"] \arrow[rr, bend left, "\gamma"] \arrow[dr, "\gamma_{n-1} \circ F_{W(k)}^{-(n-1)}"'] & \varprojlim_{m \in \mathbb{N}} R/\mathfrak{m}^m \arrow[r, "1.5.8"] \arrow[d, "pr_n"] & R \arrow[d, "\alpha_n"] \\
& R/\mathfrak{m}^n \arrow[r, "id"] & R/\mathfrak{m}^n
\end{tikzcd}$$

für alle $n \in \mathbb{N}$ kommutiert. Dann ist

$$\begin{aligned}
\alpha \circ \gamma \circ W(\alpha) &= \alpha_1 \circ \gamma \circ W(\alpha) = \gamma_0 \circ F_{W(k)}^0 \circ W(\alpha) = \gamma_0 \circ W(\alpha) \\
&\overset{(15)}{=} \alpha_1 \circ \Phi_0 = \Phi_0 \circ W(\alpha).
\end{aligned}$$

Da $W(\alpha)$ surjektiv ist, ist $\alpha \circ \gamma = \Phi_0$. Für $x = (x_n)_{n \geqslant 0}$ folgt

$$x_0 = \Phi_0(x) = \alpha \circ \gamma(x) = \gamma(x) + \mathfrak{m}.$$

Sei $\overline{\gamma} : W(k) \to R$ ein Ringhomomorphismus mit $\alpha \circ \overline{\gamma} = \Phi_0$. Da $pW(k) \subseteq \ker(\Phi_0)$ ist, gilt $\overline{\gamma}(pW(k)) \subseteq \ker(\alpha) = \mathfrak{m}$. Mit 1.2.15 folgt, dass $\overline{\gamma}$ stetig ist, da $\overline{\gamma}(p^i W(k)) \subseteq \mathfrak{m}^i$ für alle $i \geqslant 0$ ist. Wegen der Stetigkeit von $\overline{\gamma}$ gilt für alle $x \in W(k)$:

$$\overline{\gamma}(x) \underset{iii)}{\overset{3.21}{=}} \overline{\gamma}\Big(\sum_{n=0}^{\infty} p^n [x_n^{p^{-n}}]\Big) = \sum_{n=0}^{\infty} p^n \overline{\gamma}([x_n^{p^{-n}}]).$$

Da $\alpha \circ \overline{\gamma} \circ \tau = \Phi_0 \circ \tau = id_k$ und $\overline{\gamma} \circ \tau$ multiplikativ ist, ist $s = \overline{\gamma} \circ \tau$ nach 1.2.14 eindeutig und damit auch $\overline{\gamma}$ mit $\overline{\gamma}(x) = \sum_{n=0}^{\infty} p^n s(x_n^{p^{-n}})$.
iii) Sei $p1_R \neq 0$ und π ein uniformisierendes Element. Dann ist $0 \neq p \in \mathfrak{m} = \pi R$. Damit gibt es ein

$e \in \mathbb{N}$ mit $\nu(p) = e$, wobei ν die diskrete Bewertung von R ist. Für $m \in e\mathbb{N}$ wird $\pi^m = p^{\frac{m}{e}}$ gesetzt. Sei $(x_n)_{n\geqslant 0} \in \ker(\gamma)$. Dann ist

$$0 = \gamma((x_n)_{n\geqslant 0}) = \sum_{n=0}^{\infty} p^n s(x_n^{p^{-n}}) = \sum_{n=0}^{\infty} \pi^{ne} s(x_n^{p^{-n}})$$

Da nach 1.3.7 diese Darstellung eindeutig ist, ist $s(x_n^{p^{-n}}) = 0$ für alle $n \geqslant 0$. Mit 1.2.14 folgt $x_n^{p^{-n}} = 0$, also $x_n = 0$ für alle $n \geqslant 0$.
iv) Sei $pR = \mathfrak{m}$ und $x \in R$. Dann gibt es nach 1.3.7 eine eindeutige Darstellung $x = \sum_{n=0}^{\infty} p^n s(y_n)$, mit $y_n \in k$ und s wie in 1.2.14, da $\{s(z) : z \in k\} \subseteq R$ ein vollständiges Repräsentantensystem von $k = R/\mathfrak{m}$ ist, welches die 0 enthält. Dies impliziert die Surkejtivität von γ. $\square$

Beispiel 3.24
Die Abbildung $W(\mathbb{F}_p) \to \mathbb{Z}_p, \quad (x_n)_{n\geqslant 0} \mapsto \sum_{n=0}^{\infty} p^n s(x_n)$ ist ein Ringisomorphismus. Der Ring $\mathbb{Z}_p$ ist ein diskreter Bewertungsring mit seinem maximalen Ideal $p\mathbb{Z}_p$. Für den Restklassenkörper gilt $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$. Mit 3.23 folgt nun, dass die Abbildung ein Ringisomophismus ist.

4 Konstruktion eines perfektoiden Körpers der Charakteristik 0

Im 3. Kapitel wurde ein perfektoider Körper der Charakteristik 0 mithilfe des Tilts zu einem Körper der Charakteristik p. Im Folgenden wird aus einem perfektoiden Körper F der Charakteristik p ein perfektoider Körper der Charakteristik 0 konstruiert, indem aus dem Ring der Wittvektoren mit Koeffizienten des zugrundeliegenden Bewertungrings von F ein bestimmtes Hauptideal herausfaktorisiert wird. Es wird sich zeigen, dass der Quotientenkörper dieses Rings ein perfektoider Körper der Charakteristik 0 ist. Basis für die letzten beiden Kapitel dieser Arbeit ist [7].
Sei in diesem Kapitel stets $(F, |\cdot|_F)$ ein perfektoider Körper mit $char(F) = p$. Damit ist $\mathcal{O}_F$ ein perfekter Ring der Charakteristik p.

Lemma 4.1 *i) $W(\mathcal{O}_F)$ ist ein lokaler Ring mit maximalem Ideal $\mathfrak{m} := \{(x_n)_{n\geqslant 0} \in W(\mathcal{O}_F) : |x_0|_F < 1\}$.*

ii) $W(\mathcal{O}_F)$ ist p-adisch vollständig, und es gilt $\bigcap_{i\in\mathbb{N}} p^i W(\mathcal{O}_F) = 0$. Jedes Element $x \in W(\mathcal{O}_F)$ lässt sich als $x = \sum_{n=0}^{\infty} p^n [x_n^{p^{-n}}]$ darstellen.

Beweis: i) Seien $x = (x_n)_{n\geqslant 0}$, $y = (y_n)_{n\geqslant 0} \in W(\mathcal{O}_F)$ mit $|x_0|_F, |y_0|_F < 1$. Dann gilt für $x \oplus y = (x_0 + y_0, \ldots)$, dass $|x_0 + y_0|_F \leqslant \max\{|x_0|_F, |y_0|_F\} < 1$ ist. Also ist $x \oplus y \in \mathfrak{m}$. Sei nun $z = (z_n)_{n\geqslant 0} \in W(\mathcal{O}_F)$. Dann ist $z \odot x = (z_0 x_0, \ldots)$, also gilt $|z_0 x_0|_F = |z_0|_F |x_0|_F < 1$, da $|z_0|_F \leqslant 1$ und $|x_0|_F < 1$ sind. Damit ist $\mathfrak{m}$ ein Ideal.
Sei $z \in W(\mathcal{O}_F)\backslash\mathfrak{m}$. Da $|z_0|_F = 1$ ist, ist z_0 eine Einheit in $\mathcal{O}_F$. Es gilt $1 \ominus [z_0^{-1}] \odot z = (0, \ldots) \in V_1(\mathcal{O}_F)$, wobei wegen 3.19 ii) die Gleichheit $V_1(\mathcal{O}_F) = pW(\mathcal{O}_F)$ gilt. Nach 3.20 iii) ist $\sum_{i=0}^{\infty}(1 \ominus [z_0^{-1}] \odot z)^i$ das inverse Element von $1 \ominus (1 \ominus [z_0^{-1}] \odot z) = [z_0^{-1}] \odot z$. Damit ist $[z_0^{-1}] \odot z \in W(\mathcal{O}_F)^{\times}$. Im Beweis von 3.14 wurde die Gleichung $P_n((X, 0, \ldots 0, , Y, 0, \ldots, 0)) = 0$ für $n > 0$ gezeigt. Daher ist $[z_0]$ das inverse Element von $[z_0^{-1}]$. Damit ist $z \in W(\mathcal{O}_F)^{\times}$ und somit gilt $W(\mathcal{O}_F)\backslash\mathfrak{m} \subseteq W(\mathcal{O}_F)^{\times}$.
Sei nun $x \in W(\mathcal{O}_F)^{\times}$. Dann gibt es ein $y \in W(\mathcal{O}_F)^{\times}$ mit $x \odot y = (1, 0, \ldots)$ und somit $|x_0|_F = 1$. Also ist $W(\mathcal{O}_F)$ ist ein lokaler Ring.
ii) Da $char(\mathcal{O}_F) = p$ ist, folgt mit 3.18 iv), dass die Abbildung

$$\begin{array}{rcl} W(\mathcal{O}_F) & \to & \varprojlim_{i\in\mathbb{N}} W(\mathcal{O}_F)/p^i W(\mathcal{O}_F) \\ x & \mapsto & (x + p^i W(\mathcal{O}_F))_{i\geqslant 0}. \end{array}$$

ein Ringisomorphismus ist und somit nach 1.5.7 die Vollständigkeit von $W(\mathcal{O}_F)$ und die Gleichung $\bigcap_{i\in\mathbb{N}} p^i W(\mathcal{O}_F) = 0$. Nach 3.19 i) gilt für $x = (x_n)_{n\geqslant 0} \in W(\mathcal{O}_F)$ die Kongruenz $x \equiv \sum_{i=0}^{m-1} p^i [x_i^{p^{-i}}]$ mod $V_m(B)$ und nach 3.19 ii) ist $V_m(B) = p^m W(B)$. Damit ergibt sich für $m \to \infty$, dass $x = \sum_{i=0}^{\infty} p^i [x_i^{p^{-i}}]$ ist. □

Im Folgenden sei $|\cdot|$ wie folgt definiert:

$$\begin{array}{rrcl} |\cdot| \quad : & W(\mathcal{O}_F) & \to & [0,1] \subseteq \mathbb{R} \\ & \sum_{n=0}^{\infty} p^n [x_n] & \mapsto & \sup_{n\geqslant 0} |x_n|_F. \end{array}$$

Von nun an werden die Ringoperationen $\oplus$ und $\odot$ im Ring der Wittvektoren mit Koeffizienten des zugrunde liegenden Rings mit + und $\cdot$ abgekürzt.

Lemma 4.2

i) Es gilt genau dann $|x| = 0$*, wenn* $x = 0$ *ist.*

ii) Es gilt $|x+y| \leqslant \max\{|x|, |y|\}$ *für alle* $x, y \in W(\mathcal{O}_F)$.

iii) Es gilt $|1| = 1$.

iv) Für $x, y \in W(\mathcal{O}_F)$ *gilt* $|xy| \leqslant |x||y|$. *Ist* y *darüberhinaus eine Einheit in* $W(\mathcal{O}_F)$*, so gilt* $|xy| = |x||y| = |x|$.

v) Für $x \in W(\mathcal{O}_F)$ *und* $\overline{z} \in \mathcal{O}_F$ *gilt* $|x[\overline{z}]| = |x||[\overline{z}]| = |x||\overline{z}|_F$.

Beweis: i) Ist $\sup_{n \geqslant 0} |x_n|_F = 0$, dann ist $|x_n|_F = 0$ für alle $n \in \mathbb{N}$, also $x_n = 0$ für alle $n \in \mathbb{N}$ und somit $x = 0$.
ii) Seien $x = \sum_{n=0}^{\infty} p^n [x_n] = (x_0, x_1^p, x_2^{p^2}, \ldots)$ und $y = \sum_{n=0}^{\infty} p^n [y_n] = (y_0, y_1^p, y_2^{p^2}, \ldots)$. Nach 3.7 ist $S_n(X_0, X_1^p.., X_n^{p^n}, Y_0, \ldots, Y_n^{p^n})$ homogen vom Grad p^n in $\mathbb{Z}[X, Y]$. Daher gilt

$$|S_n(x_0, x_1^p, \ldots, x_n^{p^n}, y_0, \ldots, y_n^{p^n})|_F \leqslant \max\{|x_0|_F^{p^n}, \ldots, |x_n|_F^{p^n}, |y_0|_F^{p^n}, \ldots, |y_n|_F^{p^n}\}.$$

Damit ist $|S_n(x_0, x_1^p, \ldots, x_n^{p^n}, y_0, \ldots, y_n^{p^n})^{p^{-n}}|_F \leqslant \max_{i \in \{0,\ldots,n\}}\{|x_i|_F, |y_i|_F\}$. Es ergibt sich

$$\begin{aligned} |x+y| &= |\sum_{n \geqslant 0} p^n [S_n(x_0, x_1^p, \ldots, x_n^{p^n}, y_0, \ldots, y_n^{p^n})]^{p^{-n}}| \\ &= \sup_{n \geqslant 0} |S_n(x_0, x_1^p, \ldots, x_n^{p^n}, y_0, \ldots, y_n^{p^n})^{p^{-n}}|_F \\ &\leqslant \sup_{n \geqslant 0}\{\max_{i \in \{0,\ldots,n\}}\{|x_i|_F, |y_i|_F\}\} \\ &= \max\{\sup_{n \geqslant 0} |x_n|_F, \sup_{n \geqslant 0} |y_n|_F\} = \max\{|x|, |y|\}, \end{aligned}$$

wobei die vorletzte Gleichung wie folgt gezeigt wird:
Sei o.B.d.A $|x| = \sup_{n \geqslant 0} |x_n|_F \geqslant \sup_{n \geqslant 0} |y_n|_F$. Dann ist $\max\{\sup_{n \geqslant 0} |x_n|_F, \sup_{n \geqslant 0} |y_n|_F\} = |x|$ und $\sup_{n \geqslant 0}\{\max_{i \in \{0,\ldots,n\}}\{|x_i|_F, |y_i|_F\}\} \leqslant |x|$. Angenommen es gilt
$|x| > \sup_{n \geqslant 0}\{\max_{i \in \{0,\ldots,n\}}\{|x_i|_F, |y_i|_F\}\}$. Dann ist

$$\begin{aligned} |x| &> \sup_{n \geqslant 0}\{\max_{i \in \{0,\ldots,n\}}\{|x_i|_F, |y_i|_F\}\} \geqslant \sup_{n \geqslant 0}\{\max_{i \in \{0,\ldots,n\}} |x_i|_F\} \\ &\geqslant \sup_{n \geqslant 0} |x_n|_F = |x|. \end{aligned}$$

