Universität Duisburg-Essen
Fakultät für Mathematik

Masterarbeit

Das explizite Reziprozitätsgesetz von Fontaine-Witt

Julian Wilmer

Matrikelnummer: 2247977

17. Dezember 2015

Betreuer: Herr Prof. Dr. Jan Kohlhaase

Inhaltsverzeichnis

Einleitung

Ziel dieser Arbeit ist es, das von Jean-Marc Fontaine aufgestellte explizite Reziprozitätsgesetz

$$\boxed{[x,u) = Tr_{K|\mathbb{Q}_p}(res(x \cdot d_{log}(Col(u))))}$$

herzuleiten. Dabei ist u eine Einheit in einem lokalen Körper E der Charakteristik $p > 0$ und x ein Element eines geeigneten p-Cohen-Rings $\mathcal{O}_\mathcal{E}$ von E. Auf der rechten Seite der Gleichung wird durch K eine bestimmte unverzweigte Erweiterung der p-adischen Zahlen $\mathbb{Q}_p$ betrachtet und mit *res* bzw. *Col* die Residuenabbildung bzw. der Coleman-Isomorphismus bezeichnet. Es fällt sofort auf, dass hierbei viele Begriffe wie beispielsweise „p-Cohen-Ring“, „unverzweigte Erweiterung“ oder „Coleman-Isomorphismus“ auftauchen, welche nicht direkt zu verstehen sind, aber für das explizite Reziprozitätsgesetz benötigt werden. Aus diesem Grund ist die vorliegende Arbeit im Wesentlichen in zwei Teile aufgeteilt.

Der erste Teil besteht dabei aus den Kapiteln 1 bis 6, in denen essentielle Grundbegriffe erklärt werden, welche für das weitere Verständnis unabdingbar sind. Für die Beweise wird hierbei größtenteils auf die Literatur verwiesen. Dabei wird zunächst die Theorie der diskreten Bewertungsringe und Kohomologiegruppen eingeführt. In Kapitel 3 werden wir sehen, wie jedem 2-Kozyklus eine Azumaya-Algebra zugeordnet werden kann und wir somit eine Isomorphie zwischen der zweiten Kohomologiegruppe einer Körpererweiterung $E'|E$ und der Brauergruppe von Azumaya-Algebren erhalten. Dadurch lässt sich eine Brücke zwischen den Kohomologiegruppen, auf welchen die lokale Klassenkörpertheorie und die Invariantenabbildungen aufbauen, und den Azumaya-Algebren schlagen. Anschließend konstruieren wir in Kapitel 5 den Ring der Wittvektoren $W(B)$ für einen kommutativen Ring B mit Einselement 1_B. Von essentieller Bedeutung wird dabei der diskrete Bewertungsring

$$\mathcal{O}_\mathcal{E} = \left\{ \sum_{n \in \mathbb{Z}} a_n t^n \mid a_n \in W(k), \lim_{n \to -\infty} a_n = 0 \right\}$$

sein, welcher einen p-Cohen-Ring für $E \cong k((t))$ bildet, wobei k ein perfekter Körper der Charakteristik $p > 0$ ist. Abschließend für den ersten Teil gehen wir dann noch etwas genauer auf die Kategorienäquivalenz von Fontaine ein, welche im Wesentlichen aussagt, dass die Kategorie der stetigen $\mathbb{Z}_p$-linearen Darstellungen der Galoisgruppe

$G_E = Gal(E^{sep}|E)$ mit der Kategorie der etalen φ-Moduln über $\mathcal{O}_\mathcal{E}$ übereinstimmt. Da diese Arbeit auf die Vorlesungen „Algebraische Zahlentheorie II“ im Wintersemester 2014/2015 und „p-adic Galois representations“ im Sommersemester 2015 bei Herrn Prof. Dr. Jan Kohlhaase an der Universität Duisburg-Essen aufbaut, in welchen der Großteil der Resultate aus Kapitel 1-6 gezeigt wurde, wird im Folgenden für einen Beweis lediglich auf eine entsprechende Quelle verwiesen.

Der zweite Teil dieser Arbeit besteht darin, mit den Mitteln aus den ersten Kapiteln das explizite Reziprozitätsgesetz herzuleiten, wobei hier alle Beweise vollständig ausgeführt werden. Die Grundlage liefern dafür die Seiten 265-268 der Arbeit „Représentations p-adiques des corps locaux“ [Fo2] von Jean-Marc Fontaine. Dabei greifen wir auf ein wichtiges Resultat von Ernst Witt in seiner Arbeit „Zyklische Körper und Algebren der Charakteristik p vom Grad p^n. Struktur diskret bewerteter perfekter Körper mit vollkommenem Restklassenkörper der Charakteristik p.“ [Wi] zurück, welches die Invariante einer bestimmten Azumaya-Algebra explizit beschreibt. Für einen Körper $E \cong k((t))$ der Charakteristik $p > 0$ mit perfektem Restklassenkörper k werden wir dabei zunächst die Existenz eines Frobenius-Lifts φ auf dem p-Cohen-Ring $\mathcal{O}_\mathcal{E}$ nachweisen. Auf dieser Grundlage konstruieren wir zum einen die Residuenabbildung *res*, die einer sogenannten Differentialform $(\sum_{n\in\mathbb{Z}} a_n t^n) \cdot d_{log}t$ jeweils den Koeffizienten a_0 zuordnet, und zum anderen den Coleman-Isomorphismus $Col\colon E^* \xrightarrow{\sim} (\mathcal{O}_\mathcal{E})^{N_\varphi}$. Mittels der Kategorienäquivalenz von Fontaine entwickeln wir zudem eine Abbildung $\delta_\mathcal{E}$, welche jedem Element von $\mathcal{O}_\mathcal{E}$ einen stetigen Gruppenhomomorphismus von G_E in die ganzen p-adischen Zahlen $\mathbb{Z}_p$ zuordnet. Darauf aufbauend lässt sich die Abbildung

$$[*\,,*)\colon \mathcal{O}_\mathcal{E} \times E^* \to \mathbb{Z}_p,\ (x,u) \mapsto [x\,,u) := (\delta_\mathcal{E}(x))((u\,,E))$$

definieren, wobei $(\cdot\,,E)$ das sogenannte universelle Normrestsymbol bezeichnet. Im letzten Schritt werden wir dann mittels der expliziten Darstellung der Invarianten einer Azumaya-Algebra nach Witt das explizite Reziprozitätsgesetz herleiten.

1 Diskret bewertete Körper

In dem gesamten Kapitel sei durch F ein beliebiger Körper gegeben.

1.1 Diskrete Bewertungsringe

Definition 1.1. Eine *diskrete Bewertung* v auf F ist eine surjektive Abbildung $v\colon F \to \mathbb{Z} \cup \{\infty\}$, sodass für alle $x, y \in F$

(i) $v(x) = \infty \Leftrightarrow x = 0$;

(ii) $v(x) \cdot v(y) = v(x) + v(y)$;

(iii) $v(x + y) \geq \min\{v(x), v(y)\}$.

F nennt man in diesem Fall einen diskret bewerteten Körper.

Definition 1.2. Ein nichtarchimedischer Absolutbetrag auf F ist eine Abbildung $|\cdot|\colon F \to \mathbb{R}_{\geq 0}$, sodass für alle $x, y \in F$

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

(ii) $|x \cdot y| = |x| \cdot |y|$;

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

Bemerkung 1.3. (i) Ist $v\colon F \to \mathbb{Z} \cup \{\infty\}$ eine diskrete Bewertung auf F, so wird für jedes $q \in \mathbb{R}$ mit $q > 1$ durch $|\cdot|\colon F \to \mathbb{R}_{\geq 0}, x \mapsto q^{-v(x)}$ ein nichtarchimedischer Absolutbetrag auf F definiert.

(ii) Aus $v(x \cdot y) = v(x) + v(y)$ in 1.1 folgt, dass $v(-x) = v(x)$ bzw. $v(x^{-1}) = -v(x)$ für alle $x \in F$ bzw. $x \in F^*$.

(iii) Sind $x, y \in F$ mit $v(x) \neq v(y)$, dann ist $v(x + y) = \min\{v(x), v(y)\}$. Denn angenommen $v(x + y) > \min\{v(x), v(y)\}$ und ohne Einschränkung $v(x) > v(y)$, so ist $v(y) = v(x+y-x) \geq \min\{v(x+y), v(x)\} > v(y)$, was offensichtlich ein Widerspruch ist.

Definition 1.4. Ein kommutativer Ring R mit Einselement $1 = 1_R$ heißt diskreter Bewertungsring, falls gilt:

(i) R ist ein Hauptidealring;

(ii) R hat genau ein maximales Ideal $\mathfrak{m} \neq 0$.

Wegen (i) folgt dann, dass ein $\pi \in R$ existiert mit $\mathfrak{m} = \pi \cdot R$. Ein solches Element heißt Uniformisierer des diskreten Bewertungsrings R.