Also gilt Gleichheit.
iii) Es gilt $|1| = |(1, 0, \ldots)| = \sup\{|1|_F, |0|_F, \ldots\} = 1$.
iv) Seien $x = \sum_{n=0}^{\infty} p^n [x_n] = (x_0, x_1^p, x_2^{p^2}, \ldots)$ und $y = \sum_{n=0}^{\infty} p^n [y_n] = (y_0, y_1^p, y_2^{p^2}, \ldots)$. Nach 3.7 ist $P_n(x_0, x_1^p, \ldots, x_n^{p^n}, y_0, \ldots, y_n^{p^n})$ eine Summe von Monomen $x_0^{m_0}..x_n^{m_n} y_0^{m_0'}..y_n^{m_n'}$ mit $m_0 + \ldots + m_n = m_0' + \ldots + m_n' = p^n$. Seien $m, r \in \{0, \ldots, n\}$ mit $|x_m|_F = \max_{i=1,\ldots,n}\{|x_i|_F\}$ und $|y_r|_F = \max_{i=1,\ldots,n}\{|y_i|_F\}$. Dann gilt wegen der starken Dreiecksungleichung und der Ganzzahligkeit der Koeffizienten von P_n

$$\begin{aligned} |P_n(x_0, x_1^p, \ldots, x_n^{p^n}, y_0, \ldots, y_n^{p^n})|_F &\leqslant |x_m|_F^{p^n} |y_r|_F^{p^n} \\ &\leqslant (\sup_{n \geqslant 0} |x_n|_F)^{p^n} (\sup_{n \geqslant 0} |y_n|_F)^{p^n} = |x|^{p^n} |y|^{p^n} \end{aligned}$$

für alle $n \in \mathbb{N}$. Es gilt also

$$\begin{aligned} |xy| &= |\sum_{n \geqslant 0} p^n [P_n(x_0, x_1^p, \ldots, x_n^{p^n}, y_0, \ldots, y_n^{p^n})]^{p^{-n}}| \\ &= \sup_{n \geqslant 0} |P_n(x_0, x_1^p, \ldots, x_n^{p^n}, y_0, \ldots, y_n^{p^n})^{p^{-n}}|_F \leqslant |x||y|. \end{aligned}$$

Sei nun $y \in W(\mathcal{O}_F)^\times$. Dann gilt nach 4.1 i), dass $|y| = 1$ und $|y^{-1}| = 1$ ist und es folgt

$$|x| = |xyy^{-1}| \leqslant |xy||y^{-1}| = |xy| \leqslant |x||y| = |x|.$$

v) Die Behauptung folgt aus 3.14 und der Multiplikativität von $|\cdot|_F$. $\square$

Da wegen 3.19 ii) $\ker(\Phi_0) = V_1(B) = pW(B)$ ist und die Abbildung $\Phi_0 : W(B) \to B, \quad (b_n)_{n \geqslant 0} \mapsto b_0$ ein surjektiver Ringhomomorphismus ist, ist $W(\mathcal{O}_F)/pW(\mathcal{O}_F) \to \mathcal{O}_F, \quad (z_n)_{n \geqslant 0} + pW(\mathcal{O}_F) \mapsto z_0$ ein Ringisomorphismus.
Ist $z = (z_n)_{n \geqslant 0} \in W(\mathcal{O}_F)$, so schreiben wir im Folgenden $\overline{z} \in \mathcal{O}_F$ für seine Restklasse modulo p unter der Identifikation $W(\mathcal{O}_F)/pW(\mathcal{O}_F) \cong \mathcal{O}_F$. Es gilt also $z + pW(\mathcal{O}_F) = [\overline{z}] + pW(\mathcal{O}_F) = [z_0] + pW(\mathcal{O}_F)$.

Definition 4.3
Ein Element $z \in W(\mathcal{O}_F)$ heißt **primitiv**, falls $|\overline{z}|_F = \frac{1}{p}$ und $p^{-1}(z - [\overline{z}]) \in W(\mathcal{O}_F)^\times$ ist.

Beachte hierfür:
Für alle $z \in W(\mathcal{O}_F)$ ist $z - [\overline{z}] = (0, \ldots) \in pW(\mathcal{O}_F)$ und $W(\mathcal{O}_F)$ ist nach dem Beweis von 3.21 i) ein Integritätsbereich mit $p \overset{3.18i)}{=} (0, 1, 0 \ldots) \neq 0$.

Lemma 4.4
$z = (z_n)_{n \geqslant 0} \in W(\mathcal{O}_F)$ ist genau dann primitiv, wenn $|z_0|_F = \frac{1}{p}$ und $|z_1|_F = 1$.

Beweis: Sei z primitiv. Dann ist $|\overline{z}|_F = \frac{1}{p}$ und $p^{-1}(z - [\overline{z}]) \in W(\mathcal{O}_F)^\times$. Nach 3.6 iv) gilt

$$z - [\overline{z}] = z + [-\overline{z}] = (S_0(z_0, -z_0), S_1(z_0, z_1, -z_0, 0)) = (0, z_1, \ldots),$$

da $char(\mathcal{O}_F) = p$ gilt. Da $\mathcal{O}_F$ ein perfekter Ring der Charakteristik p ist, gibt es genau ein $x \in \mathcal{O}_F$ mit $x^p = z_1$. Es gilt $p = F \circ V(a_0, a_1, \ldots) = (0, a_0^p, \ldots)$. Damit ist $p^{-1}(z - [\overline{z}]) = (z_1^{-p}, \ldots)$. Angenommen $|z_1|_F \neq 1$. Dies impliziert, dass z_1 keine Einheit in $\mathcal{O}_F$ ist und somit $(z_1^{-p}, \ldots) =$
$p^{-1}(z - [\overline{z}]) \notin W(\mathcal{O}_F)^\times$ ist. Dies ist ein Widerspruch zur Voraussetzung.
Sei nun $|z_0|_F = \frac{1}{p}$ und $|z_1|_F = 1$. Dann ist $|\overline{z}|_F = \frac{1}{p}$ und $p^{-1}(z - [\overline{z}]) = (z_1^{-p}, \ldots)$. Nach 4.1 liegt $p^{-1}(z - [\overline{z}])$ in $W(\mathcal{O}_F) \backslash \mathfrak{m} = W(\mathcal{O}_F)^\times$ wegen $|z_1^{-p}|_F = |z_1|_F^{-p} = 1^{-p} = 1$. $\square$

Ein Element $x = \sum_{n \geqslant 0} p^n [x_n] \in W(\mathcal{O}_F)$ heißt **stabil**, wenn für alle $n \geqslant 0$ die Ungleichung $|x_n|_F \leqslant |x_0|_F$ gilt. Für stabile Elemente gilt also $|x| = |x_0|_F$.

Lemma 4.5
$x \in W(\mathcal{O}_F)$ ist genau dann stabil, wenn ein $u \in W(\mathcal{O}_F)^\times$ und ein $z_0 \in \mathcal{O}_F$ existieren mit $x = [z_0]u$.

Beweis: Sei $x = \sum_{n \geqslant 0} p^n [x_n] \in W(\mathcal{O}_F)$ stabil und $u_0 \in \mathcal{O}_F^\times$. Sei $z_0 := u_0^{-1}$ und $u_n := z_0^{-1} x_n$ für alle $n \geqslant 0$. Dann ist $u_n \in \mathcal{O}_F$ für alle $n \geqslant 0$, da $|z_0|_F = |u_0^{-1} x_0|_F = |x_0|_F \geqslant |x_n|_F$, also $\frac{|x_n|_F}{|z_0|_F} \leqslant 1$ für alle $n \geqslant 0$ ist. Damit folgt wegen der Multiplikativität von τ in 3.14

$$\begin{aligned} x &= \sum_{n=0}^{\infty} p^n[x_n] = \sum_{n=0}^{\infty} p^n[z_0 u_n] \\ &= [z_0] \textstyle\sum_{n=0}^{\infty} p^n[u_n] \end{aligned}$$

mit $\sum_{n=0}^{\infty} p^n[u_n] \in W(\mathcal{O}_F)^\times$ nach 4.1, da $u_0 = 1$ ist.
Sei nun $x = [z_0]\sum_{n=0}^{\infty} p^n[u_n] = \sum_{n=0}^{\infty} p^n[z_0u_n]$ mit $z_0 \in \mathcal{O}_F$ und $u = \sum_{n=0}^{\infty} p^n[u_n] \in W(\mathcal{O}_F)^\times$. Dann ist nach 4.1 $|u_0|_F = 1$. Da $u \in W(\mathcal{O}_F)$ ist, folgt $|u_n|_F \leqslant |u_0|_F$ für alle $n \geqslant 0$. Insgesamt gilt $|x_n|_F = |z_0u_n|_F \leqslant |z_0|_F|u_0|_F = |x_0|_F$. □

Proposition 4.6
Sind $x, y \in W(\mathcal{O}_F)$ stabil, so ist $|xy| = |x||y|$ und xy ist stabil.

Beweis: Seien $x, y \in W(\mathcal{O}_F)$ stabil. In 4.5 wurde gezeigt, dass $z_0^x, z_0^y \in \mathcal{O}_F$ und $u^x, u^y \in W(\mathcal{O}_F)^\times$ existieren mit $x = [z_0^x]u^x$ und $y = [z_0^y]u^y$. Damit ist $xy = [z_0^x z_0^y]u^x u^y$ mit $u^x u^y \in W(\mathcal{O}_F)^\times$ stabil nach 4.5. Insbesondere gilt $|xy| = |(xy)_0|_F = |x_0y_0|_F = |x_0|_F|y_0|_F = |x||y|$. □

Das nächste Ziel ist zu zeigen, dass für ein primitives $z \in W(\mathcal{O}_F)$ jedes Element in $W(\mathcal{O}_F)/zW(\mathcal{O}_F)$ einen stabilen Repräsentanten besitzt.
Sei $\overline{z} \in F$ mit $0 < |\overline{z}|_F \leqslant p^{-1}$ und sei

$$V_{n,m} := \ker \begin{pmatrix} W(\mathcal{O}_F) & \stackrel{W(q_{\mathcal{O}_F,(\overline{z}^m)})}{\to} & W(\mathcal{O}_F/\overline{z}^m\mathcal{O}_F) & \stackrel{q_{(0,n)}}{\to} & W_n(\mathcal{O}_F/\overline{z}^m\mathcal{O}_F) \\ (x_i)_{i\geqslant 0} & \mapsto & (x_i + \overline{z}^m\mathcal{O}_F)_{i\geqslant 0} & \mapsto & (x_i + \overline{z}^m\mathcal{O}_F)_{i\geqslant 0} + V_n(\mathcal{O}_F/\overline{z}^m\mathcal{O}_F) \end{pmatrix}.$$

$U \subseteq W(\mathcal{O}_F)$ heißt offen bzgl. der **schwachen Topologie**, falls zu jedem $x \in U$ natürliche Zahlen n und m existieren mit $x + V_{n,m} \subseteq U$.

Lemma 4.7

i) $W(\mathcal{O}_F)$ ist bzgl. der schwachen Topologie separiert und vollständig.

ii Die schwache Topologie auf $W(\mathcal{O}_F)$ stimmt mit der $(p, [\overline{z}])$-adischen Topologie überein, d.h. $U \subseteq W(\mathcal{O}_F)$ ist bzgl. der schwachen Topologie genau dann offen, wenn es zu jedem $x \in U$ ein $N \in \mathbb{N}$ gibt mit $x + (p, [\overline{z}])^N \subseteq U$.

Beweis: Siehe [3] Remark 1.5.2 und Remark 2.1.5. □

Jede $[\overline{z}]$-adische Cauchyfolge in $W(\mathcal{O}_F)$ ist auch eine $(p, [\overline{z}])$-adische Cauchyfolge, konvergiert also in $W(\mathcal{O}_F)$ bzgl. der schwachen Topologie. Jede Cauchyfolge bzgl. $|\cdot| : W(\mathcal{O}_F) \to \mathbb{R}$, $\sum_{n\geqslant 0} p^n[x_n] \mapsto \sup_{n\geqslant 0} |x_n|_F$ ist auch eine $\overline{z}$-adische Cauchyfolge für $\overline{z} \in \mathcal{O}_F$ mit $|\overline{z}|_F = p^{-1}$, denn für eine Cauchyfolge $(a_n)_{n\geqslant 0}$ mit $a_n \in W(\mathcal{O}_F)$ gibt es ein $N_1 \in \mathbb{N}$ mit $|a_n - a_m| < p^{-N}$ für alle $m, n \geqslant N_1$. Dann ist $a_n - a_m = \sum_{i\geqslant 0} p^i[z_i]$ mit $|z_i|_F < p^{-N}$ für alle $i \geqslant 0$ für $n, m \geqslant N_1$. Mit 1.2.12 folgt, dass $z_i \in \overline{z}^N$ ist. Es gibt also $z_i' \in \mathcal{O}_F$ mit $z_i = \overline{z}^N z_i'$. Damit ist $a_n - a_m = \sum_{i\geqslant 0} p^i[\overline{z}^N z_i'] = [\overline{z}]^N \sum_{i\geqslant 0} p^i[z_i'] \in \overline{z}^N W(\mathcal{O}_F)$. Das bedeutet, dass jede Cauchyfolge bzgl. $|\cdot|$ in $W(\mathcal{O}_F)$ bzgl. der schwachen Topologie konvergiert.

Lemma 4.8
Sei $z \in W(\mathcal{O}_F)$ primitiv. Zu jedem Element in $W(\mathcal{O}_F)/zW(\mathcal{O}_F)$ existiert ein stabiler Repräsentant.