Bemerkung 1.5. Sei (F, v) ein diskret bewerteter Körper, $q \in \mathbb{R}$ mit $q > 1$ und $|\cdot| : F \to \mathbb{R}_{\geq 0}, x \mapsto q^{-v(x)}$, der zugehörige nichtarchimedische Absolutbetrag. Dann ist F zusammen mit $d(x, y) := |x - y|$ ein metrischer Raum und wir können die typischen topologischen Begriffe auf F definieren.

- Eine Folge $(x_n)_{n\geq 1}$ mit Elementen aus F konvergiert gegen ein $x \in F$, falls

$$\forall C \geq 0 \, \exists N \in \mathbb{N} \, \forall n \geq N : v(x - x_n) \geq C.$$

- Eine Folge $(x_n)_{n\geq 1}$ in F heißt Cauchyfolge, falls

$$\forall C \geq 0 \, \exists N \in \mathbb{N} \, \forall n, m \geq N : v(x_n - x_m) \geq C.$$

  Man beachte dabei, dass aufgrund von (iii) in 1.1 dies äquivalent ist zu

$$\forall C \geq 0 \, \exists N \in \mathbb{N} \, \forall n \geq N : v(x_{n+1} - x_n) \geq C.$$

- Auf F wird wie folgt eine Topologie definiert:

$$U \subset F \text{ ist offen } \Leftrightarrow \forall x \in U \, \exists n \in \mathbb{N} : \{y \in F \mid v(x - y) > n\} \subset U.$$

Lemma 1.6. *Sei R ein diskreter Bewertungsring mit maximalem Ideal $\mathfrak{m}$ und Uniformisierer $\pi \in R$. Dann gilt:*

(i) $R^* = R \backslash \mathfrak{m}$;

(ii) Jedes Ideal ungleich Null in R ist von der Form $\pi^n R$ für ein $n \in \mathbb{N}$;

(iii) Die Abbildung $R^* \times \mathbb{N}_0 \to R \backslash \{0\}$, $(u, n) \mapsto u\pi^n$, ist eine Bijektion.

Beweis. Die Inklusion $R^* \subset R \backslash \mathfrak{m}$ ist trivial. Da zudem jedes echte Ideal in einem maximalen Ideal enthalten ist und $\mathfrak{m}$ das einzige maximale Ideal in R ist, ist auch $R \backslash \mathfrak{m} \subset R^*$. Ist $q \in R$ ein Primelement, so ist auch q ein Uniformisierer, da qR ein maximales Ideal in dem Hauptidealring R ist, also $qR = \mathfrak{m} = \pi R$. Damit ist π bis auf Multiplikation mit einer Einheit das einzige Primelement in R. Aufgrund der eindeutigen Primfaktorzerlegung in Hauptidealringen folgt die Behauptung in (iii).
Sei nun schließlich noch $I \neq 0$ ein Ideal in R. Da R ein Hauptidealring ist, existiert ein $a \in R$ mit $I = a \cdot R$. Nach (iii) ist $a = u\pi^n$ für ein $u \in R^*$ und $n \geq 0$. Damit ist $I = aR = u\pi^n R = \pi^n R$. Aufgrund der Bijektivität in (iii) ist zudem $n \geq 0$ eindeutig. □

Definition 1.7. Sei R ein diskreter Bewertungsring und $\pi \in R$ ein Uniformisierer. Nach Lemma 1.6 gibt es für $x \in R\backslash\{0\}$ ein eindeutiges $n \in \mathbb{N}_0$ mit $xR = \pi^n R$. Damit wird durch

$$v: R\backslash\{0\} \to \mathbb{Z},\ x \mapsto v(x) = n,$$

zusammen mit $v(0) := \infty$ eine diskrete Bewertung auf R definiert. Man beachte dabei, dass diese Abbildung unabhängig von der Wahl des Uniformisierers ist, da sich zwei Uniformisierer $\pi, \pi' \in R$ wegen $\pi R = \mathfrak{m} = \pi' R$ nur um eine Einheit unterscheiden.

Bemerkung 1.8. Sei R ein diskreter Bewertungsring, $v: R \to \mathbb{Z} \cup \{\infty\}$ die nach Definition 1.7 zugehörige diskrete Bewertung und $K := Quot(R)$ der Quotientenkörper von R. Nach den Eigenschaften von v ist dann

$$v: K \to \mathbb{R}_{\geq 0},\ \frac{x}{y} \mapsto v(x) - v(y) \text{ für } x \in R, y \in R\backslash\{0\},$$

eine diskrete Bewertung auf K. Außerdem ist

$$\{z \in K \mid v(z) \geq 0\} = \{{}^{x}/_{y} \in K \mid v(x) \geq v(y)\} = \{{}^{x}/_{y} \in K \mid xR \subset yR\} = R.$$

Lemma 1.9. *Sei (F, v) ein diskret bewerteter Körper. Dann ist $\mathcal{O}_F := \{x \in F \mid v(x) \geq 0\}$ ein diskreter Bewertungsring mit maximalem Ideal $\mathfrak{m}_F = \{x \in F \mid v(x) > 0\}$, Einheitengruppe ${\mathcal{O}_F}^* = \{x \in F \mid v(x) = 0\}$ und $Quot(\mathcal{O}_F) = F$. Außerdem stimmt die zu $\mathcal{O}_F$ assoziierte diskrete Bewertung aus Definition 1.7 mit v überein.*

Beweis. Wegen Definition 1.1 (ii) und (iii) ist $\mathcal{O}_F$ ein Ring und $\mathfrak{m}_F$ ein Ideal. Außerdem gilt für $x \in \mathcal{O}_F$:

$$x \in {\mathcal{O}_F}^* \Leftrightarrow \exists y \in \mathcal{O}_F \text{ mit } x \cdot y = 1 \Leftrightarrow v(x) = 0 \Leftrightarrow x \in \mathcal{O}_F\backslash\mathfrak{m}_F.$$

Also ist $\mathfrak{m}_F$ das einzige maximale Ideal in $\mathcal{O}_F$. Ist nun $I \neq 0$ ein Ideal in $\mathcal{O}_F$, so setzen wir $n := \min\{v(a) \mid a \in I\}$ und wählen $a \in I$ mit $v(a) = n$. Nach Wahl von a und n ist dann $I = a \cdot \mathcal{O}_F$ und somit ist $\mathcal{O}_F$ ein Hauptidealring und schließlich sogar ein diskreter Bewertungsring.
Ist nun $a \in \mathcal{O}_F, a \neq 0$ und $\pi \in \mathcal{O}_F$ ein Uniformisierer, so ist nach Lemma 1.6 $a\mathcal{O}_F = \pi^n \mathcal{O}_F$ für ein $n \geq 0$. Damit unterscheiden sich a und π^n nur um eine Einheit und es ist $n = v(\pi^n) = v(a)$. Nach Konstruktion der zu $\mathcal{O}_F$ assoziierten diskreten Bewertung stimmt diese mit v überein.
$Quot(\mathcal{O}_F) = F$ ist trivial, da entweder $x \in \mathcal{O}_F$ oder $x^{-1} \in \mathcal{O}_F$ für alle $x \in F$. □

Definition 1.10. Ein diskreter Bewertungsring (R, v) bzw. ein diskret bewerteter Körper (F, v) heißt vollständig, falls jede Cauchyfolge in R bzw. K einen Grenzwert in R bzw. K besitzt.

Lemma 1.11. *Sei R ein diskreter Bewertungsring, $F = Quot(R)$ und $v: F \to \mathbb{Z} \cup \{\infty\}$ die zugehörige diskrete Bewertung. Dann ist (R, v) vollständig genau dann, wenn (F, v) vollständig ist.*

Beweis. Sei (F,v) vollständig, $(x_n)_n$ eine Cauchyfolge in R und $x \in F$ ein Grenzwert von $(x_n)_n$. Wir müssen nun zeigen, dass x bereits in R liegt, d.h. $v(x) \geq 0$ gilt. Ist $x = 0$, so ist trivialerweise $x \in R$, d.h. wir können ohne Einschränkung $x \neq 0$ annehmen. Damit existiert ein $N \in \mathbb{N}$, sodass $v(x - x_n) > v(x) \in \mathbb{Z}$ für alle $n \geq N$. Zusammen mit der Bemerkung 1.3 (iii) folgt somit

$$v(x) = \min\{v(x), v(x - x_n)\} = v(x - (x - x_n)) = v(x_n) \geq 0 \text{ für alle } n \geq N.$$

Sei nun umgekehrt (R,v) vollständig und $(x_n)_n$ eine Cauchyfolge in F. Damit existiert ein $N \in \mathbb{N}$, sodass $v(x_{n+1} - x_n) \geq 0$ für alle $n \geq N$. Wegen der strengen Dreiecksungleichung folgt damit für alle $n \geq N$:

$$v(x_n) \geq \min\{v(x_n - x_{n-1}), \ldots, v(x_{N+1} - x_N), v(x_N)\} \geq \min\{0, v(x_N)\} =: m \in \mathbb{Z}.$$

Ist nun $\pi \in R$ ein Uniformisierer, so ist wegen $v(\pi^{-m}x_n) = v(x_n) - m \geq 0$ für alle $n \geq N$, $(\pi^{-m}x_n)_{n\geq N}$ eine Folge in R. Außerdem ist $(\pi^{-m}x_n)_{n\geq N}$ eine Cauchyfolge in R, da $(x_n)_{n\geq N}$ eine Cauchyfolge in F ist und $v(\pi^{-m}x_{n+1} - \pi^{-m}x_n) = v(x_{n+1} - x_n) - m$. Also existiert ein $y \in R$ mit $\lim_{n\to\infty} \pi^{-m}x_n = y$. Man sieht dann sofort, dass $\pi^m y \in F$ ein Grenzwert der Folge $(x_n)_n$ ist. □

In einem vollständigen diskret bewertetem Körper F sieht man recht leicht, dass aufgrund der vereinfachten Cauchyfolgen-Eigenschaft eine Reihe $\sum_{n=0}^{\infty} a_n$ in F genau dann konvergiert, wenn die Folge $(a_n)_{n\geq 0}$ eine Nullfolge ist. Da natürlich nicht jeder Körper vollständig ist, geht man häufig zur eindeutigen Vervollständigung über.

Satz 1.12. *Für einen diskret bewerteten Körper (F,v) gibt es einen bis auf isometrische Isomorphie eindeutigen, vollständigen, diskret bewerteten Körper $(\hat{F},\hat{v})$, sodass F dicht in $\hat{F}$ liegt und $\hat{v}_{|_F} = v$. Der Körper $(\hat{F},\hat{v})$ ist die sogenannte Vervollständigung von (F,v).*
Damit hat auch jeder diskrete Bewertungsring (R,v) eine bis auf isometrische Isomorphie eindeutige Vervollständigung $(\hat{R},\hat{v})$ mit den obigen Eigenschaften.

Beweis. Einen Beweis der eindeutigen Vervollständigung findet man in [Lo2] in *§23, Satz 2* auf Seite 63. Dabei sei angemerkt, dass in dem Beweis ein zu v assoziierter Absolutbetrag genommen wird, was aber keinen Unterschied macht. □

Definition 1.13. Sei R ein Ring, M ein R-Modul und $(M_j)_{j\in\mathbb{N}_0}$ eine absteigende Sequenz von R-Untermoduln von M, d.h. M_j ist ein R-Untermodul von M für alle $j \in \mathbb{N}_0$ und $M_0 \supset M_1 \supset M_2 \supset \ldots$. Dann definiert

$$U \subset M \text{ ist offen bzgl. } (M_j)_{j\in\mathbb{N}_0} \Leftrightarrow \forall x \in U\, \exists j \in \mathbb{N}_0 : x + M_j \subset U$$

eine Topologie auf M und es lassen sich die üblichen Konvergenzbegriffe wie z.B. Cauchyfolge und Vollständigkeit auf M einführen.

Bemerkung 1.14. Sei R ein Ring, M ein R-Modul und $I \subset R$ ein zweiseitiges Ideal. Die durch $(I^j M)_{j\in\mathbb{N}_0}$ definierte Topologie auf M wird als I-adische Topologie bezeichnet. Ist (R, v) sogar ein diskreter Bewertungsring mit maximalem Ideal $\mathfrak{m}$, so stimmt die durch v induzierte Topologie auf R mit der $\mathfrak{m}$-adischen Topologie überein.

Satz 1.15. *Sei R ein Ring, M ein R-Modul und $(M_j)_{j\in\mathbb{N}_0}$ eine absteigende Sequenz von R-Untermoduln von M. Man sieht leicht, dass dann*

$$\left((M/M_j)_{j\in\mathbb{N}_0}, (f_{ij}: M/M_j \to M/M_i,\ m + M_j \mapsto m + M_i)_{i\leq j}\right)$$

ein projektives System bildet. Die kanonische R-lineare Abbildung

$$\begin{aligned} g: M &\to \varprojlim_{j\in\mathbb{N}_0} M/M_j = \left\{ (m_j + M_j)_{j\in\mathbb{N}_0} \in \prod_{j\in\mathbb{N}_0} M/M_j \mid \forall\, j \leq i:\ m_j - m_i \in M_j \right\} \\ m &\mapsto (m + M_j)_{j\in\mathbb{N}_0} \end{aligned}$$

ist

(i) injektiv $\Leftrightarrow \bigcap_{j\in\mathbb{N}_0} M_j = 0 \Leftrightarrow$ M ist separiert bzgl. $(M_j)_{j\in\mathbb{N}_0}$;

(ii) surjektiv $\Leftrightarrow$ M ist vollständig bzgl. $(M_j)_{j\in\mathbb{N}_0}$.

Beweis. Zu (i): Nach Definition von g ist $\ker(g) = \bigcap_{j\in\mathbb{N}_0} M_j$, womit bereits die erste Äquivalenz gezeigt wäre. Wir nehmen nun an, dass $\bigcap_{j\in\mathbb{N}_0} M_j = 0$ gilt und wählen $x, y \in M$ mit $x \neq y$. Dann ist $x - y \neq 0$ und es existiert ein $j \in \mathbb{N}_0$ mit $x - y \notin M_j$. Damit sind aber $x + M_j$, $y + M_j$ disjunkte, offene Umgebungen von x bzw. y und deshalb M separiert. Sei umgekehrt nun M separiert und o.B.d.A. $M \neq 0$. Für ein $x \in M$ mit $x \neq 0$ existiert dann eine offene Menge $U \subset M$ mit $0 \in U$ und $x \notin U$. Da $U \subset M$ offen ist, existiert ein $j \in \mathbb{N}_0$ mit $M_j = 0 + M_j \subset U$. Damit ist aber insbesondere $x \notin M_j$ und deshalb $\bigcap_{j\in\mathbb{N}_0} M_j = 0$.

Zu (ii): Wir nehmen zunächst an, dass g surjektiv ist und betrachten eine Cauchyfolge $(x_i)_{i\in\mathbb{N}_0}$ in M. Fixieren wir ein $j \in \mathbb{N}_0$, so existiert ein $N_j \in \mathbb{N}_0$, sodass für alle $n \geq N_j$: $x_n - x_{N_j} \in M_j$. Also wird die Folge $(x_m + M_j)_{m\in\mathbb{N}_0}$ stationär in M/M_j, denn $x_m + M_j = x_{N_j} + M_j$ für alle $m \geq N_j$. Ist zudem $i \leq j$ und $n \geq \max\{N_i, N_j\}$, so gilt:

$$x_{N_j} + M_i \overset{M_j \subset M_i}{=} x_{N_j} + M_j + M_i = x_n + M_j + M_i = x_{N_i} + M_j + M_i = x_{N_i} + M_i.$$

Also ist $y := (x_{N_j} + M_j)_{j\in\mathbb{N}_0}$ ein wohldefiniertes Element von $\varprojlim_{j\in\mathbb{N}_0} M/M_j$. Wegen der Surjektivität von g existiert ein $x \in M$ mit $y = g(x) = (x + M_j)_{j\in\mathbb{N}_0}$, d.h. $x - x_{N_j} \in M_j$ für alle $j \in \mathbb{N}_0$. Wählen wir nun $n \geq N_j$ für ein beliebiges $j \in \mathbb{N}_0$, so folgt: $x - x_n = x - x_{N_j} + x_{N_j} - x_n \in M_j$. Also konvergiert $(x_j)_{j\in\mathbb{N}_0}$ gegen x und somit ist M vollständig.

Sei nun umgekehrt M vollständig und $(x_j + M_j)_{j\in\mathbb{N}_0}$ ein beliebiges Element von

$\varprojlim_{j\in\mathbb{N}_0} M/M_j$. Nach Definition von $\varprojlim_{j\in\mathbb{N}_0}$ ist dann $x_j - x_i \in M_j$ für alle $j \le i$. Daher gilt für alle $n, m \ge j$:

$$x_n - x_m = x_n - x_j + x_j - x_m \in M_j,$$

d.h. $(x_j)_{j\in\mathbb{N}_0}$ ist eine Cauchyfolge in M. Wegen der Vollständigkeit von M existiert somit eine Grenzwert $x \in M$ der Folge $(x_j)_{j\in\mathbb{N}_0}$. Für $j \in \mathbb{N}_0$ gibt es daher ein $n \ge j$ mit $x - x_n \in M_j$. Dann gilt aber

$$x - x_j = x - x_n + x_n - x_j \in M_j.$$

Daraus ergibt sich $(x_j + M_j)_{j\in\mathbb{N}_0} = (x + M_j)_{j\in\mathbb{N}_0} = g(x)$ und somit die Surjektivität von g. □

Definition 1.16. Sei (R, v) ein diskreter Bewertungsring mit maximalem Ideal $\mathfrak{m}$. Wir bezeichnen mit $k_R := R/\mathfrak{m}$ den Restklassenkörper von R.