Beweis: Sei $z \in W(\mathcal{O}_F)$ primitiv. Nach 4.4 gibt es eine Darstellung $z = [\overline{z}]+pz_1$ mit $z_1 \in W(\mathcal{O}_F)^\times$. Sei $x \in W(\mathcal{O}_F)$. Nun wird ein spezielles Element konstruiert, das kongruent zu $x \mod zW(\mathcal{O}_F)$ ist. Anschließend wird man sehen, dass dieses Element stabil ist. Seien dazu $x_0 := x$. Angenommen x_l ist für $l \geqslant 0$ bereits konstruiert mit $x_l \equiv x \mod zW(\mathcal{O}_F)$. Dann schreibe $x_l = \sum_{n=0}^\infty p^n[\overline{x_{l,n}}]$ mit eindeutigen Elementen $\overline{x_{l,n}}$, wie in 4.1 ii). Man setze $x_{l,1} := \sum_{n=0}^\infty p^n[\overline{x_{l,n+1}}]$ und $x_{l+1} := x_l - x_{l,1}z_1^{-1}z$. Damit ist auch $x_{l+1} \equiv x \mod zW(\mathcal{O}_F)$.

1. Fall: Es gibt ein $l \in \mathbb{N}$ mit $|\overline{x_{l,n}}|_F < p|\overline{x_{l,0}}|_F$ für alle $n > 0$. Dann ist

$$\begin{aligned} x_{l+1} &= x_l - x_{l,1}z_1^{-1}z = x_l - x_{l,1}z_1^{-1}([\overline{z}]+pz_1) = x_l - x_{l,1}z_1^{-1}[\overline{z}] - px_{l,1} \\ &= x_l - px_{l,1} - x_{l,1}z_1^{-1}[\overline{z}] \\ &= \sum_{n=0}^\infty p^n[\overline{x_{l,n}}] - p\sum_{n=0}^\infty p^n[\overline{x_{l,n+1}}] - x_{l,1}z_1^{-1}[\overline{z}] \\ &= \sum_{n=0}^\infty p^n[\overline{x_{l,n}}] - \sum_{n=0}^\infty p^{n+1}[\overline{x_{l,n+1}}] - x_{l,1}z_1^{-1}[\overline{z}] \\ &= [\overline{x_{l,0}}] - x_{l,1}z_1^{-1}[\overline{z}]. \end{aligned} \tag{16}$$

Damit ist

$$|x_{l+1}| = |[\overline{x_{l,0}}] - x_{l,1}z_1^{-1}[\overline{z}]| \leqslant \max\{|\overline{x_{l,0}}|_F, |x_{l,1}z_1^{-1}[\overline{z}]|\} = |\overline{x_{l,0}}|_F,$$

da $|\overline{z}|_F = p^{-1}$, $|z_1^{-1}| = 1$ und $|x_{l,1}| = \sup_{n\geqslant 0}|\overline{x_{l,n+1}}|_F < p|\overline{x_{l,0}}|_F$ ist, wobei letzte Ungleichung wegen $|\overline{x_{l,n}}|_F < p|x_{l,0}|_F$ für alle $n > 0$ gilt. Damit ist $|\overline{x_{l+1,n}}|_F \leqslant |\overline{x_{l,0}}|_F$ für alle $n \geqslant 0$.
Wegen $\overline{x_{l+1,0}} = \overline{x_{l,0}} - \overline{zx_{l,1}z_1^{-1}}$ und $|\overline{zx_{l,1}}|_F|\overline{z_1^{-1}}|_F = p^{-1}|\overline{x_{l,1}}|_F < |\overline{x_{l,0}}|_F$ ist $|\overline{x_{l+1,0}}|_F = |\overline{x_{l,0}}|_F \geqslant |\overline{x_{l+1,n}}|_F$ für alle $n \geqslant 0$. Das Element x_{l+1} ist somit stabil und es erfüllt per Konstruktion die Kongruenz $x \equiv x_{l+1} \mod zW(\mathcal{O}_F)$.

2. Fall: Nun existiere zu jedem $l \in \mathbb{N}$ ein $n_l > 0$ mit $|\overline{x_{l,n_l}}|_F \geqslant p|\overline{x_{l,0}}|_F$. Dann gilt nach 4.2 iv) und v) $|x_{l,1}z_1^{-1}[\overline{z}]| = |x_{l,1}||z_1||\overline{z}|_F = \sup_{n\geqslant 0}|\overline{x_{l,n+1}}|_F p^{-1} \geqslant |\overline{x_{l,0}}|_F$, woraus die Ungleichung

$$\begin{aligned} |x_{l+1}| &\overset{(16)}{=} |[\overline{x_{l,0}}] - x_{l,1}z_1^{-1}[\overline{z}]| \leqslant |x_{l,1}z_1^{-1}[\overline{z}]| \\ &= p^{-1}\sup_{n\geqslant 0}|\overline{x_{l,n+1}}|_F = p^{-1}\sup_{n\geqslant 0}|\overline{x_{l,n}}|_F = p^{-1}|x_l| \end{aligned} \tag{17}$$

folgt. Die Vorletzte Gleichung von (17) gilt wegen der Voraussetzung $|\overline{x_{l,0}}|_F \leqslant p|\overline{x_{l,0}}|_F \leqslant |\overline{x_{l,n_l}}|_F$ für ein $n_l > 0$. Außerdem ist für alle $m \geqslant 0$

$$|x_m| = \sup_{n\geqslant 0}|\overline{x_{m,n}}|_F \geqslant \sup_{n\geqslant 0}|\overline{x_{m,n+1}}|_F = |x_{m,1}|. \tag{18}$$

Mit (17) und (18) ist nun leicht zu zeigen, dass $(\sum_{l=0}^n x_{l,1}z_1^{-1})_{n\geqslant 0}$ eine Cauchyfolge in $W(\mathcal{O}_F)$ bzgl. $|\cdot|$ ist. Nach 1.3.2 i) und 4.2 genügt es dafür zu zeigen, dass die Abstände zweier aufeinander folgender Folgenglieder beliebig klein werden. Sei $\epsilon > 0$. Für $N \in \mathbb{N}$ mit $p^{-N}|x_0| < \epsilon$ und für alle $n \geqslant N$ gilt

$$|\sum_{l=0}^n x_{l,1}z_1^{-1} - \sum_{l=0}^{n-1} x_{l,1}z_1^{-1}| = |x_{n,1}z_1^{-1}| \overset{(18)}{\leqslant} |x_n| \overset{(17)}{\leqslant} p^{-n}|x_0| \leqslant p^{-N}|x_0| < \epsilon.$$

Damit ist $(\sum_{l=0}^n x_{l,1}z_1^{-1})_{n\geqslant 0}$ eine $(p,[\overline{z}])$-adische Cauchyfolge und konvergiert bzgl. dieser Topo-

logie gegen $y := \sum_{l=0}^{\infty} x_{l,1} z_1^{-1}$.
Die Folge $(\sum_{l=0}^{n} x_{l,1} z_1^{-1} z)_{n \geqslant 0}$ konvergiert gegen x, da $(\sum_{l=0}^{n} x_{l,1} z_1^{-1} z) - x = -x_{n+1}$ für alle $n \in \mathbb{N}$ und $(-x_n)_{n \geqslant 0}$ wegen (17) offensichtlich eine Nullfolge ist. Damit ist $x = yz$. In diesem Fall gilt also $x \equiv 0 \mod zW(\mathcal{O}_F)$. Als stabiler Repräsentant kann 0 gewählt werden.

□

Lemma 4.9
Jedes stabile Element in $W(\mathcal{O}_F)$, welches in einem durch ein primitives Element erzeugten Hauptideal liegt, ist 0.

Beweis: Sei $x = \sum_{n=0}^{\infty} p^n [\overline{x_n}] \in zW(\mathcal{O}_F)$ stabil mit $z = [\overline{z}] + pz_1 \in W(\mathcal{O}_F)$ primitiv und $z_1 \in W(\mathcal{O}_F)^\times$ und $y := xz^{-1} = \sum_{n=0}^{\infty} p^n [\overline{y_n}]$. Dann ist $\overline{x} = \overline{y_0 z}$ und da $|\overline{z}|_F = p^{-1}$ ist, folgt $p|\overline{x}|_F = |\overline{y}|_F$. Außerdem ist $x = yz = y([\overline{z}] + pz_1) = pz_1 y + [\overline{z}]y$. Da $|pz_1| = 1 > p^{-1} = |[\overline{z}]|$ ist, gilt nach 4.2 iv) und v)

$$|x| = \max\{|pz_1 y|, |[\overline{z}]y|\} = |pz_1 y| = |y|.$$

Das bedeutet $\sup_{n \geqslant 0} |\overline{x_n}| = \sup_{n \geqslant 0} |\overline{y_n}|$. Nach Voraussetzung ist x stabil und es gilt $|x| = |\overline{x}|_F$. Daher ist

$$|y| = \sup_{n \geqslant 0} |\overline{y_n}| \geqslant |\overline{y}|_F = p|\overline{x}|_F = p|x| = p|y|.$$

Dies ist nur für $|y| = 0$, also $y = 0$ möglich. Somit ist auch $x = 0$. □

Korollar 4.10
Seien $z \in W(\mathcal{O}_F)$ primitiv und $x, y \in W(\mathcal{O}_F)$ stabil mit $x \equiv y \mod zW(\mathcal{O}_F)$. Dann ist $|\overline{x}|_F = |\overline{y}|_F$.

Beweis: Sei $w := x - y = \sum_{n=0}^{\infty} p^n [\overline{w_n}]$ mit stabilen Elementen $x = \sum_{n=0}^{\infty} p^n [\overline{x_n}]$ und $y = \sum_{n=0}^{\infty} p^n [\overline{y_n}]$, sodass $w \in zW(\mathcal{O}_F)$ ist. Es gilt $|\overline{w_n}|_F \leqslant \max\{|\overline{x_0}|_F, |\overline{y_0}|_F\}$ für alle $n \geqslant 0$. Angenommen $|\overline{x_0}|_F \neq |\overline{y_0}|_F$. Dann ist $|\overline{w_0}|_F = \max\{|\overline{x_0}|_F, |\overline{y_0}|_F\} > 0$ und $w \neq 0$ ist stabil wegen $|\overline{w_n}|_F \leqslant \max\{|\overline{x_0}|_F, |\overline{y_0}|_F\}$ für alle $n \geqslant 0$. Darüberhinaus liegt w in $zW(\mathcal{O}_F)$. Dies ist ein Widerspruch zu 4.9. □

Sei $(F, |\cdot|_F)$ perfektoid mit $char(F) = p$. Sei ferner $z \in W(\mathcal{O}_F)$ primitiv. Für den Rest des Kapitels wird $W(\mathcal{O}_F)/zW(\mathcal{O}_F)$ mit $\mathcal{O}_K$ bezeichnet.
Sei $x \in \mathcal{O}_K$. Dann gibt es nach 4.8 ein stabiles Element $y \in W(\mathcal{O}_F)$ mit $x \equiv y \mod zW(\mathcal{O}_F)$. Die Zuordnung

$$\begin{array}{rccl} |\cdot|_K & : & \mathcal{O}_K & \to & [0,1] \subseteq \mathbb{R}_{\geqslant 0} \\ & & x & \mapsto & |y_0|_F \end{array}$$

ist nach 4.10 wohldefiniert.
Der folgende Satz wird nun zeigen, dass $\mathcal{O}_K$ nullteilerfrei und $Quot(\mathcal{O}_K)$ ein perfektoider Körper der Charakteristik 0 ist mit Tilt F. Genauer gilt:

Theorem 4.11

i) $|x|_K$ ist unabhängig von der Wahl von y.

ii) $|\cdot|_K$ erfüllt die Eigenschaften eines nicht-archimedischen Absolutbetrags auf $\mathcal{O}_K$.

iii) *Es gilt* $\mathcal{O}_K/p\mathcal{O}_K \cong \mathcal{O}_F/\overline{z}\mathcal{O}_F$.

iv) $\mathcal{O}_K$ *ist nullteilerfrei mit* $char(\mathcal{O}_K) = 0$. $|\cdot|_K$ *setzt sich zu einem nicht-archimedischen Absolutbetrag auf* $K := Quot(\mathcal{O}_K) = \mathcal{O}_K[\frac{1}{p}]$ *fort mit Bewertungsring* $\mathcal{O}_K$.

v) $\mathcal{O}_K$ *ist bzgl.* $|\cdot|_K$ *vollständig.*

vi) K *ist ein perfektoider Körper.*

vii) $K^\flat$ *ist isometrisch isomorph zu* F.

Beweis: i) gilt nach 4.10.
ii) Genau dann ist $|x|_K = |y| = 0$ mit y stabil, wenn $y = 0$ ist, da $0 = |x|_K = |y| = \sup_{n\geqslant 0} |y_n|_F$. Es folgt $x \equiv y = 0 \mod zW(\mathcal{O}_F)$.
Seien $x, x' \in \mathcal{O}_K$ und $y, y' \in \mathcal{O}_K$ stabil, mit $x \equiv y \mod zW(\mathcal{O}_F)$ und $x' \equiv y' \mod zW(\mathcal{O}_F)$. Nach 4.6 ist yy' stabil mit $x' \equiv yy' \mod zW(\mathcal{O}_F)$, sodass nach 4.6

$$|xx'|_K = |yy'| = |y||y'| = |x|_K|x'|_K.$$

Seien $x, x' \in \mathcal{O}_K$ und $y, y' \in W(\mathcal{O}_F)$ mit $x \equiv y \mod zW(\mathcal{O}_F)$ und $x' \equiv y' \mod zW(\mathcal{O}_F)$. Dann ist $x + x' \equiv y + y' \mod zW(\mathcal{O}_F)$. Als stabiler Repräsentant $w \equiv y + y' \mod zW(\mathcal{O}_F)$ wird ein Element wie in 4.8 gewählt, also $w = 0$, falls $x + x' \equiv 0 \mod zW(\mathcal{O}_F)$, oder $w = w_{l+1} = w_l - w_{l,1}z_1^{-1}z$ mit $z = [\overline{z}] + pz_1$, wobei $z_1 \in W(\mathcal{O}_F)^\times$, $w_l = \sum_{n=0}^{\infty} p^n[\overline{x_{l,n}}] \equiv x + x' \mod zW(\mathcal{O}_F), w_0 = y + y'$ und $w_{l,1} = \sum_{n=0}^{\infty} p^n[\overline{w_{l,n+1}}]$ sind, falls $x + x' \neq 0$ in $W(\mathcal{O}_K)$.
Damit ergibt sich

$$|w_{l,1}z_1^{-1}z| \underset{\text{iv)}}{\overset{4.2}{\leqslant}} |w_{l,1}||z_1^{-1}||z| \underset{\text{iv)}}{\overset{4.2}{=}} |w_{l,1}||z| \overset{4.4}{=} |w_{l,1}| \leqslant |w_l|.$$