Lemma 1.17. *Sei (R, v) ein diskreter Bewertungsring und $(\hat{R}, \hat{v})$ seine Versvollständigung. Dann stimmen die Restklassenkörper von R und $\hat{R}$ überein.*

Beweis. Ist $\pi \in R$ ein Uniformisierer von R, so ist π wegen $\hat{v}(\pi) = v(\pi) = 1$ auch ein Uniformisierer von $\hat{R}$. Damit ist wegen $R \subset \hat{R}$ bereits $k_R \subset k_{\hat{R}}$.
Für ein $\hat{x} \in \hat{R}$ existiert aber auch ein $x \in R$ mit $\hat{x} - x \in \pi\hat{R}$, da R dicht in $\hat{R}$ liegt. Also ist

$$x + \pi R = \hat{x} + (x - \hat{x}) + \pi\hat{R} = \hat{x} + \pi\hat{R}$$

und dementsprechend auch $k_{\hat{R}} = \hat{R}/\pi\hat{R} \subset R/\pi R = k_R$. □

Beispiel 1.18 (Die p-adischen Zahlen). Für ein $x \in \mathbb{Q}^*$ schreiben wir $x = {}^m\!/_n$ mit $m, n \in \mathbb{Z}\backslash\{0\}$. Dann können wir für p eine feste Primzahl m, n schreiben als $m = p^r m'$ und $n = p^s n'$ mit eindeutig bestimmten $s, r \in \mathbb{N}_0$, $m', n' \in \mathbb{Z}\backslash\{0\}$, sodass $\mathrm{ggt}(m', p) = \mathrm{ggt}(n', p) = 1$. Setzen wir $v_p(x) := r - s$ und $v_p(0) := \infty$, so erhalten wir durch $v_p\colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ eine wohldefinierte diskrete Bewertung auf $\mathbb{Q}$ mit Bewertungsring

$$\mathbb{Z}_{(p)} = \{x \in \mathbb{Q} \mid v_p(x) \ge 0\} = \left\{\frac{m}{n} \in \mathbb{Q} \mid m \in \mathbb{Z}, n \in \mathbb{Z}\backslash p\mathbb{Z}\right\}$$

und Uniformisierer p. Wir definieren

$$\mathbb{Q}_p := \text{Vervollständigung von } \mathbb{Q} \text{ bzgl. } v_p \quad (p\text{-adischen Zahlen});$$

$$\mathbb{Z}_p := \text{Vervollständigung von } \mathbb{Z}_{(p)} \text{ bzgl. } v_p \quad (\text{ganzen } p\text{-adischen Zahlen}).$$

Wie man in [Ne1] in *Kapitel 2, §1 & §2* detailiert nachlesen kann, ist

$$\begin{aligned}\mathbb{Z}_p &= \varprojlim_{n\in\mathbb{N}} \mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)} \cong \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z} \\ &= \left\{(a_n + p^n\mathbb{Z})_{n\ge 0} \in \prod_{n\ge 0} \mathbb{Z}/p^n\mathbb{Z} \mid \forall m \le n : a_m - a_n \in p^m\mathbb{Z}\right\}\end{aligned}$$

und $\mathbb{Q}_p = Quot(\mathbb{Z}_p)$. Nach Lemmma 1.17 ist zudem der Restklassenkörper von $\mathbb{Q}_p$ gegeben durch $k_{\mathbb{Q}_p} = \mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \mathbb{F}_p$.

Beispiel 1.19 (Der Körper der formalen Laurentreihen). Es sei k ein Körper und

$$k[[t]] = \left\{ \sum_{m \geq 0} a_m t^m \mid a_m \in k \right\}$$

der Ring der formalen Potenzreihen über k in der Variable t. Man sieht recht leicht, dass $k[[t]]$ ein vollständiger, diskreter Bewertungsring mit maximalem Ideal $t \cdot k[[t]]$ ist. Wir bezeichnen mit $k((t)) := Quot(k[[t]])$ den sogenannten Körper der formalen Laurentreihen über k in der Variable t, d.h. Reihen der Form $\sum_{m \geq m_0} a_m t^m$ mit $a_m \in k$ und $m_0 \in \mathbb{Z}$. Damit ist nach Lemma 1.11 der Körper $k((t))$ ein vollständiger, diskret bewerteter Körper mit Restklassenkörper k.

Von nun an fixieren wir die folgenden Notationen:

- (F, v) sei ein vollständiger, diskret bewerteter Körper;
- $\mathcal{O}_F = \{x \in F \mid v(x) \geq 0\}$ sein Bewertungsring, welcher nach Lemma 1.9 und 1.11 ein vollständiger, diskreter Bewertungsring ist;
- $\mathfrak{m}_F = \{x \in F \mid v(x) > 0\} = \pi \mathcal{O}_F$ das maximale Ideal von $\mathcal{O}_F$ und damit $\pi \in \mathcal{O}_F$ ein Uniformisierer;
- $k_F = \mathcal{O}_F / \mathfrak{m}_F$ der Restklassenkörper von F.

Lemma 1.20. *Sei $S \subset \mathcal{O}_F$ ein vollständiges Repräsentantensystem von k_F mit $0 \in S$ und $\pi_m \in F$ mit $v(\pi_m) = m$ für alle $m \in \mathbb{Z}$. Dann hat jedes $x \in F$ eine eindeutige Darstellung*

$$x = \sum_{m \in \mathbb{Z}} a_m \cdot \pi_m$$

mit $a_m \in S$ und $a_m = 0$ für fast alle $m < 0$. Außerdem ist $v(x) = \min\{m \in \mathbb{Z} \mid a_m \neq 0\}$.

Beweis. Einen Beweis der Aussage findet man in [Lo2] in *§24, F2* auf Seite 92. □

Lemma 1.21. *Sei p eine Primzahl, R ein kommutativer Ring mit Einselement 1_R und $I \subset R$ ein Ideal mit $p \cdot 1_R \in I$. Sind $m, n \geq 1, a, b \in R$, sodass $a \equiv b \mod I^m$, dann ist*

$$a^{p^n} \equiv b^{p^n} \mod I^{m+n}.$$

Beweis. Es genügt den Fall $n = 1$ zu beweisen, da man dadurch induktiv auf alle $n \in \mathbb{N}$ schließen kann. Wir setzen

$$P(X, Y) := \sum_{i=0}^{p-1} X^i Y^{p-1-i} \in \mathbb{Z}[X, Y].$$

Wegen $I^m \subset I$ ist insbesondere $a \equiv b \mod I$ und damit

$$P(a, b) \equiv P(a, a) \mod I \equiv p \cdot a^{p-1} \mod I \equiv 0 \mod I, \text{ da } p \cdot 1_R \in I.$$

Also ist $a^p - b^p = (a - b) \cdot P(a, b) \in I^{m+1}$, d.h. $a^p \equiv b^p \mod I^{m+1}$. □

Satz 1.22. *Ist k_F ein perfekter Körper der Charakteristik p, so gilt:*

(i) Es existiert eine eindeutige multiplikative Abbildung $s: k_F \to \mathcal{O}_F$ mit $s(0) = 0$ und $s(1) = 1$, deren Komposition mit der kanonischen Abbildung can: $\mathcal{O}_F \to k_F$ die Identität ist.

(ii) Ist zusätzlich $char(F) = p$, so ist $s: k_F \to \mathcal{O}_F$ ein Ringhomomorphismus und F ist isometrisch isomorph zu $k_F((t))$.

Beweis. Einen Beweis der Aussage und die Konstruktion von s findet man in [Ar] in *ChapterTen* auf den Seiten 190-192. □

Satz 1.23 (Hensel's Lemma)**.** *Sei $f \in \mathcal{O}_F[X]$ sodass $f \mod \mathfrak{m}_F = \bar{g} \cdot \bar{h}$ in $k_F[X]$ mit zueinander teilerfremden $\bar{g}, \bar{h} \in k_F[X]$ und $\bar{g}$ ist normiert. Dann gibt es $g, h \in \mathcal{O}_F[X]$ mit g normiert, $g \mod \mathfrak{m}_F = \bar{g}, h \mod \mathfrak{m}_F = \bar{h}$ und $f = g \cdot h$ in $\mathcal{O}_F[X]$.*

Beweis. Für einen Beweis des Henselschen Lemmas sei auf [Lo2], *§23, Satz 3* auf Seite 72 verwiesen. □

Satz 1.24. *Sei (F, v) ein diskret bewerteter Körper und $E|F$ eine endliche Körpererweiterung. Dann existiert genau eine diskrete Bewertung v_E auf E derart, dass (E, v_E) wieder vollständig ist und $v_{E|_F} = e(E|F) \cdot v$ für ein $e(E|F) \in \mathbb{N}$ mit $e(E|F) \mid [E : F]$.*

Beweis. Eine allgemeinere Aussage für einen Schiefkörper E wird in [Ke], *Lemma 12.6* auf Seite 72 bewiesen. □

Definition 1.25. Sei (F, v) ein diskret bewerteter Körper und $E|F$ eine endliche Körpererweiterung. Die in Satz 1.24 eingeführte Zahl $e(E|F) \in \mathbb{N}$ bezeichnet man als Verzweigungsindex der Körpererweiterung $E|F$. Ist $\pi_F \in F$ bzw. $\pi_E \in E$ ein Uniformisierer von F bzw. E, so ist wegen Satz 1.24 $\pi_F \in \pi_E^{e(E|F)} \mathcal{O}_E \subset \pi_E \mathcal{O}_E$.
Daher ist k_E eine Körpererweiterung von k_F und man bezeichnet mit $f(E|F) := [k_E : k_F]$ den Restklassengrad von $E|F$.