Dies impliziert $|w_{l+1}| \leqslant \max\{|w_l|, |w_{l,1}z_1^{-1}z|\} = |w_l|$ und somit $|w_{l+1}| \leqslant |w_l| \leqslant .. \leqslant |w_0| = |y + y'|$, nach der induktiven Konstruktion von w_{l+1}. Daraus folgt

$$|x + x'|_K = |w| = |w_{l+1}| \leqslant |y + y'| \underset{\text{ii)}}{\overset{4.2}{\leqslant}} \max\{|y|, |y'|\} = \max\{|x|_K, |x'|_K\}.$$

iii) Nach dem zweiten Isomorphiesatz für Ringe gilt

$$\begin{aligned} \mathcal{O}_K/p\mathcal{O}_K &\cong (W(\mathcal{O}_F)/zW(\mathcal{O}_F))/p(W(\mathcal{O}_F)/zW(\mathcal{O}_F)) \cong W(\mathcal{O}_F)/(p, z) \\ &\cong (W(\mathcal{O}_F)/pW(\mathcal{O}_F))/\overline{z}(W(\mathcal{O}_F)/pW(\mathcal{O}_F)) \cong \mathcal{O}_F/\overline{z}\mathcal{O}_F, \end{aligned}$$

wobei die Abbildung gegeben ist durch $(x + zW(\mathcal{O}_F)) + p\mathcal{O}_K \mapsto x_0 + \overline{z}\mathcal{O}_F$.
iv) $\mathcal{O}_K$ ist nullteilerfrei, denn nach i) ist genau dann $xy = 0$, wenn $0 = |xy|_K = |x|_K|y|_K \in \mathbb{R}$. Das ist genau dann der Fall, wenn $x = 0$ oder $y = 0$.
Da $\mathcal{O}_K$ ein Integritätsbereich ist, ist entweder $char(\mathcal{O}_K) = 0$ oder $char(\mathcal{O}_K) = q$, wobei q eine Primzahl ist. Wegen iii), $char(\mathcal{O}_F) = p$ und 1.1.1 ist $char(\mathcal{O}_K/p\mathcal{O}_K) = char(\mathcal{O}_F/\overline{z}\mathcal{O}_F) = p$. Wegen 1.1.1 ist $char(\mathcal{O}_K) = 0$ oder $char(\mathcal{O}_K) = p$.
Angenommen $char(\mathcal{O}_K) = p$, d.h. $p \in zW(\mathcal{O}_F)$. Dann gibt es ein $w \in W(\mathcal{O}_F)$ mit $p = wz$. Nach 4.4 gibt es die Darstellung $z = [\overline{z}] + pz_1$ mit $z_1 \in W(\mathcal{O}_F)^\times$. Wegen $p = wz = w[\overline{z}] + pwz_1$ ist $w[\overline{z}] \in pW(\mathcal{O}_F) = \{(y_n)_{n\geqslant 0} : y_0 = 0\}$. Da $|\overline{z}|_F = p^{-1}$ und $w[\overline{z}] = (w_0\overline{z}, \ldots) = (0, \ldots)$ ist $w \in pW(\mathcal{O}_F)$. Es gibt also $w' \in W(\mathcal{O}_F)$ mit $w = pw'$. Damit ist $p = wz = pw'z$ und somit $w'z = 1$, da $W(\mathcal{O}_F)$ ein Integritätsring ist. Dies sieht man im Beweis von 3.21. Das Element z liegt in $W(\mathcal{O}_F)^\times$ und somit ist

$|z_0|_F = |\overline{z}|_F = 1$. Da z primitiv ist, ist dies ein Widerspruch. Also ist $char(\mathcal{O}_K) = 0$.
Nach einem allgemeinen Prinzip setzt sich der Absolutbetrag $|\cdot|_K$ auf $\mathcal{O}_K$ eindeutig zu einem Absolutbetrag $|\cdot|_K$ auf $K = Quot(\mathcal{O}_K)$ fort via

$$\begin{array}{rcccl} |\cdot|_K & : & K = Quot(\mathcal{O}_K) & \to & \mathbb{R}_{\geqslant 0} \\ & & xy^{-1} & \mapsto & |x|_K|y|_K^{-1}. \end{array}$$

Es ist noch zu zeigen, dass $\mathcal{O}_K = \{w \in K : |w|_K \leqslant 1\}$. Dabei ist offensichtlich
$\mathcal{O}_K \subseteq \{w \in K : |w|_K \leqslant 1\}$.
Sei $w = \frac{x}{y}$ mit $|w|_K = \frac{|x|_K}{|y|_K} \leqslant 1$. Damit ist $|x|_K \leqslant |y|_K$. Seien x' bzw. $y' \in W(\mathcal{O}_F)$ stabile Repräsentanten von x bzw. y. Dann gibt es nach 4.5 $u, v \in W(\mathcal{O}_F)^\times$ und $x_0', y_0' \in \mathcal{O}_F$ mit $x' = u[x_0']$ und $y' = v[y_0']$. Das Element $z_0' := \frac{x_0'}{y_0'}$ liegt in $\mathcal{O}_F$, da $|x|_K = |x'| = |x_0'|_F \leqslant |y|_K = |y_0'|_F$. Damit ist $r := uv^{-1}[z_0'] \in W(\mathcal{O}_F)$ und $ry' = x'$. Wegen $(r + zW(\mathcal{O}_F))y = x$ ist $w = \frac{x}{y} = r + zW(\mathcal{O}_F) \in W(\mathcal{O}_F)/zW(\mathcal{O}_F) = \mathcal{O}_K$.
Offensichtlich ist $\mathcal{O}_K[\frac{1}{p}] \subseteq K$, wobei $p \neq 0$ in K, wie oben gesehen.
Es gilt $\mathcal{O}_K/p\mathcal{O}_K \cong \mathcal{O}_F/\overline{z}\mathcal{O}_F \neq 0$, da $|\overline{z}|_F = p^{-1}$. Damit ist $p \notin \mathcal{O}_K^\times$, also $|p|_K < 1$. Sei $\frac{x}{y} \in K$ und $n \in \mathbb{N}$ mit $|p|_K^n \leqslant |y|_K \leqslant 1$. Nach 1.2.12 liegt p^n in $y\mathcal{O}_K$, also gibt es ein $b \in \mathcal{O}_K$ mit $p^n = by$. Das Element $\frac{p^n}{b} = y$ liegt in K und es gilt $\frac{x}{y} = \frac{xb}{p^n} \in \mathcal{O}_K[\frac{1}{p}]$.
v) In iv) wurde gezeigt, dass $0 < |p|_K < 1$. Damit ist die durch $|\cdot|_K$ induzierte Topologie auf $\mathcal{O}_K$ die p-adische Topologie. Sei also $(x_n)_{n\geqslant 0}$ eine p-adische Cauchyfolge in $\mathcal{O}_K$ mit $x_0 = x_0' + zW(\mathcal{O}_F)$, wobei $x_0' \in W(\mathcal{O}_F)$. Sei $x_n' \in W(\mathcal{O}_F)$ mit $x_n = x_n' + zW(\mathcal{O}_F)$ wie folgt gewählt: falls $x_{n-1} = x_n$ wird $x_n' := x_{n-1}'$ gesetzt. Für $x_{n-1} \neq x_n$ sei $N \in \mathbb{N}$ maximal gewählt mit $x_n - x_{n-1} \in p^N\mathcal{O}_K$. Dann gibt es ein $b_n \in \mathcal{O}_K$ mit $x_n - x_{n-1} = p^N b_n$. Schreibe $b_n = b_n' + zW(\mathcal{O}_F)$. Dann wird $x_n' := x_{n-1}' + p^N b_n'$ gesetzt. Nach Konstruktion ist dann $(x_n')_{n\geqslant 0}$ eine p-adische Cauchyfolge in $W(\mathcal{O}_F)$. Wegen 3.18 iv) ist $W(\mathcal{O}_F)$ p-adisch vollständig und somit konvergiert $(x_n')_{n\geqslant 0}$ in $W(\mathcal{O}_F)$. Sei $x' = \lim_{n\to\infty} x_n' \in W(\mathcal{O}_F)$. Damit gibt es für $N \in \mathbb{N}$ ein $n_0 \in \mathbb{N}$ mit $x' - x_n' \in p^N W(\mathcal{O}_F)$ für alle $n \geqslant n_0$. Für $x := x' + zW(\mathcal{O}_F) \in \mathcal{O}_K$ und $n \geqslant n_0$ gilt daher $x - x_n = x' - x_n' + zW(\mathcal{O}_F) \in p^N(W(\mathcal{O}_F)/zW(\mathcal{O}_F) = p^N\mathcal{O}_K$. Das bedeutet x ist p-adischer Grenzwert von $(x_n)_{n\geqslant 0}$.
vi) Da $\mathcal{O}_K$ nach v) bzgl. $|\cdot|_K$ vollständig ist, ist K nach 1.3.9 vollständig.
Für alle $x_0 \in \mathcal{O}_F$ ist $[x_0] \in W(\mathcal{O}_F)$ stabil. Damit ist $|[x_0] + zW(\mathcal{O}_F)|_K = |x_0|_F$ und somit $|F|_F \subseteq |K|_K$. Die umgekehrte Inklusion gilt per Definition, sodass $|K|_K = |F|_F \subseteq \mathbb{R}_{\geqslant 0}$ dicht liegt.
Da F perfektoid mit $char(F) = p$ ist, ist der Frobenius $\mathcal{O}_F \to \mathcal{O}_F, \quad x \mapsto x^p$ surjektiv. Damit ist $\mathcal{O}_F/\overline{z}\mathcal{O}_F \to \mathcal{O}_F/\overline{z}\mathcal{O}_F, \quad x \mapsto x^p$ surjektiv und wegen iii) auch $\mathcal{O}_K/p\mathcal{O}_K \to \mathcal{O}_K/p\mathcal{O}_K, \quad x \to x^p$. K ist demnach perfektoid.
vii) Es gilt $\mathcal{O}_{K^\flat} = \varprojlim_{x\mapsto x^p} \mathcal{O}_K/p\mathcal{O}_K \cong \varprojlim_{x\mapsto x^p} \mathcal{O}_F/\overline{z}\mathcal{O}_F$. Zunächst wird gezeigt, dass

$$\begin{array}{rcccl} \omega & : & \mathcal{O}_F & \to & \varprojlim\limits_{x\mapsto x^p} \mathcal{O}_F/\overline{z}\mathcal{O}_F \\ & & x & \mapsto & (x^{p^{-n}} + \overline{z}\mathcal{O}_F)_{n\geqslant 0} \end{array}$$

ein Ringhomomorphismus ist. ω ist ein Homomorphismus, da der Frobenius auf $\mathcal{O}_F$ ein Ringisomorphismus ist.
Sei $x \in \ker(\omega)$. Damit ist $x^{p^{-n}} \in \overline{z}\mathcal{O}_F$ für alle $n \in \mathbb{N}$. Für alle $n \in \mathbb{N}$ ist somit $|x|_F \leqslant |\overline{z}|_F^{p^n} = p^{-p^n}$. Dadurch ist $|x|_F = 0$, also $x = 0$ und somit ist ω injektiv.

Sei nun $(x_n + \overline{z}\mathcal{O}_F)_{n\geqslant 0} \in \varprojlim_{x\mapsto x^p} \mathcal{O}_F/\overline{z}\mathcal{O}_F$. Dann ist

$$x_{n+1}^{p^{n+1}} - x_n^{p^n} = (x_{n+1}^p - x_n)^{p^n} \in \overline{z}^{p^n}\mathcal{O}_F$$

mit $|\overline{z}|_F = p^{-1}$. Da $|\cdot|_F$ ein nicht-archimedischer Absolutbetrag ist, ist $(x_n^{p^n})_{n\geqslant 0}$ eine Cauchyfolge in $\mathcal{O}_F$. Sei $x := \lim_{n\to\infty} x_n^{p^n} \in \mathcal{O}_F$. Dieser Grenzwert existiert wegen der Vollständigkeit von $\mathcal{O}_F$. Sei für $n \in \mathbb{N}$ das Element $m \in \mathbb{N}$ groß genug gewählt mit $x - x_{n+m}^{p^{n+m}} \in \overline{z}^{p^n}$. Wegen der Definition von $\varprojlim_{x\mapsto x^p} \mathcal{O}_F/\overline{z}\mathcal{O}_F$ gilt $x_{n+m}^{p^{n+m}} - x_n^{p^n} = (x_{n+m}^{p^m} - x_n)^{p^n} \in \overline{z}^{p^n}\mathcal{O}_F$. Somit ist

$$x - x_n^{p^n} = x - x_{n+m}^{p^{n+m}} + x_{n+m}^{p^{n+m}} - x_n^{p^n} \in \overline{z}^{p^n}\mathcal{O}_F.$$

Es gilt $x^{p^{-n}} \equiv x_n \mod \overline{z}\mathcal{O}_F$. Damit ist $\omega(x) = (x^{p^{-n}} + \overline{z}\mathcal{O}_F)_{n\geqslant 0} = (x_n + \overline{z}\mathcal{O}_F)_{n\geqslant 0}$. Die Abbildung ω ist daher ein Ringisomorphismus. Damit ist $\mathcal{O}_{K^\flat} \cong \mathcal{O}_F$ und somit auch $K^\flat = (\mathcal{O}_{K^\flat}) \cong Quot(\mathcal{O}_F) = F$. Es ist noch zu zeigen, dass dieser Isomorphismus eine Isometrie ist. Der Isomorphismus

$$\mathcal{O}_{K^\flat} = \varprojlim_{x\mapsto x^p} \mathcal{O}_K/p\mathcal{O}_K \overset{\text{iii)}}{\cong} \varprojlim_{x\mapsto x^p} \mathcal{O}_F/\overline{z}\mathcal{O}_F \xrightarrow{\omega^{-1}} \mathcal{O}_F$$

bildet $y = (y_n + zW(\mathcal{O}_F) + p\mathcal{O}_K)_{n\geqslant 0}$ ab auf $x = \lim_{n\to\infty} \overline{y_n}^{p^n}$. Für $n \geqslant 0$ sei $y_n' \in W(\mathcal{O}_F)$ stabil mit $y_n \equiv y_n' \mod zW(\mathcal{O}_F)$. Da $\overline{y_n'} \equiv \overline{y_n} \mod \overline{z}\mathcal{O}_F$ für alle $n \geqslant 0$ folgt aus dem Beweis der Bijektivität von ω, dass $x = \lim_{n\to\infty} \overline{y_n'}^{p^n}$ und daher

$$|y|_\flat = |y^\#|_K = \lim_{n\to\infty} |y_n^{p^n} zW(\mathcal{O}_F)|_K = \lim_{n\to\infty} |(y_n')^{p^n}| \overset{4.6}{=} \lim_{n\to\infty} |(\overline{y_n'})^{p^n}|_F = |x|_F.$$

$\square$

Damit ist also $K = Quot(W(\mathcal{O}_F)/zW(\mathcal{O}_F)$ für einen perfektoiden Körper F der Charakteristik p und ein primitives Element $z \in W(\mathcal{O}_F)$ ein perfektoider Körper der Charakteristik 0. Darüber hinaus sind $K^\flat$ und F isometrisch isomorph.

5 Die Äquivalenz

Sei in diesem Kapitel stets $(K, |\cdot|)$ ein perfektoider Körper mit $char(K) = 0$ und $K^\flat$ sein Tilt mit $char(K^\flat) = p$. Da p die Charakteristik des Restklassenkörpers ist, ist $p \in \mathfrak{m}$, wobei $\mathfrak{m}$ das maximale Ideal in $\mathcal{O}_K$ ist. Damit ist $|p| < 1$. In 4.11 v) wurde gezeigt, dass die durch diesen Absolutbetrag induzierte Toplogie der p-adischen Topologie entspricht. Indem wir eventuell zu einem äquivalenten Absolutbetrag übergehen, dürfen wir nach 1.2.3 im Folgenden stets $|p| = p^{-1}$ annehmen. Wir werden nun zeigen, dass K bis auf isometrische Isomorphie von der Form wie in 4.11 ist mit $F = K^\flat$.

Proposition 5.1

i) Es gibt genau einen Ringhomomorphismus $\vartheta : W(\mathcal{O}_{K^\flat}) \to \mathcal{O}_K$ mit $\vartheta([y]) = y^\#$ für alle $y \in \mathcal{O}_{K^\flat}$. Er ist gegeben durch $\vartheta(\sum_{n=0}^\infty p^n[x_n]) = \sum_{n=0}^\infty p^n x_n^\#$.

ii) ϑ ist surjektiv.

iii) $\ker(\vartheta)$ ist ein Hauptideal und wird von einem primitiven Element $z \in W(\mathcal{O}_{K^\flat})$ erzeugt.

iv) Für jedes Element $z' = (z'_0, z'_1, \ldots) \in W(\mathcal{O}_{K^\flat})$ mit $|z'_0|_\flat = p^{-1}$ und $z' \in \ker(\vartheta)$ gilt $\ker(\vartheta) = z'W(\mathcal{O}_{K^\flat})$.

Beweis: i) Zunächst wird die Eindeutigkeit gezeigt und die Existenz des Ringhomomorphismus ϑ vorausgesetzt. ϑ ist nach 1.5.5 p-adisch stetig. Sei $x \in W(\mathcal{O}_{K^\flat})$ mit $x = \sum_{n=0}^\infty p^n[x_n]$. Dann ist

$$\vartheta(x) = \vartheta(\sum_{n=0}^\infty p^n[x_n]) = \sum_{n=0}^\infty p^n \vartheta([x_n]) = \sum_{n=0}^\infty p^n x_n^\#.$$

$\mathcal{O}_K$ ist p-adisch vollständig, da wie im Beweis von 4.11 v) der Absolutbetrag von K der p-adischen Topologie entspricht. Damit konvergiert die Reihe $\sum_{n=0}^\infty p^n x_n^\#$ in $\mathcal{O}_K$ und ϑ ist dadurch eindeutig.
Es ist noch zu zeigen, dass ϑ existiert. Dazu wird ein Homomorphismus $\tilde{\vartheta}$ konstruiert, der $\tilde{\vartheta} \circ [\cdot] = (\cdot)^\#$ erfüllt. Die Abbildung $\Phi_n : W(\mathcal{O}_K) \to \mathcal{O}_K$ ist nach 3.8 ii) ein Ringhomomorphismus mit $\Phi_n(V_{n+1}(\mathcal{O}_K)) = \{0\}$, da $V_{n+1}(\mathcal{O}_K) = \{(x_m)_{m \geqslant 0} : x_0 = x_1 = .. = x_n = 0\}$. Daher induziert Φ_n den Ringhomomorphismus

$$\begin{array}{rrcl} \Phi'_n : & W_{n+1}(\mathcal{O}_K) = W(\mathcal{O}_K)/V_{n+1}(\mathcal{O}_K) & \to & \mathcal{O}_K \\ & (x_0, \ldots, x_n, 0, 0, \ldots) + V_{n+1}(\mathcal{O}_K) & \mapsto & \Phi_n(x_0, \ldots, x_n). \end{array}$$

Nach 3.8 iii) induziert $q_{\mathcal{O}_K,(p)} : \mathcal{O}_K \to \mathcal{O}_K/p\mathcal{O}_K$ die surjektiven Ringhomomorphismen

$$\begin{array}{rrcl} W(q_{\mathcal{O}_K,(p)}) : & W(\mathcal{O}_K) & \to & W(\mathcal{O}_K/p\mathcal{O}_K) \\ & (x_n)_{n \geqslant 0} & \mapsto & (x_n + p\mathcal{O}_K)_{n \geqslant 0} \end{array}$$

$$\begin{array}{rrcl} W_n(q_{\mathcal{O}_K,(p)}) : & W_n(\mathcal{O}_K) & \to & W_n(\mathcal{O}_K/p\mathcal{O}_K) \\ & x + V_n(\mathcal{O}_K) & \mapsto & W(q_{\mathcal{O}_K,(p)})(x) + V_n(\mathcal{O}_K/p\mathcal{O}_K) \quad . \end{array}$$

Für $n \geqslant m$ definiere für einen Ring R den Ringhomomorphismus

$$\begin{array}{rrcl} q_{(n,m)} : & W_n(R) & \to & W_m(R) \\ & x + V_n(R) & \mapsto & x + V_m(R). \end{array}$$

Der Kern des surjektiven Ringhomomorphismus

$$\begin{array}{ccccc} W_{n+1}(\mathcal{O}_K) & \xrightarrow{q_{(n+1,n)}} W_n(\mathcal{O}_K) & \xrightarrow{W_n(q_{\mathcal{O}_K,(p)})} & W_n(\mathcal{O}_K/p\mathcal{O}_K) \\ & (x_m)_{m\geqslant 0} + V_{n+1}(\mathcal{O}_K) & \longmapsto & (x_m + p\mathcal{O}_K)_{m\geqslant 0} + V_n(\mathcal{O}_K/p\mathcal{O}_K) \end{array}$$

ist $\{(x_m)_{m\geqslant 0} + V_{n+1}(\mathcal{O}_K) : x_0, \ldots, x_{n-1} \in p\mathcal{O}_K\}$ und liegt im Kern des Ringhomomorphismus

$$W_{n+1}(\mathcal{O}_K) \xrightarrow{\Phi'_n} \mathcal{O}_K \xrightarrow{q_{\mathcal{O}_K,(p^n)}} \mathcal{O}_K/p^n\mathcal{O}_K,$$

da für $(x_0, \ldots, x_{n-1}, x_n, \ldots) + V_{n+1}(\mathcal{O}_K) \in \ker(W_n(q_{\mathcal{O}_K,(p)})) \circ q_{(n+1,n)})$ mit $x_i = py_i$ für alle $i \in \{0, \ldots, n-1\}$ das Element

$$\Phi_n(x_0, \ldots, x_n) = (py_0)^{p^n} + p(py_1)^{p^{n-1}} + p^2(py_2)^{p^{n-2}} + \ldots + p^{n-1}(py_{n-1})^p + p^n x_n$$

in $p^n\mathcal{O}_K$ liegt wegen $p^{p^i} \in p^i\mathbb{Z}$. Nach dem Homomorphiesatz gibt es einen eindeutigen Homomorphismus ϑ_n, sodass folgendes Diagramm kommutiert:

$$\begin{tikzcd} W_{n+1}(\mathcal{O}_K) \arrow[r, "\Phi'_n"] \arrow[d, "q_{(n+1,n)}"'] & \mathcal{O}_K \arrow[r, "q_{\mathcal{O}_K,(p^n)}"] & \mathcal{O}_K/p^n\mathcal{O}_K \\ W_n(\mathcal{O}_K) \arrow[d, "W_n(q_{\mathcal{O}_K,(p)})"'] & & \\ W_n(\mathcal{O}_K/p\mathcal{O}_K) \arrow[uurr, "\vartheta_n"'] & & \end{tikzcd} .$$

Er erfüllt

$$\vartheta_n((x_0 + p\mathcal{O}_K, \ldots, x_{n-1} + p\mathcal{O}_K, \ldots) + V_n(\mathcal{O}_K/p\mathcal{O}_K)) = \sum_{i=0}^{n-1} p^i x_i^{p^{n-i}} + p^n\mathcal{O}_K.$$

Definiere die Abbildung für $m \geqslant n$

$$\begin{array}{cccc} \overline{q_{(m,n)}} : & \mathcal{O}_K/p^m\mathcal{O}_K & \to & \mathcal{O}_K/p^n\mathcal{O}_K \\ & x + p^m\mathcal{O}_K & \mapsto & x + p^n\mathcal{O}_K. \end{array}$$

Damit kommutiert

$$\begin{tikzcd} (x_m + p\mathcal{O}_K)_{m\geqslant 0} + V_{n+1}(\mathcal{O}_K/p\mathcal{O}_K) \arrow[dd, mapsto] & W_{n+1}(\mathcal{O}_K/p\mathcal{O}_K) \arrow[r, "\vartheta_{n+1}"] \arrow[d, "q_{(n+1,n)}"'] & \mathcal{O}_K/p^{n+1}\mathcal{O}_K \arrow[dd, "\overline{q_{(n+1,n)}}"] & x + p^{n+1}\mathcal{O}_K \arrow[dd, mapsto] \\ & W_n(\mathcal{O}_K/p\mathcal{O}_K) \arrow[d, "F"'] & & \\ (x_m^p + p\mathcal{O}_K)_{m\geqslant 0} + V_n(\mathcal{O}_K/p\mathcal{O}_K) & W_n(\mathcal{O}_K/p\mathcal{O}_K) \arrow[r, "\vartheta_n"'] & \mathcal{O}_K/p^n\mathcal{O}_K & x + p^n\mathcal{O}_K, \end{tikzcd} \tag{19}$$

da

$$\begin{aligned}
&\overline{q_{(n+1,n)}} \circ \vartheta_{n+1}((x_0 + p\mathcal{O}_K, \ldots, x_n + p\mathcal{O}_K, \ldots) + V_{n+1}(\mathcal{O}_K/p\mathcal{O}_K)\\
&= \overline{q_{(n+1,n)}}(\sum_{i=0}^{n} p^i x_i^{p^{n+1-i}} + p^{n+1}\mathcal{O}_K) = \sum_{i=0}^{n} p^i x_i^{p^{n+1-i}} + p^n\mathcal{O}_K\\
&= \sum_{i=0}^{n-1} p^i x_i^{p^{n+1-i}} + p^n\mathcal{O}_K = \sum_{i=0}^{n-1} p^i (x_i^p)^{p^{n-i}} + p^n\mathcal{O}_K\\
&= \vartheta_n((x_0^p + p\mathcal{O}_K, \ldots, x_{n-1}^p + p\mathcal{O}_K, \ldots) + V_n(\mathcal{O}_K/p\mathcal{O}_K))\\
&= \vartheta_n \circ F \circ q_{(n+1,n)}((x_0 + p\mathcal{O}_K, \ldots, x_n + p\mathcal{O}_K, \ldots) + V_{n+1}(\mathcal{O}_K/p\mathcal{O}_K)).
\end{aligned}$$

Mit den Ringhomomorphismen

$$\begin{array}{cccccc}
q_n & : & W(\mathcal{O}_{K^\flat}) \overset{q_{(0,n)}}{\to} & W_n(\mathcal{O}_{K^\flat}) \overset{W_n(pr_n)}{\to} & W_n(\mathcal{O}_K/p\mathcal{O}_K) \\
 & & ((\alpha_i^{(m)})_{i\geqslant 0})_{m\geqslant 0} & \longmapsto & (\alpha_n^{(m)})_{m\geqslant 0} + V_n(\mathcal{O}_K/p\mathcal{O}_K)
\end{array}$$

ist das Diagramm

$$\begin{tikzcd}
W(\mathcal{O}_{K^\flat}) \arrow[r, "q_{n+1}"] \arrow[ddr, "q_n"'] & W_{n+1}(\mathcal{O}_K/p\mathcal{O}_K) \arrow[d, "q_{(n+1,n)}"] & (\alpha_0, \ldots, \alpha_n, \ldots) + V_{n+1}(\mathcal{O}_K/p\mathcal{O}_K) \arrow[dd, mapsto] \\
 & W_n(\mathcal{O}_K/p\mathcal{O}_K) \arrow[d, "F"] & \\
 & W_n(\mathcal{O}_K/p\mathcal{O}_K) & (\alpha_0^p, \ldots, \alpha_{n-1}^p, \ldots) + V_n(\mathcal{O}_K/p\mathcal{O}_K)
\end{tikzcd} \tag{20}$$

kommutativ, da

$$\begin{aligned}
&F \circ q_{(n+1,n)} \circ q_{n+1}(((\alpha_i^{(m)})_{i\geqslant 0})_{m\geqslant 0})\\
&= F \circ q_{(n+1,n)}((\alpha_{n+1}^{(0)}, \alpha_{n+1}^{(1)}, \ldots, \alpha_{n+1}^{(n)}, \ldots) + V_{n+1}(\mathcal{O}_K/p\mathcal{O}_K))\\
&= ((\alpha_{n+1}^{(0)})^p, \ldots, (\alpha_{n+1}^{(n-1)})^p, \ldots) + V_n(\mathcal{O}_K/p\mathcal{O}_K) = (\alpha_n^{(0)}, \ldots, \alpha_n^{(n-1)}, \ldots) + V_n(\mathcal{O}_K/p\mathcal{O}_K)\\
&= q_n(((\alpha_i^{(m)})_{i\geqslant 0})_{m\geqslant 0}),
\end{aligned}$$

wobei vorletzte Gleichheit wegen $(\alpha_i^{(m)})_{i\geqslant 0} \in \mathcal{O}_{K^\flat}$ für alle $m \in \mathbb{N}$ und somit $(\alpha_{n+1}^{(m)})^p = \alpha_n^{(m)}$ für alle $m, n \in \mathbb{N}$ gilt.
Mit den Diagrammen (19) und (20) ist auch das Diagramm

$$\begin{tikzcd}
W(\mathcal{O}_{K^\flat}) \arrow[r, "q_{n+1}"] \arrow[dr, "q_n"'] & W_{n+1}(\mathcal{O}_K/p\mathcal{O}_K) \arrow[r, "\vartheta_{n+1}"] \arrow[d, "F\circ q_{(n+1,n)}"] & \mathcal{O}_K/p^{n+1}\mathcal{O}_K \arrow[dd, "\overline{q_{(n+1,n)}}"] \\
 & W_n(\mathcal{O}_K/p\mathcal{O}_K) \arrow[dr, "\vartheta_n"'] & \\
 & & \mathcal{O}_K/p^n\mathcal{O}_K
\end{tikzcd}$$

kommutativ. Wegen der universellen Eigenschaft des projektiven Limes in 1.5.1 gibt es für das projektive System $((\mathcal{O}_K/p^n\mathcal{O}_K)_{n\geqslant 0}, (\overline{q_{(m,n)}})_{m\geqslant n})$ einen eindeutigen Homomorphismus $\tilde{\vartheta}$, sodass folgendes