Lemma 1.26. *Sei $E|F$ eine endliche Körpererweiterung. Dann gilt:*

(i) $[E : F] = e(E|F) \cdot f(E|F)$;

(ii) $\mathcal{O}_E$ ist ein freier $\mathcal{O}_F$-Modul vom Rang $[E : F]$;

(iii) Sind $y_1, \ldots, y_{f(E|F)} \in \mathcal{O}_E$ Vertreter einer k_F-Basis von k_E und $\pi_E \in \mathcal{O}_E$ ein Uniformisierer in $\mathcal{O}_E$, so ist

$$\{y_j \pi_E^i\}_{\substack{1 \le j \le f(E|F), \\ 0 \le i \le e(E|F)-1}}$$

sowohl eine F-Basis von E, als auch eine $\mathcal{O}_F$-Basis von $\mathcal{O}_E$.

Beweis. In [Ar] findet man in *Chapter 3, Theorem 6 & Theorem 7*, auf den Seiten 58-59 einen vollständigen Beweis der Behauptungen. □

1.2 Unverzweigte Erweiterungen

Definition 1.27. Eine endliche Erweiterung $E|F$ eines vollständigen diskret bewerteten Körpers (F, v) heißt unverzweigt, falls $e(E|F) = 1$ und $k_E|k_F$ separabel ist.

Bevor wir uns nun mit unverzweigten Erweiterungen beschäftigen, mögen wir uns nochmal gewisse Grundlagen der Galoistheorie vor Augen halten. Ist nämlich $E|F$ eine beliebige Galoiserweiterung, so entspricht

$$Gal(E|F) = \varprojlim_{\substack{F\subset E'\subset E \\ E'|F \text{ endl. Galois}}} Gal(E'|F) \subset \prod_{\substack{F\subset E'\subset E \\ E'|F \text{ endl. Galois}}} Gal(E'|F)$$

dem projektiven Limes des projektiven Systems über alle endlichen Galoiserweiterungen von F in E.

Versieht man $Gal(E'|F)$ mit der diskreten Topologie, $\prod Gal(E'|F)$ mit der Produkttopologie und $Gal(E|F) \subset \prod Gal(E'|F)$ mit der induzierten Topologie, so gilt in $Gal(E|F)$:

$$U \subset Gal(E|F) \text{ ist offen } \Leftrightarrow \forall \sigma \in U\, \exists\, F \subset E_\sigma \subset E, E_\sigma|F \text{ endl. Galois: } \sigma \cdot Gal(E|E_\sigma) \subset U.$$

Diese Topologie auf $Gal(E|F)$ wird auch Krull-Topologie genannt. Nach dem Hauptsatz der Galoistheorie erhält man durch

$$\begin{aligned} \{E' \mid F \subset E' \subset E, [E' : F] < \infty\} &\leftrightarrows \{H \mid H \leq Gal(E|F) \text{ ist offen}\} \\ E' &\mapsto Gal(E|E') \\ E^H &\leftarrow\!\shortmid H \end{aligned}$$

wohldefinierte, inklusionsumkehrende, zueinander inverse Bijektionen. Des Weiteren ist $E'|F$, mit $F \subset E' \subset E$, endlich Galois genau dann, wenn $Gal(E|E') \trianglelefteq Gal(E|F)$ mit endlichem Index.
Für eine etwas detailiertere Ausführung dazu sei hierbei auf [Bo], *Kapitel 4.2*, Seiten 146-154 verwiesen.

Für den folgenden Satz sei an die Konventionen nach Beispiel 1.19 erinnert.

Satz 1.28. *Sei $E|F$ eine endliche Körpererweiterung. Dann gilt:*

(i) Ist $E|F$ unverzweigt, so ist $E|F$ separabel;

(ii) die Abbildung

$$\begin{aligned} \left\{F \subset E' \subset \overline{F} \mid E'|F \text{ endl. unverzweigt}\right\} &\to \left\{k_F \subset l \subset \overline{k_F} \mid l|k_F \text{ endl. separabel}\right\} \\ E' &\mapsto k_{E'} \end{aligned}$$

ist eine Bijektion, wobei $\overline{F}$ bzw. $\overline{k_F}$ einen algebraischen Abschluss von F bzw. k_F bezeichnet;

(iii) *$E|F$ ist unverzweigt und Galois genau dann, wenn $k_E|k_F$ Galois ist. In diesem Fall ist*

$$Gal(E|F) \to Gal(k_E|k_F), \sigma \mapsto \bar{\sigma} := (x + \mathfrak{m}_E \mapsto \sigma(x) + \mathfrak{m}_E),$$

ein Isomorphismus.

Beweis. Einen vollständigen Beweis findet man in [Lo2], *§24, Satz 3* auf Seite 95. □

Lemma 1.29. *Das Kompositum zweier unverzweigter Erweiterungen von F ist wieder unverzweigt.*

Beweis. Es sei hierbei auf [Ne1] *Kapitel 2, Korollar 7.3,* Seite 161 verwiesen, wo die Behauptung bewiesen wird. □

Satz 1.30. *Sei (F, v) ein vollständiger, diskret bewerteter Körper. Dann gilt:*

(i)

$$F^{nr} := \bigcup_{\substack{F \subset E \subset \overline{F} \\ E|F \text{ endl.} \\ \text{unverzweigt}}} E$$

ist eine Galoiserweiterung von F, die sogenannte maximale unverzweigte Erweiterung von F.

(ii) *F^{nr} ist ein diskret bewerteter Körper mit Bewertungsring*

$$\mathcal{O}_{F^{nr}} = \bigcup_{\substack{F \subset E \subset \overline{F} \\ E|F \text{ endl.} \\ \text{unverzweigt}}} \mathcal{O}_E \quad ,$$

Uniformisierer $\pi_F \in F \subset F^{nr}$ und Restklassenkörper ${k_F}^{sep}$. Des Weiteren ist

$$Gal(F^{nr}|F) \to Gal({k_F}^{sep}|k_F), \sigma \mapsto \bar{\sigma} := (x + \mathfrak{m}_E \mapsto \sigma(x) + \mathfrak{m}_E),$$

ein Isomorphismus von Gruppen.

Beweis. Wegen Lemma 1.29 ist F^{nr} ein Körper und nach Satz 1.28 auch separabel. Sei nun $E|F$ endlich unverzweigt und $\sigma \in Gal(F^{sep}|F)$. Aufgrund der Eindeutigkeit von $v_{\sigma(E)}$ in Satz 1.24 ist $v_{\sigma(E)} = v \circ \sigma^{-1}$. Damit ist $e(\sigma(E)|F) = e(E|F) = 1$, $\mathcal{O}_E \cong \mathcal{O}_{\sigma(E)}$ und $\mathfrak{m}_E \cong \mathfrak{m}_{\sigma(E)}$, was zu einem Isomorphismus $\bar{\sigma}: k_E \to k_{\sigma(E)}$ führt. Da $k_E|k_F$ separabel ist, ist auch $k_{\sigma(E)}|k_F$ wieder separabel. Dementsprechend ist $\sigma(E)|F$ wieder unverzweigt, d.h. $\sigma(E) \subset F^{nr}$ und damit $F^{nr}|F$ normal.

Für (ii) sei $x \in F^{nr}$ und $E|F$ endlich unverzweigt mit $x \in E$. Wir definieren die Abbildung

$$v: F^{nr} \to \mathbb{Z} \cup \{\infty\}, x \mapsto v_E(x).$$

Da F^{nr} die Vereinigung unverzweigter Körper ist, ist v eine wohldefinierte diskrete Bewertung von F^{nr} und

$$\mathcal{O}_{F^{nr}} = \bigcup_{\substack{F\subset E\subset\overline{F}\\ E|F \text{ endl.}\\ \text{unverzweigt}}} \mathcal{O}_E$$

mit Uniformisierer $\pi_F \in F$. Zusammen mit Lemma 1.28 folgt schließlich noch

$$k_{F^{nr}} = \bigcup_{\substack{k_F\subset l\subset\overline{k_F}\\ l|k_F \text{ endl.}\\ \text{separabel}}} l = {k_F}^{sep}$$

und

$$\begin{aligned} Gal(F^{nr}|F) = \varprojlim_{\substack{F\subset E\subset F^{nr}\\ E|F \text{ endl. Galois}}} Gal(E|F) &= \varprojlim_{\substack{F\subset E\subset\overline{F}\\ E|F \text{ endl. Galois}\\ \& \text{ unverzweigt}}} Gal(E|F) \\ &\cong \varprojlim_{\substack{k_F\subset l\subset {k_F}^{sep}\\ l|k_F \text{ endl.}}} Gal(l|k_F) \\ &= Gal({k_F}^{sep}|k_F). \end{aligned}$$

□

Lemma 1.31. *Sei (F,v) ein vollständiger, diskret bewerteter Körper mit $char(k_F) = p > 0$ und $\varphi: \mathcal{O}_F \to \mathcal{O}_F$ ein Ringhomomorphismus, sodass $\varphi(x) \equiv x^p \mod \mathfrak{m}_F$. Dann existiert ein eindeutiger Ringhomomorphismus $\varphi: \mathcal{O}_{F^{nr}} \to \mathcal{O}_{F^{nr}}$, welcher φ fortsetzt, sodass $\varphi(x) \equiv x^p \mod \mathfrak{m}_{F^{nr}}$ für alle $x \in \mathcal{O}_{F^{nr}}$.*
Diese Fortsetzung ist stetig bzgl. der π_F-adischen Topologie und lässt sich eindeutig auf $\widehat{\mathcal{O}_{F^{nr}}} = \mathcal{O}_{\widehat{F^{nr}}}$ fortsetzen.
Ein Ringhomomorphismus $\varphi: \mathcal{O}_F \to \mathcal{O}_F$ mit $\varphi(x) \equiv x^p \mod \mathfrak{m}_F$ für alle $x \in \mathcal{O}_F$ nennt man dabei einen Frobenius-Lift.