Diagramm kommutiert

$$\begin{tikzcd} W(\mathcal{O}_{K^\flat}) \arrow[r, "\tilde{\vartheta}"] \arrow[dr, "\vartheta_n \circ q_n"'] & \varprojlim_{i\in\mathbb{N}} \mathcal{O}_K/p^i\mathcal{O}_K \arrow[d, "pr_n"] \\ & \mathcal{O}_K/p^n\mathcal{O}_K. \end{tikzcd}$$

Außerdem ist nach 1.5.7 $\varprojlim_{i\in\mathbb{N}} \mathcal{O}_K/p^i\mathcal{O}_K \cong \mathcal{O}_K$, da $\mathcal{O}_K$ vollständig und $\bigcap_{n\in\mathbb{N}} p^n\mathcal{O}_K = 0$ ist. Wie bezeichnen mit ϑ den zusammengesetzten Homomorphismus $W(\mathcal{O}_{K^\flat}) \xrightarrow{\tilde{\vartheta}} \varprojlim_{i\in\mathbb{N}} \mathcal{O}_K/p^i\mathcal{O}_K \cong \mathcal{O}_K$. Sei $((\alpha_i^{(m)})_{i\geqslant 0})_{m\geqslant 0} \in W(\mathcal{O}_{K^\flat})$ und $x_n^{(i)} \in \mathcal{O}_K$ mit $x_n^{(i)} + p\mathcal{O}_K = \alpha_n^{(i)}$. Dann ist

$$\tilde{\vartheta}(((\alpha_i^{(m)})_{i\geqslant 0})_{m\geqslant 0}) + p^n\mathcal{O}_K = \vartheta_n \circ q_n(((\alpha_i^{(m)})_{i\geqslant 0})_{m\geqslant 0}) = \sum_{i=0}^{n-1} p^i (x_n^{(i)})^{p^{n-i}} + p^n\mathcal{O}_K$$

für alle $n \in \mathbb{N}$. Damit gilt

$$\tilde{\vartheta}([(\alpha_i^{(0)})_{i\geqslant 0}]) + p^n\mathcal{O}_K = (x_n^{(0)})^{p^n} + p^n\mathcal{O}_K = ((\alpha_i^{(0)})_{i\geqslant 0})^{\#} + p^n\mathcal{O}_K \tag{21}$$

für alle $n \in \mathbb{N}$. Dazu wird noch gezeigt, warum $(x_n^{(0)})^{p^n} + p^n\mathcal{O}_K = ((\alpha_i^{(0)})_{i\geqslant 0})^{\#} + p^n\mathcal{O}_K$ ist. Für $\#$ gilt $((\alpha_i^{(0)})_{i\geqslant 0})^{\#} = \lim_{i\to\infty} (x_i^{(0)})^{p^i}$. Die Folge $((x_i^{(0)})^{p^i} - (x_n^{(0)})^{p^n})_{i\geqslant 0}$ liegt in $p^n\mathcal{O}_K$ und ist eine Nullfolge, denn für $m > n$ gilt

$$(x_m^{(0)})^{p^m} - (x_n^{(0)})^{p^n} = ((x_m^{(0)})^{p^{m-n}})^{p^n} - (x_n^{(0)})^{p^n} \in p^{n+1}\mathcal{O}_K \subseteq p^n\mathcal{O}_K,$$

da für Elemente $(\alpha_i^{(0)})_{i\geqslant 0} \in \mathcal{O}_{K^\flat}$ gilt $(x_m^{(0)})^{p^{m-n}} - x_n^{(0)} \in p\mathcal{O}_K$ und wegen 1.1.2 ist $((x_m^{(0)})^{p^{m-n}})^{p^n} - (x_n^{(0)})^{p^n} \in p^{n+1}\mathcal{O}_K$.

Da (21) für alle $n \in \mathbb{N}$ gilt, ist $\vartheta \circ [\cdot] = (\cdot)^{\#}$.

ii) Sei $x \in \mathcal{O}_K$. Die Abbildung $\mathcal{O}_{K^\flat} \to \mathcal{O}_K/p\mathcal{O}_K, \quad (\alpha_i)_{i\geqslant 0} \mapsto \alpha_0$ surjektiv, also gibt es ein $y_0 \in \mathcal{O}_{K^\flat}$ mit 0-ter Komponente $x + p\mathcal{O}_K$. Da $x + p\mathcal{O}_K = y_0^{\#} + p\mathcal{O}_K$ wegen 2.2 ii), gilt $x - y_0^{\#} \in p\mathcal{O}_K$ und es gibt ein $x_1 \in \mathcal{O}_K$ mit $x - y_0^{\#} = px_1$. Ebenso gibt es $y_1 \in \mathcal{O}_{K^\flat}$ und $x_2 \in \mathcal{O}_K$ mit $x_1 - y_1^{\#} = px_2$. Somit kann man rekursiv $x_n - y_n^{\#} = px_{n+1}$ für alle $n \in \mathbb{N}$ definieren. Also folgt $x - \sum_{i=0}^n p^i y_i^{\#} = p^{n+1}x_{n+1}$ für alle $n \in \mathbb{N}$. Damit ist

$$x = \sum_{i=0}^{\infty} p^i y_i^{\#} \overset{i)}{=} \sum_{i=0}^{\infty} p^i \vartheta([y_i]) \overset{1.5.5}{=} \vartheta(\sum_{i=0}^{\infty} p^i [y_i]).$$

iii) & iv) Zunächst wird gezeigt, dass ein primitives Element $z \in W(\mathcal{O}_{K^\flat})$ existiert, welches in $\ker(\vartheta)$ liegt. Es gibt ein $\overline{z} \in \mathcal{O}_{K^\flat}$ mit $|\overline{z}|_\flat = p^{-1}$, da nach 2.3 ii) die Gleichung $|\mathcal{O}_K| = |\mathcal{O}_{K^\flat}|_\flat$ gilt. Damit ist $\vartheta([\overline{z}]) = \overline{z}^{\#} \in p\mathcal{O}_K^{\times}$, da $|\overline{z}^{\#}| = |\overline{z}|_\flat = p^{-1} = |p|$ ist. Da ϑ surjektiv ist, gibt es ein $z_1 \in W(\mathcal{O}_{K^\flat})$ mit $\vartheta(z_1) = -\overline{z}^{\#}p^{-1} \in \mathcal{O}_K^{\times}$. Das Element $z := [\overline{z}] + pz_1$ liegt in $\ker(\vartheta)$. Als nächstes ist zu zeigen, dass z primitiv ist. Seien dazu $x_n \in \mathcal{O}_{K^\flat}$ die eindeutig bestimmten Elemente mit $z_1 = \sum_{n=0}^{\infty} p^n[x_n]$. Dann gilt für $\vartheta(z_1) \in \mathcal{O}_K^{\times}$, dass $\vartheta(z_1) = \sum_{n=0}^{\infty} p^n x_n^{\#} = x_0^{\#} + p\sum_{n=1}^{\infty} p^{n-1}x_n^{\#}$ ist. Damit ist $x_0^{\#} \in \mathcal{O}_K^{\times} = \mathcal{O}_K \backslash p\mathcal{O}_K$, da $p\sum_{n=1}^{\infty} p^{n-1}x_n^{\#} \in p\mathcal{O}_K$ und $\vartheta(z_1) \in \mathcal{O}_K^{\times} = \mathcal{O}_K \backslash p\mathcal{O}_K$. Dies impliziert $x_0 \in \mathcal{O}_{K^\flat}^{\times}$, da $|x_0|_\flat = |x_0^{\#}| = 1$ ist. Nach 4.1 i) gilt $z_1 \in W(\mathcal{O}_{K^\flat})$, sodass z per Definition primitiv ist.

Sei nun $z' = (z_0', z_1', \ldots) \in \ker(\vartheta)$ mit $|z_0'|_\flat = p^{-1}$. Zunächst wird die Inklusion $\ker(\vartheta) \subseteq z'W(\mathcal{O}_{K^\flat}) + pW(\mathcal{O}_{K^\flat})$ gezeigt. Sei dazu $y = \sum_{n=0}^{\infty} p^n[x_n] \in \ker(\vartheta)$. Dann ist $x_0^{\#} = -p\sum_{n=1}^{\infty} p^{n-1}x_n^{\#} \in p\mathcal{O}_K$ und somit $|x_0|_\flat = |x_0^\#| \leqslant p^{-1} = |z_0'|_\flat$, also $x_0 \in z_0'\mathcal{O}_{K^\flat}$. Sei $\overline{w} \in \mathcal{O}_{K^\flat}$ mit $x_0 = \overline{w}z_0'$. Damit ist wegen 3.11 ii) $y - [\overline{w}]z' = (x_0, \ldots) - (\overline{w}z_0', \ldots) = (0, \ldots) \in pW(\mathcal{O}_{K^\flat})$ und somit liegt y in $pW(\mathcal{O}_{K^\flat}) + z'W(\mathcal{O}_{K^\flat})$. Nun wird $\ker(\vartheta) = z'W(\mathcal{O}_{K^\flat})$ gezeigt. Sei $y_0 = z'w_0 + py_1 \in \ker(\vartheta)$ mit $y_1, w_0 \in W(\mathcal{O}_{K^\flat})$. Es gilt $p\vartheta(y_1) = \vartheta(py_1) = \vartheta(y_0 - z'w_0) = 0$ und somit $y_1 \in \ker(\vartheta) \subseteq (p, z)$, da $\mathcal{O}_K$ ein Integritätsbereich und $char(\mathcal{O}_K) = 0$ ist. Nun werden $w_n \in W(\mathcal{O}_{K^\flat})$ und $y_{n+1} \in \ker(\vartheta)$ rekursiv mit $y_n = z'w_n + py_{n+1}$ definiert. Damit ist $\sum_{n=0}^{\infty} p^n w_n \in W(\mathcal{O}_{K^\flat})$ und $y_0 - z' \sum_{i=0}^{n} p^i w_i = p^{n+1} y_{n+1}$ für alle $n \in \mathbb{N}$. Folglich liegt $y_0 = z' \sum_{i=0}^{\infty} p^i w_i$ in $z'W(\mathcal{O}_{K^\flat})$. □

In 5.1 iv) wurde ein primitives Element $z \in W(\mathcal{O}_{K^\flat})$ konstruiert mit $\ker(\vartheta) = zW(\mathcal{O}_{K^\flat})$. Tatsächlich ist jedes $z' = (z_0', z_1', \ldots) \in \ker(\vartheta)$ mit $|z_0'|_\flat = p^{-1}$ automatisch primitiv. Sei dazu $z' = [z_0'] + pz''$ für ein geeignetes Element $z'' = (z_0'', z_1'', \ldots) \in W(\mathcal{O}_{K^\flat})$. Wegen $\vartheta(z') = 0 = (z_0')^\# + p\sum_{i=0}^{\infty} p^i (z_i'')^\#$ gilt $p(z_0'')^\# = -(z_0')^\# - p\sum_{i=1}^{\infty} p^i (z_i'')^\#$. Da $p\sum_{i=1}^{\infty} p^i (z_i'')^\#$ in $p^2\mathcal{O}_K$ liegt, folgt wegen der starken Dreiecksungleichung $p^{-1}|z_0''|_\flat = |(z_0')^\#| = p^{-1}$ und somit $z_0'' \in \mathcal{O}_{K^\flat}^\times$, also $z'' \in W(\mathcal{O}_{K^\flat})$.

Korollar 5.2
Sei F ein perfektoider Körper mit $char(F) = p$, $z \in W(\mathcal{O}_F)$ ein primitives Element und $K = Quot(W(\mathcal{O}_F)/zW(\mathcal{O}_F))$, wie in 4.11 mit dem isometrischen Isomorphismus $\psi : F \to K^\flat$. Dann ist die Hintereinanderausführung $W(\mathcal{O}_F) \underset{\sim}{\overset{W(\psi)}{\to}} W(\mathcal{O}_{K^\flat}) \xrightarrow{\vartheta} \mathcal{O}_K$ die natürliche Restklassenabbildung $y \mapsto y + zW(\mathcal{O}_F)$.