Beweis. Nach Satz 1.30 ist der Bewertungsring von F^{nr} die Vereinigung aller Bewertungsringe endlicher, unverzweigter Erweiterungen $E|F$ und damit genügt es zu zeigen, dass $\varphi: \mathcal{O}_F \to \mathcal{O}_F$ eindeutig fortgesetzt werden kann zu $\varphi: \mathcal{O}_E \to \mathcal{O}_E$.

Da $k_E|k_F$ separabel ist, existiert ein $x \in \mathcal{O}_E, \bar{x} := x + \mathfrak{m}_E \in k_E$, sodass $k_E = k_F[\bar{x}]$. Wir setzen $\bar{f}$ bzw. f als das Minimalpolynom von $\bar{x}$ bzw. x über k_F bzw. F. Trivialerweise ist dann $\deg(\bar{f}) \leq \deg(f)$, da f normiert ist und $f \mod \mathfrak{m}_E$ die Nullstelle $\bar{x}$ besitzt. Aufgrund von $e(E|F) = 1$ und Lemma 1.26 ist aber auch

$$\deg(f) = [F[x] : F] \leq [E : F] = [k_E : k_F] = [k_F[\bar{x}] : k_F] = \deg(\bar{f}) \leq \deg(f).$$

Also gilt sogar überall Gleichheit und damit $\bar{f} = f \mod \mathfrak{m}_E$ und $E = F[x]$. Nach Lemma 1.26 (iii) ist zudem $\{1, x, x^2, \ldots, x^{f(E|F)-1}\}$ eine $\mathcal{O}_F$-Basis von $\mathcal{O}_E$, d.h.

$$\mathcal{O}_E = \mathcal{O}_F[x] \cong \mathcal{O}_F[t]/(f).$$

wir definieren $\varphi: k_E \to k_E, y \mapsto y^p$, und setzen $\varphi: k_E \to k_E$ bzw. $\varphi: \mathcal{O}_F \to \mathcal{O}_F$ fort auf $k_E[t]$ bzw. $\mathcal{O}_F[t]$, indem man φ auf die jeweiligen Koeffizienten anwendet. Damit ist $\varphi(f) \in \mathcal{O}_F[t]$ mit

$$\begin{aligned}\varphi(f) \mod \mathfrak{m}_E = \varphi(\bar{f}) &= \varphi((t - \bar{x}) \cdot g(t)) = \varphi(t - \bar{x}) \cdot \varphi(g(t)) \\ &= (t - \bar{x}^p) \cdot \varphi(g(t)) \text{ für ein } g(t) \in k_E[t].\end{aligned}$$

Aufgrund der Separabilität von $k_E|k_F$ ist $\operatorname{ggt}(t - \bar{x}, g) = 1$ und damit existieren $r, s \in k_E[t]$ mit $1 = r(t - \bar{x}) + sg$. Wenden wir φ auf diese Gleichung an, so erhalten wir

$$1 = \varphi(1) = \varphi(r)\varphi(t - \bar{x}) + \varphi(s)\varphi(g) = \varphi(r)(t - \bar{x}^p) + \varphi(s)\varphi(g),$$

das heißt auch $\operatorname{ggt}(t - \bar{x}^p, \varphi(g)) = 1$. Nach Hensel's Lemma existiert somit ein $y \in \mathcal{O}_E$ mit $(\varphi(f))(y) = 0$ und $y \equiv x^p \mod \mathfrak{m}_E$.

Als nächstes betrachten wir den Ringhomomorphismus

$$\psi: \mathcal{O}_F[t] \to \mathcal{O}_E, h := \sum_i a_i t^i \mapsto \sum_i \varphi(a_i) y^i = (\varphi(h))(y).$$

Da y eine Nullstelle von $\varphi(f)$ ist, faktorisiert ψ durch

$$\varphi: \mathcal{O}_E \cong \mathcal{O}_F[t]/(f) \xrightarrow{\psi} \mathcal{O}_E, \sum_{i=0}^{[E:F]-1} a_i x^i \mapsto \sum_{i=0}^{[E:F]-1} a_i t^i + (f) \mapsto \sum_{i=0}^{[E:F]-1} \varphi(a_i) y^i.$$

Modulo dem maximalen Ideal $\mathfrak{m}_E$ gilt dann für ein $z = \sum_{i=0}^{[E:F]-1} a_i x^i \in \mathcal{O}_E$:

$$\begin{aligned}\varphi(z) \mod \mathfrak{m}_E &\equiv \sum_{i=0}^{[E:F]-1} \varphi(a_i) y^i \mod \mathfrak{m}_E \\ &\equiv \sum_{i=0}^{[E:F]-1} a_i^p (x^p)^i \mod \mathfrak{m}_E, \text{ da } \varphi \text{ ein Frobenius-Lift ist,} \\ &\equiv \left(\sum_{i=0}^{[E:F]-1} a_i x^i \right)^p \mod \mathfrak{m}_E, \text{ da char } (k_E) = p > 0, \\ &\equiv z^p \mod \mathfrak{m}_E\end{aligned}$$

und damit insbesondere $\varphi(\mathfrak{m}_E) \subset \mathfrak{m}_E$. Da φ ein Ringhomomorphismus ist, ist $\varphi(\mathfrak{m}_E^n) \subset \varphi(\mathfrak{m}_E)^n$ für alle $n \in \mathbb{N}$, woraus die Stetigkeit von $\varphi: \mathcal{O}_E \to \mathcal{O}_E$ folgt.

Somit bleibt nur noch die Eindeutigkeit von φ zu zeigen. Sei dafür $\phi: \mathcal{O}_E \to \mathcal{O}_E$ eine weitere Fortsetzung von $\varphi: \mathcal{O}_F \to \mathcal{O}_F$ mit $\phi(x) \equiv x^p \mod \mathfrak{m}_E$ für alle $x \in \mathcal{O}_E$.
Da $\bar{f}$ separabel ist und $\varphi: k_E \to k_E, y \mapsto y^p$ injektiv, hat auch $\varphi(\bar{f}) = \varphi(f) \mod \mathfrak{m}_E$ keine mehrfachen Nullstellen in k_E. Sind also $z, \tilde{z} \in \mathcal{O}_E$ zwei Nullstellen von $\varphi(f)$ mit $z - \tilde{z} \in \mathfrak{m}_E$, so muss bereits $z = \tilde{z}$ gelten. Nun ist aber

$$(\varphi(f))(y) = 0 = \phi(0) = \phi(f(x)) = \underbrace{(\phi(f))}_{=\varphi(f)}(\phi(x)) = (\varphi(f))(\phi(x))$$

und damit wegen $\phi(x) \equiv x^p \equiv y \mod \mathfrak{m}_E$ entsprechend $\phi(x) = y = \varphi(x)$. Aufgrund von $\mathcal{O}_E = \mathcal{O}_F[x]$ und $\phi_{|\mathcal{O}_F} = \varphi$ ist dann $\phi = \varphi$. □

1.3 Lokale Körper

Es sei wie gewohnt (F, v) ein diskret bewerteter Körper mit Bewertungsring $\mathcal{O}_F$ und Restklassenkörper k_F.

Definition 1.32. (F, v) heißt lokal, falls der Restklassenkörper k_F endlich und F bzgl. $|\cdot|: F \to \mathbb{R}_{\geq 0}$, $x \mapsto |x| := |k_F|^{-v(x)}$ vollständig ist.

In Beispiel 1.18 haben wir bereits gesehen, dass für eine beliebige Primzahl $p > 0$ die p-adischen Zahlen $\mathbb{Q}_p$ einen lokalen Körper bilden. Ein weiteres Beispiel liefert der Körper der formalen Laurentreihen $k((t))$, wenn der Körper k endlich ist.

Als nächstes wollen wir untersuchen wie sich Satz 1.28 und Satz 1.30 für lokale Körper formulieren lassen.

Satz 1.33. *Sei F ein lokaler Körper und $E|F$ eine endliche unverzweigte Erweiterung. Dann gilt:*

(i) $E|F$ ist Galois;

(ii) die Abbildung $Gal(E|F) \to Gal(k_E|k_F), \sigma \mapsto \bar{\sigma} := (x + \mathfrak{m}_E \mapsto \sigma(x) + \mathfrak{m}_E)$ ist ein wohldefinierter Isomorphismus von zyklischen Gruppen;

(iii) ist $\varphi_{E|F} \in Gal(E|F)$ der zu $(\bar{x} \mapsto \bar{x}^{|k_F|}) \in Gal(k_E|k_F)$ korrespondierende Automorphismus, so ist $\varphi_{E|F}$ ein Erzeuger von $Gal(E|F)$ und wir nennen $\varphi_{E|F}$ den Frobeniusautomorphismus von $E|F$.

Beweis. Einen Beweis der Aussage findet man in [Lo2], *§24, Satz 4 (iii)*, auf Seite 97. □

Satz 1.34. *Sei F ein lokaler Körper und $n \in \mathbb{N}$. Dann gibt es genau eine unverzweigte Erweiterung $F_n|F$ mit $[F_n : F] = n$. Damit ist außerdem k_{F_n} die eindeutige Erweiterung von k_F vom Grad n. F_n ist dabei gegeben durch $F(\zeta)$, wobei ζ eine primitive $(|k_F|^n - 1)$-te Einheitswurzel ist.*

Beweis. Die Behauptung wird in [Lo2], *§24, Satz 4 (i)*, auf Seite 97 bewiesen. □

2 Kohomologie für endliche Gruppen

Während des gesamten Kapitels sei G eine endliche multiplikative Gruppe mit Einselement $1 = 1_G$. Die folgenden Ausführungen und Vorgehensweisen orientieren sich dabei an [Ne2].

2.1 G-Moduln

Definition 2.1. (i) Ein G-Modul ist eine abelsche Gruppe $(A, +)$ zusammen mit einer Abbildung $G \times A \to A, (\sigma, a) \mapsto \sigma \cdot a$, sodass

- $1 \cdot a = a$;
- $\sigma \cdot (\tau \cdot a) = (\sigma\tau) \cdot a$;
- $\sigma \cdot (a + b) = \sigma \cdot a + \sigma \cdot b$.

für alle $\sigma, \tau \in G$ und $a, b \in A$.

(ii) Sind A, B G-Moduln und $f: A \to B$ ein Gruppenhomomorphismus, dann nennen wir f einen G-Homomorphismus bzw. G-äquivariant, falls $f(\sigma \cdot a) = \sigma \cdot f(a)$ für alle $\sigma \in G$ und $a \in A$.

(iii) Wir setzen $Hom(A, B)$ als die Menge der Gruppenhomomorphismen von A nach B und $Hom_G(A, B)$ als die Menge der G-Homomorphismen von A nach B. Dabei wird $Hom(A, B)$ durch $(\sigma \cdot f)(a) := \sigma \cdot f(\sigma^{-1} \cdot a)$ selbst zu einem G-Modul.

Definition 2.2. Mit $\mathbb{Z}[G]$ bezeichnen wir die freie additive Gruppe über den Elementen von G;

$$\mathbb{Z}[G] := \left\{ \sum_{\sigma \in G} n_\sigma \sigma \mid n_\sigma \in \mathbb{Z} \right\}.$$

Mit der üblichen Summen-Multiplikation wird $\mathbb{Z}[G]$ zu einem Ring mit Einselement $1_{\mathbb{Z}[G]} := 1_{\mathbb{Z}} 1_G$.

Definition 2.3. (i) Der Ringhomomorphismus $\varepsilon: \mathbb{Z}[G] \to \mathbb{Z}, \sum_{\sigma \in G} n_\sigma \sigma \mapsto \sum_{\sigma \in G} n_\sigma$ heißt Augmentation und wir setzen

$$I_G := ker(\varepsilon) = \left\{ \sum_{\sigma \in G} n_\sigma \sigma \in \mathbb{Z}[G] \mid \sum_{\sigma \in G} n_\sigma = 0 \right\}$$

als das sogenannte Augmentationsideal.

(ii) Mit dem Element $N_G := \sum_{\sigma \in G} \sigma \in \mathbb{Z}[G]$ bezeichnen wir die sogenannte Norm von $\mathbb{Z}[G]$.

(iii) $\mathbb{Z}N_G$ ist ein Ideal in $\mathbb{Z}[G]$ und wir setzen $J_G := \mathbb{Z}[G]/\mathbb{Z}N_G$.

Bemerkung 2.4. Man beachte, dass ein G-Modul A durch $(\sum_{\sigma \in G} n_\sigma \sigma) \cdot a := \sum_{\sigma \in G} n_\sigma (\sigma \cdot a)$ automatisch zu einem $\mathbb{Z}[G]$-Modul wird. Auf der anderen Seite wird auch jeder $\mathbb{Z}[G]$-Modul B durch die Einschränkung $G \hookrightarrow \mathbb{Z}[G], \sigma \mapsto 1_{\mathbb{Z}}\sigma$, zu einem G-Modul.

Lemma 2.5. *Sei X ein freier $\mathbb{Z}[G]$-Modul und $0 \to A \xrightarrow{g} B \xrightarrow{h} C \to 0$ eine kurze exakte Sequenz von G-Moduln. Dann ist die Sequenz*

$$0 \longrightarrow Hom_G(X, A) \xrightarrow{f \mapsto g \circ f} Hom_G(X, B) \xrightarrow{f' \mapsto h \circ f'} Hom_G(X, C) \longrightarrow 0$$

von Homomorphismen von abelschen Gruppen exakt.

Beweis. Einen Beweis findet man in [Ne2], *Satz 1.6*, auf Seite 9. □

Lemma 2.6. *Ist $\ldots \leftarrow X_{q-1} \xleftarrow{d_q} X_q \xleftarrow{d_{q+1}} X_{q+1} \leftarrow \ldots$ eine exakte Sequenz von freien $\mathbb{Z}$-Moduln und D ein beliebiger $\mathbb{Z}$-Modul, so ist*

$$\ldots \longrightarrow Hom(X_{q-1}, D) \xrightarrow{f \mapsto f \circ d_q} Hom(X_q, D) \xrightarrow{f \mapsto f \circ d_{q+1}} Hom(X_{q+1}, D) \longrightarrow \ldots$$

eine exakte Sequenz von $\mathbb{Z}$-Moduln.

Beweis. Es sei auf [Ne2], *Lemma 1.7*, Seite 10 verwiesen. □

2.2 Kohomologiegruppen

Wir möchten nun die Kohomologiegruppen einer Gruppe G und eines G-Moduls A definieren. Bei der Vorgehensweise orientieren wir uns an [Ne2] und müssen zunächst bestimmte $\mathbb{Z}[G]$-Moduln X_q zusammen mit G-Homomorphismen $d_q \colon X_q \to X_{q-1}$ definieren.

- $X_0 := X_{-1} := \mathbb{Z}[G]$ als freien $\mathbb{Z}[G]$-Modul von Rang 1.
- Für $q \geq 1$: $X_q := X_{-q-1} := \mathbb{Z}[G][G^q] := \bigoplus_{(\sigma_1, \ldots, \sigma_q) \in G^q} \mathbb{Z}[G](\sigma_1, \ldots, \sigma_q)$ als den freien $\mathbb{Z}[G]$-Modul mit Basis G^q.

Die G-Homomorphismen $d_q \colon X_q \to X_{q-1}$ definieren wir über die Basiselemente wie folgt:

- $d_0(1) := N_G$;

- $d_1(\sigma) := \sigma - 1$;
- $d_q((\sigma_1,\dots,\sigma_q)) := \sigma_1(\sigma_2,\dots,\sigma_q) + \sum_{i=1}^{q-1}(-1)^i(\sigma_1,\dots,\sigma_{i-1},\sigma_i\sigma_{i+1},\sigma_{i+2},\dots,\sigma_q)$ $+ (-1)^q(\sigma_1,\dots,\sigma_{q-1})$ für $q > 1$;
- $d_{-1}(1) := \sum_{\sigma\in G}(\sigma^{-1}(\sigma) - (\sigma))$;
- $d_{-q-1}((\sigma_1,\dots,\sigma_q)) := \sum_{\sigma\in G}\sigma^{-1}(\sigma,\sigma_1,\dots,\sigma_q)$ $+ \sum_{\sigma\in G}\sum_{i=1}^{q}(-1)^i(\sigma_1,\dots,\sigma_{i-1},\sigma_i\sigma,\sigma^{-1},\sigma_{i+1},\dots,\sigma_q) + \sum_{\sigma\in G}(-1)^{q+1}(\sigma_1,\dots,\sigma_q,\sigma)$ für $q > 0$.

Damit erhalten wir den folgenden Satz.

Satz 2.7. *Die Sequenz*

$$\dots \xleftarrow{d_{-2}} X_{-2} \xleftarrow{d_{-1}} X_{-1} \xleftarrow{d_0} X_0 \xleftarrow{d_1} X_1 \xleftarrow{d_2} \dots$$

von freien $\mathbb{Z}[G]$-Moduln mit $\mathbb{Z}[G]$-linearen Abbildungen ist exakt.

Beweis. Einen ausführlichen Beweis findet man in [Ne2] auf den Seiten 11-16. □

Definition 2.8. $(X_q, d_q)_{q\in\mathbb{Z}}$ bezeichnet man als den freien Standardkomplex der Gruppe G.