Beweis: Da es für $y \in W(\mathcal{O}_F)$ eine Darstellung $y = \sum_{n=0}^{\infty} p^n [y_n]$ gibt und $\vartheta \circ W(\psi)$ ein Homomorphismus ist und somit p-adisch stetig, genügt es die Aussage für Teichmüllerrepräsentanten zu beweisen. Sei $y \in \mathcal{O}_F$. Dann ist $W(\psi)([y]) = (\psi(y), 0, \ldots) = [\psi(y)] \in W(\mathcal{O}_{K^\flat})$, wobei $\psi : \mathcal{O}_F \xrightarrow{\sim} \mathcal{O}_{K^\flat},\ \ y \mapsto ([y^{p^{-n}}] + zW(\mathcal{O}_F) + p\mathcal{O}_K)_{n \geqslant 0}$. Damit ist

$$\begin{aligned} \vartheta \circ W(\psi)([y]) &= \vartheta([\psi(y)]) = \psi(y)^\# = \lim_{n\to\infty} ([y^{p^{-n}}]^{p^n} + zW(\mathcal{O}_F)) \\ &= \lim_{n\to\infty} ([y] + zW(\mathcal{O}_F)) = [y] + zW(\mathcal{O}_F). \end{aligned}$$

□

Korollar 5.3
Sei $z \in W(\mathcal{O}_{K^\flat})$ ein primitives Element mit $\ker(\vartheta) = zW(\mathcal{O}_{K^\flat})$. Dann ist der durch ϑ induzierte Ringisomorphismus $\overline{\vartheta} : W(\mathcal{O}_{K^\flat})/zW(\mathcal{O}_{K^\flat}) \to \mathcal{O}_K$ eine Isometrie bzgl. $|\cdot|_K$ auf $W(\mathcal{O}_{K^\flat})/zW(\mathcal{O}_{K^\flat})$, wie von 4.11.

Beweis: Sei $x \in W(\mathcal{O}_{K^\flat})$. Nach 4.8 existiert ein stabiles Element $y = \sum_{n=0}^{\infty} p^n [y_n] \in W(\mathcal{O}_{K^\flat})$ mit $x - y \in zW(\mathcal{O}_{K^\flat})$. Damit ist $|y_n|_\flat \leqslant |y_0|_\flat$ für alle $n \in \mathbb{N}$. Nach 4.11 ist $|x + zW(\mathcal{O}_{K^\flat})|_K := |y + zW(\mathcal{O}_{K^\flat})|_K = \sup_{n \geqslant 0} |y_n|_\flat = |y_0|_\flat = |y_0^\#|$. Ist $y_0 \neq 0$, so ist für alle $n \geqslant 0$ $\frac{y_n}{y_0} \in \mathcal{O}_{K^\flat}$. Damit ist $y = \sum_{n=0}^{\infty} p^n [y_n] = [y_0] \sum_{n=0}^{\infty} p^n [\frac{y_n}{y_0}] = [y_0]u$ mit $u := \sum_{n=0}^{\infty} p^n [\frac{y_n}{y_0}] \in W(\mathcal{O}_{K^\flat})^\times$ und es gilt $\vartheta(y) = \vartheta([y_0])\vartheta(u) = y_0^\# \vartheta(u)$ mit $\vartheta(u) \in \mathcal{O}_K^\times$. Der Homomorphismus ϑ ist eine Isometrie, da $x - y \in zW(\mathcal{O}_F) = \ker(\vartheta)$ und

$$|x + zW(\mathcal{O}_{K^\flat})|_K = |y_0^\#| = |y_0^\#||\vartheta(u)| = |\vartheta(y)| = |\vartheta(x - (x - y))| = |\vartheta(x)|.$$

□

Lemma 5.4
Sei $(F, |\cdot|)$ ein perfektoider Körper mit $char(F) = p$ und $E|F$ eine endliche Körpererweiterung. Dann ist auch E ein perfektoider Körper.

Beweis: Da F vollständig ist, gibt es nach 1.4.10 eine eindeutige Fortsetzung des Absolutbetrags auf E und E ist diesbezüglich vollständig. Zur Vereinfachung wird die Fortsetzung ebenfalls mit $|\cdot|$ bezeichnet. Die Menge $|E|$ liegt dicht in $\mathbb{R}_{\geqslant 0}$, da $|F| \subseteq |E|$ und $|F|$ in $\mathbb{R}_{\geqslant 0}$ dicht liegt. F ist perfekt, da der Frobenius auf $\mathcal{O}_F$ surjektiv ist. Für endliche Körpererweiterungen perfekter Körper gilt, dass diese ebenfalls perfekt sind. Also ist der Frobenius auf $\mathcal{O}_E$ surjektiv. □

Lemma 5.5
Sei K ein perfektoider Körper der Charakteristik 0 und sei $z \in W(\mathcal{O}_{K^\flat})$ ein primitives Element mit $zW(\mathcal{O}_{K^\flat}) = \ker(\vartheta)$, welches nach 5.1 iii) existert. Seien ferner $E'|K^\flat$ eine endliche Körpererweiterung,
$\mathcal{O}_E := W(\mathcal{O}_{E'})/zW(\mathcal{O}_{E'})$ und $E := \mathcal{O}_E[\frac{1}{p}]$. Dann ist E über $\mathcal{O}_K \overset{\overline{\vartheta}}{\cong} W(\mathcal{O}_{K^\flat})/zW(\mathcal{O}_{K^\flat}) \hookrightarrow \mathcal{O}_E$ eine Körpererweiterung von K mit $[E : K] = [E' : K^\flat]$. Darüberhinaus ist E selbst perfektoid mit einem isometrischen Isomorphismus $E^\flat \cong E'$.

Beweis: Ein Element $z \in W(\mathcal{O}_{K^\flat}) \subseteq W(\mathcal{O}_{E'})$, welches in $W(\mathcal{O}_{K^\flat})$ primitiv ist, ist auch in $W(\mathcal{O}_{E'})$ primitiv. Damit ist $\mathcal{O}_E = W(\mathcal{O}_{E'})/zW(\mathcal{O}_{E'})$ der Bewertungsring eines perfektoiden Körpers E mit $char(E) = 0$, da E' nach 5.4 ein perfektoider Körper ist und somit nach 4.11 iv) auch E. Nun ist zu zeigen, dass E ein Oberkörper von K ist.
Der Ringhomomorphismus $W(\mathcal{O}_{K^\flat}) \hookrightarrow W(\mathcal{O}_{E'})$ mit der komponentenweise Inklusionabbildung $\mathcal{O}_{K^\flat} \hookrightarrow \mathcal{O}_{E'}$ induziert einen Ringhomomorphismus

$$\mathcal{O}_K \cong W(\mathcal{O}_{K^\flat})/zW(\mathcal{O}_{K^\flat}) \xrightarrow{\Omega} W(\mathcal{O}_{E'})/zW(\mathcal{O}_{E'}) = \mathcal{O}_E. \tag{22}$$

Da $\mathcal{O}_E$ nullteilerfrei ist, ist der Kern von Ω ein Primideal. Die einzigen Primideale in $\mathcal{O}_K$ sind das Nullideal und das maximale Ideal. Angenommen es gilt $\ker(\Omega) = \mathfrak{m}$. Da $p \in \mathfrak{m}$ ist, gilt $\Omega(p) = p\Omega(1_K) = p1_E = 0$. Dies ist aber ein Widerspruch zu $char(E) = 0$. Daher ist Ω injektiv E ist ein Oberkörper von K.
Als nächstes wird $[E : K] = [E' : K^\flat]$ gezeigt. Da $K^\flat$ perfekt ist, ist $E'|K^\flat$ separabel. Sei $E''|K^\flat$ der Galoisabschluss von E' in $(K^\flat)^{sep}$, d.h. E'' sei die kleinste Galoiserweiterung, die E' enthält. Dann ist $\mathcal{O}_L := W(\mathcal{O}_{E''})/zW(\mathcal{O}_{E''})$ wie oben der Bewertungsring eines perfektoiden Oberkörpers L von E und insbesondere von K. Sei $G := Gal(E''|K^\flat)$. Dann operiert G auf $W(\mathcal{O}_{E''})$ durch $y \mapsto W(\sigma)(y)$ für alle $\sigma \in G, y \in W(\mathcal{O}_{E''})$ und es gilt $W(\mathcal{O}_{E''})^G = W(\mathcal{O}_{K^\flat})$. Insbesondere gilt $W(\sigma)(z) = z$. Dies induziert eine Operation von G auf $\mathcal{O}_L = W(\mathcal{O}_{E''})/zW(\mathcal{O}_{E''})$ durch $x + zW(\mathcal{O}_{E''}) \mapsto W(\sigma)(x) + zW(\mathcal{O}_{E''})$ für alle $\sigma \in G, x \in W(\mathcal{O}_{E''})$.
Als nächstes wird gezeigt, dass für jede Untergruppe $H \subseteq G$ die Isomorphie

$$L^H \cong (W(\mathcal{O}_{(E'')^H})/zW(\mathcal{O}_{(E'')^H}))[\frac{1}{p}] \tag{23}$$

gilt. Da $E''|E''^H$ eine endliche Körpererweiterung perfektoider Körper der Charakteristik p ist, gilt wie in (22) die Injektivität der entsprechenden Abbildung$W(\mathcal{O}_{(E'')^H})/zW(\mathcal{O}_{(E'')^H}) \overset{\Omega'}{\hookrightarrow} W(\mathcal{O}_{E''})/zW(\mathcal{O}_{E''}) = \mathcal{O}_L$. Da H auf $W(\mathcal{O}_{(E'')^H})/zW(\mathcal{O}_{(E'')^H})$ trivial operiert, gilt

$$W(\mathcal{O}_{(E'')^H})/zW(\mathcal{O}_{(E'')^H}) = (W(\mathcal{O}_{(E'')^H})/zW(\mathcal{O}_{(E'')^H}))^H \overset{\Omega'}{\hookrightarrow} \mathcal{O}_L^H,$$

und somit

$$(W(\mathcal{O}_{(E'')^H})/zW(\mathcal{O}_{(E'')^H}))[\frac{1}{p}] \overset{\Omega'}{\hookrightarrow} \mathcal{O}_L^H[\frac{1}{p}] = L^H.$$

Um die letzte Gleichheit einzusehen, sei $x \in L^H \subseteq L$. Dann gibt es $n \in \mathbb{N}$ und $y \in \mathcal{O}_L$ mit $x = p^{-n}y$. Dann muss $y \in \mathcal{O}_L^H$ sein, da $\sigma(p^{-n}) = p^{-n}$ für alle $\sigma \in G$ ist, also insbesondere auch für alle $\sigma \in H$. Außerdem ist $\mathcal{O}_L$ ein Integritätsbereich.
Um (23) zu beweisen, genügt es zu zeigen, dass y in $(W(\mathcal{O}_{(E'')^H})/zW(\mathcal{O}_{(E'')^H}))[\frac{1}{p}]$ liegt. Sei $y' \in W(\mathcal{O}_{E''})$ mit $y = y' + zW(\mathcal{O}_{E''})$ und $\widetilde{y'} := \sum_{\sigma\in H} W(\sigma)(y') \in W(\mathcal{O}_{E''})$. Dann gilt $W(\sigma)(\widetilde{y'}) = \widetilde{y'}$ für alle $\sigma \in H$ und somit ist $\widetilde{y'} \in W(\mathcal{O}_{(E'')^H}) = W(\mathcal{O}_{E''})^H$. Damit ist

$$ord(H)y \quad = \quad \textstyle\sum_{\sigma\in H} W(\sigma)(y') + zW(\mathcal{O}_{E''}) = \widetilde{y'} + zW(\mathcal{O}_{E''}) \in W(\mathcal{O}_{(E'')^H})/zW(\mathcal{O}_{(E'')^H})$$

und somit

$$y = \frac{1}{ord(H)}(\widetilde{y'} + zW(\mathcal{O}_{(E'')^H})) \in (W(\mathcal{O}_{(E'')^H})/zW(\mathcal{O}_{(E'')^H}))[\frac{1}{p}] \cong L^H.$$

Im Folgenden wird gezeigt, dass

$$\begin{array}{rcl} Gal(E''|K^\flat) & \to & Gal(L|K) \\ \sigma & \mapsto & \sigma^\# \end{array} \tag{24}$$

ein Gruppenisomorphismus ist mit $\sigma^\#(x + zW(\mathcal{O}_{E''})) := W(\sigma) + zW(\mathcal{O}_{E''})$, wie zuvor. Dazu betrachtet man den Gruppenhomomorphismus

$$\begin{array}{rcl} Gal(L|K) & \to & Gal(L^\flat|K^\flat) \\ \sigma & \mapsto & \sigma^\flat \end{array}$$

mit $\sigma^\flat((\alpha_n + p\mathcal{O}_L)_{n\geqslant 0}) := (\sigma(\alpha_n) + p\mathcal{O}_L)_{n\geqslant 0}$ für alle $(\alpha_n + p\mathcal{O}_L)_{n\geqslant 0} \in \mathcal{O}_{L^\flat}$. Mit der Isomorphie $L^\flat \cong E''$ aus 4.11 vii) lässt sich zeigen, dass die Hintereinanderausführungen beider Homomorphismen jeweils Identitäten sind. Sei dazu der Isomorphismus

$$\begin{array}{rcccccl} \varphi: & \mathcal{O}_{E''} & \overset{\omega}{\to} & \varprojlim_{x\mapsto x^p} \mathcal{O}_{E''}/\overline{z}\mathcal{O}_{E''} & \to & \varprojlim_{x\mapsto x^p} \mathcal{O}_L/z\mathcal{O}_L = \mathcal{O}_{L^\flat} \\ & x & \mapsto & (x^{p^{-n}} + \overline{z}\mathcal{O}_{E''})_{n\geqslant 0} & \mapsto & ([x^{p^{-n}}] + zW(\mathcal{O}_{E''}) + (p))_{n\geqslant 0} \end{array}$$

wie im Beweis von 4.11 vii). Zunächst wird gezeigt, dass

$$Gal(L^\flat|K^\flat) \to Gal(L|K) \to Gal(L^\flat|K^\flat)$$

mit obigen Gruppenhomomorphismen die Identität ist. Sei $\sigma \in G$ und $x \in \mathcal{O}_{E''}$. Dann ist

$$\begin{array}{rcl} \varphi(\sigma(x)) & = & ([\sigma(x)^{p^{-n}}] + zW(\mathcal{O}_{E''}) + (p))_{n\geqslant 0} = (\sigma^\#([x^{p^{-n}}] + zW(\mathcal{O}_{E''})) + (p)))_{n\geqslant 0} \\ & = & (\sigma^\#)^\flat(([x^{p^{-n}}] + zW(\mathcal{O}_{E''}) + (p))_{n\geqslant 0}) = (\sigma^\#)^\flat(\varphi(x)). \end{array}$$

Identifiziert man also $L^\flat$ mit E'', folgt $\sigma = (\sigma^\#)^\flat$ für alle $x \in L^\flat$. Damit ist (24) ein injektiver Gruppenhomomorphismus und $G = Gal(E''|K^\flat)$ kann als Untergruppe von $Aut(L|K)$ aufgefasst werden. Die Körpererweiterung $L|L^G$ ist Galois. Da $(E'')^G = K^\flat$ und nach (23)

$$L^G = (W(\mathcal{O}_{(E'')^G})/zW(\mathcal{O}_{(E'')^G}))[\frac{1}{p}] = (W(\mathcal{O}_{K^\flat})/zW(\mathcal{O}_{K^\flat}))[\frac{1}{p}] = \mathcal{O}_K[\frac{1}{p}] = K$$

ist, ist $L|K$ eine endliche Galoiserweiterung mit $[L : K] = ord(G) = [E'' : K^\flat]$. Der Gruppenhomomorphismus (24) ist also bijektiv.
Für $H := Gal(E''|E')$ gilt

$$L^H = (W(\mathcal{O}_{(E''))^H})/zW(\mathcal{O}_{(E'')^H}))[\frac{1}{p}] = (W(\mathcal{O}_{E'})/zW(\mathcal{O}_{E'}))[\frac{1}{p}] = \mathcal{O}_E[\frac{1}{p}] = E,$$

sodass auch $L|E$ eine endliche Galoiserweiterung mit $[L : E] = ord(H)$ ist. Insgesamt folgt

$$[E : K] = \frac{[L : K]}{[L : E]} = \frac{ord(G)}{ord(H)} = \frac{[E'' : K^\flat]}{[E'' : E']} = [E' : K^\flat].$$

□

Theorem 5.6
Sei K ein perfektoider Körper der Charakteristik 0. Dann gilt

i) Jeder endliche Erweiterungskörper E von K ist ebenfalls perfektoid.

ii) Die Abbildung

$$\begin{array}{rcl} \{E : E|K \, \textit{endl. Körpererw.}\} & \mapsto & \{E' : E'|K^\flat \, \textit{endl. Körpererw.}\} \\ E & \mapsto & E^\flat \end{array}$$

ist Grad erhaltend und bijektiv.

iii) Ist $E|K$ eine endliche Körpererweiterung, so ist $E|K$ genau dann eine Galoiserweiterung, wenn $E^\flat|K^\flat$ eine Galoiserweiterung. In diesem Fall ist

$$\begin{array}{rcl} Gal(E|K) & \to & Gal(E^\flat|K^\flat) \\ \sigma & \mapsto & \sigma^\flat \end{array}$$

ein Isomorphismus von Gruppen.

Beweis: Um das Theorem zu beweisen, wird zunächst gezeigt, dass

$$\widetilde{E} := \bigcup_{E'|K^\flat \text{ endl.}} (W(\mathcal{O}_{E'})/zW(\mathcal{O}_{E'}))[\frac{1}{p}] = \overline{K}$$

gilt, wobei $z \in W(\mathcal{O}_{K^\flat}) = \ker(\vartheta)$ ein primitives Element in $W(\mathcal{O}_{K^\flat})$ ist mit $zW(\mathcal{O}_{K^\flat}) = \ker(\vartheta)$. Dabei ist ϑ wie in 5.1 gewählt. Nach 1.4.15 ist $M' := \widehat{\overline{K^\flat}}$ algebraisch abgeschlossen. Sei $M := W(\mathcal{O}_{M'})/zW(\mathcal{O}_{M'})[\frac{1}{p}]$. Nach 2.9 und den Argumenten am Anfang des Beweises von 5.5 ist M ein perfektoider Oberkörper von $K = W(\mathcal{O}_{K^\flat})/zW(\mathcal{O}_{K^\flat})[\frac{1}{p}]$. Nach 5.5 gilt $M^\flat \cong M'$. Darüberhinaus ist wegen 2.10 M algebraisch abgeschlossen. $\widetilde{E}$ liegt in M, da $W(\mathcal{O}_{E'_1})/zW(\mathcal{O}_{E'_1})$ und $W(\mathcal{O}_{E'_2})/zW(\mathcal{O}_{E'_2})$ in $W(\mathcal{O}_{E'_1E'_2})/zW(\mathcal{O}_{E'_1E'_2})$ liegen. Nun wird gezeigt, dass $\widetilde{E}$ in M dicht liegt.

Seien dazu $\sum_{n=0}^{\infty} p^n[y_{n,0}] + zW(\mathcal{O}_{M'}) \in \mathcal{O}_M$, $y_0 := \sum_{n=0}^{\infty} p^n[y_{n,0}]$ und $\epsilon > 0$. Nach 4.11 ist $0 < |p + zW(\mathcal{O}_{M'})|_M < 1$. Damit existiert ein $N \in \mathbb{N}$ mit $|p^N + zW(\mathcal{O}_{M'})|_M < p^{-N}$ und $\epsilon < p^{-N}$. Da $\mathcal{O}_{\overline{K^\flat}}$ dicht in $\mathcal{O}_{\widehat{\overline{K^\flat}}}$ liegt, gibt es ein $y_0' \in \mathcal{O}_{\overline{K^\flat}}$ mit $|y_{0,0} - y_0'|_\flat \leqslant p^{-N}$. Damit ist $y - [y_0'] = (y_{0,0} - y_0', \ldots)$ und somit $y - [y_0'] - [y_{0,0} - y_0'] \in pW(\mathcal{O}_{M'})$. Sei $y_1 = \sum_{n=0}^{\infty} p^n[y_{n,1}] \in W(\mathcal{O}_{M'})$ mit $y - [y_0'] - [y_{0,0} - y_0'] = py_1$. Entsprechen werden y_1' und y_2 konstruiert mit $|y_{0,1} - y_1'|_\flat < p^{-N}$ und $y_1 - [y_1'] - [y_{0,1} - y_1'] = py_2 \in pW(\mathcal{O}_{M'})$. Auf diese Weise werden $y_0', \ldots, y_{N-1}' \in \mathcal{O}_{\overline{K^\flat}}$, $y_0, \ldots, y_N \in W(\mathcal{O}_{M'})$ rekursiv konstruiert, sodass für $y_i = \sum_{n=0}^{\infty} p^n[y_{n,i}]$ die Abschätzung $|y_{0,i} - y_i'|_\flat < p^{-N}$ und $y - \sum_{j=0}^{i} p^j[y_j'] = \sum_{j=0}^{i} p^j[y_{0,j} - y_j'] + p^{i+1}y_{i+1}$ gilt. Sei $x := \sum_{j=0}^{N-1} p^j[y_j'] \in W(\mathcal{O}_{K^\flat(y_0', \ldots, y_{N-1}')})$, wobei $K^\flat(y_0', \ldots, y_{N-1}')|K^\flat$ endlich ist, da $y_0', \ldots, y_{N-1}' \in \overline{K^\flat}$. Damit ist $x + W(\mathcal{O}_{K^\flat(y_0', \ldots, y_{N-1}')}) \in \widetilde{E}$. Es gilt $y - x = \sum_{j=0}^{N-1} p^j[y_{0,j} - y_j'] + p^N y_N$. Nach 4.8 gibt es ein stabiles Element $\rho = \sum_{n=0}^{\infty} p^n[x_n] \in W(\mathcal{O}_{M'})$ mit $\rho - \sum_{j=0}^{N-1} p^j[y_{0,j} - y_j'] \in zW(\mathcal{O}_{M'})$. Im Beweis von 4.8 ist zu sehen, dass für dieses konstruierte ρ die Abschätzung

$$|\sum_{j=0}^{N-1} p^j[y_{0,j} - y_j'] + zW(\mathcal{O}_{M'})|_M = |\rho| \leqslant \sup_{n \in \{0, \ldots, N-1\}} |y_{0,n} - y_n'|_\flat < p^{-N}$$

gilt. Es ergibt sich

$$\begin{aligned} & |(y + zW(\mathcal{O}_{M'})) - (x + zW(\mathcal{O}_{M'})|_M = |(y - x) + zW(\mathcal{O}_{M'})|_M \\ = \; & |(\sum_{j=0}^{N-1} p^j[y_{0,j} - y_j'] + zW(\mathcal{O}_{M'})) + (p^N y_N + zW(\mathcal{O}_{M'}))|_M \\ \leqslant \; & \max\{|\sum_{j=0}^{N-1} p^j[y_{0,j} - y_j'] + zW(\mathcal{O}_{M'})|_M, |p^N(y_N + zW(\mathcal{O}_{M'}))|_M\} < p^{-N} < \epsilon. \end{aligned}$$

Das zeigt, dass $\widetilde{E}$ dicht in M liegt. Nach 1.3.10 ist $\widehat{\widetilde{E}} \cong \widehat{M} = M$. Da M algebraisch abgeschlossen ist, ist $\widetilde{E}$ nach 1.4.16 separabel abgeschlossen. $\widetilde{E}$ ist darüberhinaus sogar algebraisch abgeschlossen, da $char(\widetilde{E}) = 0$ ist. Also ist $\widetilde{E} = \overline{K}$.

i) Sei $E|K$ eine endliche Körpererweiterung und $E_1|K$ eine endliche Körpererweiterung mit $E \subseteq E_1$ und $\mathcal{O}_{E_1} = W(\mathcal{O}_{E_1'})/zW(\mathcal{O}_{E_1'})$ für eine endliche Körpererweiterung $E_1'|K^\flat$. Dies ist möglich, da nach den obigen Vorüberlegungen $\mathcal{O}_{\overline{K}} = \bigcup_{E'|K^\flat \text{ endl.}} W(\mathcal{O}_{E'})/zW(\mathcal{O}_{E'})$ ist. Sei o.B.d.A. $E_1'|K^\flat$ eine endliche Galoiserweiterung. Nach 5.5 ist $ord(Gal(E_1'|K^\flat)) = [E_1'|K^\flat] = [E_1|K]$. Im Beweis von 5.5 war zu sehen, dass $Gal(E_1'|K^\flat) \cong Gal(E_1|K)$ gilt und dass $E_1|K$ eine Galoiserweiterung ist. Sei $H := Gal(E_1|E) \subseteq Gal(E_1|K) \cong Gal(E_1'|K^\flat)$. Ebenfalls hat man im Beweis von 5.5 gesehen, dass $(W(\mathcal{O}_{(E_1')^H})/zW(\mathcal{O}_{(E_1')^H}))[\frac{1}{p}] = E_1^H = E$ ist. Dieser Körper ist nach 5.5 perfektoid.

ii) Die Umkehrabbildung ist

$$\begin{array}{rcl} \{E' : E'|K^\flat \text{ endl. Körpererw.}\} & \mapsto & \{E : E|K \text{ endl. Körpererw.}\} \\ E' & \mapsto & (W(\mathcal{O}_{E'})/zW(\mathcal{O}_{E'})))[\frac{1}{p}] \end{array} \quad ,$$

denn nach 5.5 gilt für eine endliche Körpererweiterung $E'|K^\flat$, dass $((W(\mathcal{O}_{E'})/zW(\mathcal{O}_{E'}))[\frac{1}{p}])^\flat \cong E'$ ist und nach 5.1 gilt für eine endliche Körpererweiterung $E|K$, dass $(W(\mathcal{O}_{E^\flat})/zW(\mathcal{O}_{E^\flat}))[\frac{1}{p}] \cong E$ ist.

iii) In 5.5 wurde gezeigt, dass $E|K$ eine Galoiserweiterung ist, wenn $E^\flat|K^\flat$ eine Galoiserweiterung ist. Sei $E|K$ eine endliche Galoiserweiterung. Seien ferner E_1 und H wie im Beweis von i). Damit ist H ein Normalteiler in $Gal(E_1|K) \cong Gal(E_1'|K^\flat)$. Daher ist die Körpererweiterung $(E_1')^H = E^\flat|K^\flat$ eine Galoiserweiterung. □

Für einen perfektoiden Körper K der Charakteristik 0 ist der Funktor $(\cdot)^\flat$ nach 2.8 und 5.6 eine Kategorienäquivalenz von der Kategorie der endlichen Körpererweiterungen von K in die Kategorie der Körpererweiterungen von $K^\flat$. Die Morphismen sind jeweils die isometrischen Körperhomomorphismen über K bzw. $K^\flat$. Er schränkt sich zu einer Äquivalenz von Galoiskategorien $\{E|K : E|K \text{ endlich Galoissch}\} \overset{(\cdot)^\flat}{\to} \{E'|K^\flat : E' \text{ endlich Galoissch}\}$ ein. Insbesondere gilt $Gal(E|K) \cong Gal(E^\flat|K^\flat)$ für alle endlichen Galoiserweiterungen $E|K$. Aus dem Hauptsatz der unendlichen Galoistheorie folgt daher:

Korollar 5.7
Ist K ein perfektoider Körper der Charakteristik 0, so sind die absoluten Galoisgruppen von K und $K^\flat$ kanonisch topologisch isomorph:

$$Gal(\overline{K}|K) \cong Gal(\overline{K^\flat}|K^\flat).$$

Der Fall $K = \widehat{\mathbb{Q}_p[\mu_{p^\infty}]}$ in 2.1 i) wurde zuerst von Fontaine und Wintenberger in [2] bewiesen. Die Methoden waren allerdings anders.

Literatur

[1] P. Scholze, Perfectoid Spaces, Publications mathématiques de l'IHÉS, 116, (2012), 245–313

[2] J.M. Fontaine & J.P. Wintenberger, Extensions algebriques et corps des normes des extensions APF des corps locaux, Comptes rendus, série A, 288, (1979), 441-444

[3] P. Schneider, Skript "Galois representations and (φ, Γ)-modules", http://www.math.uni-muenster.de/u/pschnei/publ/lectnotes/phi-Gamma-modules-1.pdf

[4] J. Neukirchen, Algebraische Zahlentheorie, Springer Verlag, (1992)

[5] S. Bosch, Algebra, 8. Auflage, Springer Verlag, (2013)

[6] T. Oertel-Jäger, Skript " Funktionalanalysis ", http://www.math.tu-dresden.de/ enpdyn/funkana.pdf

[7] K.S. Kedlaya, New methods for (φ, Γ)-modules, Mathematical Sciences (2015), 2: 20. doi:10.1186/s40687-015-0031-z

Selbständigkeitserklärung

Hiermit versichere ich, dass ich die vorliegende Masterarbeit selbstständig und nur unter Zuhilfenahme der angegebenen Quellen erstellt habe.

Oberhausen, den 17.12.2016

Katharina Janiszczak