Sei $(X_q, d_q)_{q\in\mathbb{Z}}$ der freie Standardkomplex und A ein beliebiger G-Modul. Wir definieren für $q \in \mathbb{Z}$

$$\partial_q : Hom_G(X_{q-1}, A) \to Hom_G(X_q, A),\ f \mapsto f \circ d_q\ .$$

Nach Satz 2.7 und Lemma 2.6 ist dann

$$\dots \longrightarrow Hom_G(X_{q-1}, A) \xrightarrow{\partial_q} Hom_G(X_q, A) \xrightarrow{\partial_{q+1}} Hom_G(X_{q+1}, A) \longrightarrow \dots$$

eine Sequenz mit $\partial_{q+1} \circ \partial_q = 0$, d.h. insbesondere ist $\mathrm{im}(\partial_q) \subset \ker(\partial_{q+1})$ für alle $q \in \mathbb{Z}$. Wir setzen

$$Z_q := Z_q(G, A) := \ker(\partial_{q+1}) \text{ (q-Kozykel von } G \text{ mit Koeffizienten in } A);$$

$$R_q := R_q(G, A) := \mathrm{im}(\partial_q) \text{ (q-Koränder von } G \text{ mit Koeffizienten in } A).$$

Definition 2.9. Für einen beliebigen G-Modul A und $q \in \mathbb{Z}$ definieren wir die q-te Kohomologiegruppe von G mit Koeffizienten in A als

$$H^q(G, A) := Z_q/R_q = \ker(\partial_{q+1})/\mathrm{im}(\partial_q)\ .$$

Um $H^q(G,A)$ in etwas expliziterer Weise angeben zu können, untersuchen wir zunächst ∂_q. Wir setzen $A_q := Hom_G(X_q,A)$ für $q \in \mathbb{Z}$. Wegen Bemerkung 2.4 ist $Hom_G(X_q,A) = Hom_{\mathbb{Z}[G]}(X_q,A)$ und es ist jedes $f \in Hom_G(X_q,A)$ eindeutig dadurch bestimmt, was f auf den Basiselementen von X_q bewirkt. Daher ist

$$A_0 = A_{-1} = Hom_G(\mathbb{Z}[G],A) = Hom_{\mathbb{Z}[G]}(\mathbb{Z}[G],A) \cong Maps(\{1_G\},A) \cong A\,;$$

$$A_q = A_{-q-1} = Hom_G(\mathbb{Z}[G][G^q],A) \cong Maps(G^q,A).$$

Mit Hilfe der Definition der Homomorphismen d_q des Standardkomplexes ergeben sich für ∂_q die expliziten Definitionen

- $\partial_0(x) = N_G x \qquad$ für $x \in A_{-1} = A$;
- $(\partial_1(x))(\sigma) = \sigma x - x \qquad$ für $x \in A_0 = A$ und $\sigma \in G$;
- $(\partial_q(f))(\sigma_1,\dots,\sigma_q) = \sigma_1 f(\sigma_2,\dots,\sigma_q) + \sum_{i=1}^{q-1}(-1)^i f(\sigma_1,\dots,\sigma_{i-1},\sigma_i\sigma_{i+1},\sigma_{i+2},\dots,\sigma_q)$
  $+ (-1)^q f(\sigma_1,\dots,\sigma_{q-1}) \qquad$ für $f \in A_{q-1}, (\sigma_1,\dots,\sigma_q) \in G^q$ und $q > 1$;
- $\partial_{-1}(f) = \sum_{\sigma\in G}(\sigma^{-1}f(\sigma) - f(\sigma)) \qquad$ für $f \in A_{-2}$;
- $(\partial_{-q-1}(f))(\sigma_1,\dots,\sigma_q) = \sum_{\sigma\in G}[\sigma^{-1}f(\sigma,\sigma_1,\dots,\sigma_q)$
  $+ \sum_{i=1}^{q}(-1)^i f(\sigma_1,\dots,\sigma_{i-1},\sigma_i\sigma,\sigma^{-1},\sigma_{i+1},\dots,\sigma_q)$
  $+ (-1)^{q+1} f(\sigma_1,\dots,\sigma_q,\sigma)] \qquad$ für $f \in A_{-q-2}, (\sigma_1,\dots,\sigma_q) \in G^q$ und $q > 0$.

Mit dieser Beschreibung der ∂_q können wir nun die q-te Kohomologiegruppe für kleine $q \in \mathbb{Z}$ explizit angeben.

- $H^{-1}(G,A)$:

$$\begin{aligned} Z_{-1} &= \ker(\partial_0) = {}_{N_G}A = \{x \in A \mid N_G \cdot x = 0\} \\ R_{-1} &= \mathrm{im}(\partial_{-1}) = I_G A \\ H^{-1}(G,A) &= {}_{N_G}A/I_G A \end{aligned}$$

- $H^0(G,A)$:

$$\begin{aligned} Z_0 &= \ker(\partial_1) = A^G = \{x \in A \mid \forall \sigma \in G:\ \sigma \cdot x = x\} \\ R_0 &= \mathrm{im}(\partial_0) = N_G A \\ H^0(G,A) &= A^G/N_G A \end{aligned}$$

- $H^1(G,A)$:

$$\begin{aligned} Z_1 &= \ker(\partial_2) = \{f\colon G \to A \mid \forall \sigma,\tau \in G:\ f(\sigma\tau) = \sigma f(\tau) + f(\sigma)\} \\ R_1 &= \mathrm{im}(\partial_1) = \{f\colon G \to A \mid \exists x \in A \forall \sigma \in G:\ f(\sigma) = \sigma x - x\} \\ H^1(G,A) &= Z_1/R_1 \end{aligned}$$

- $H^2(G,A)$:

  $Z_2 = \ker(\partial_3) = \{f: G \times G \to A \mid \forall \sigma,\tau,\rho \in G:\ f(\sigma\tau,\rho) + f(\sigma,\tau) = \sigma f(\tau,\rho) + f(\sigma,\tau\rho)\}$
  $R_2 = \mathrm{im}(\partial_2) = \{f: G \times G \to A \mid \exists g: G \to A \forall \sigma,\tau \in G:\ f(\sigma,\tau) = \sigma g(\tau) - g(\sigma\tau) + g(\sigma)\}$
  $H^2(G,A) = Z_2/R_2$

Operiert G auf A sogar trivial, dann ist $H^1(G,A)$ gegeben durch $Hom(G,A)$. Für eine detailiertere Beschreibung der Herleitung sei auf die Seiten 17-19 in [Ne2] verwiesen.

2.3 Der Verbindungshomomorphismus δ_q

Es seien A, A' zwei G-Moduln und $f: A \to A'$ ein G-Homomorphismus. Wir definieren einen Gruppenhomomorphismus $f_q: A_q \to A'_q$ durch

- $f_q = f$ für $q \in \{0,-1\}$;
- $f_q(F) := f \circ F$ für $F \in A_q$ und $q \in \mathbb{Z}\backslash\{0,-1\}$.

Aufgrund der G-Äquivarianz von f ist dann $f_{q+1} \circ \partial_{q+1} = \partial_{q+1} \circ f_q$, also bildet f_q q-Kozykel auf q-Kozykel und q-Koränder auf q-Koränder ab und impliziert damit einen wohldefinierten Gruppenhomomorphismus

$$\bar{f}_q: H^q(G,A) \to H^q(G,A'),\ z + R_q(G,A) \mapsto f_q(z) + R_q(G,A')\ .$$

Ist nun $0 \to A \xrightarrow{f} A' \xrightarrow{g} A'' \to 0$ eine exakte Sequenz von G-Moduln, so wollen wir für ein $q \in \mathbb{Z}$ eine Abbildung $\delta_q: H^q(G,A'') \to H^{q+1}(G,A)$ definieren und gehen dabei wie folgt vor.

Sei zunächst $\overline{z''_q} := z''_q + R_q(G,A'') \in H^q(G,A'')$ mit $z''_q \in Z_q(G,A'') = \ker(\partial_{q+1})$, d.h. $\partial_{q+1}(z''_q) = 0$. Wegen der Exaktheit der Sequenz $0 \to A \xrightarrow{f} A' \xrightarrow{g} A'' \to 0$ ist nach Lemma 2.5 auch $0 \to A_q \xrightarrow{f_q} A'_q \xrightarrow{g_q} A''_q \to 0$ exakt. Also existiert für $z''_q \in Z_q(G,A'') \subset A''_q$ ein $z'_q \in A'_q$ mit $g_q(z'_q) = z''_q$. Man beachte, dass dann

$$g_{q+1}(\partial_{q+1}(z'_q)) = \partial_{q+1}(g_q(z'_q)) = \partial_{q+1}(z''_q) = 0\,,$$

d.h. $\partial_{q+1}(z'_q) \in \ker(g_{q+1}) = \mathrm{im}(f_{q+1})$. Damit lässt sich $\partial_{q+1}(z'_q)$ schreiben als $\partial_{q+1}(z'_q) = f_{q+1}(z_{q+1})$ für ein $z_{q+1} \in A_{q+1}$.
Aufgrund der Injektivität von f_{q+2} folgt aus

$$f_{q+2}(\partial_{q+2}(z_{q+1})) = \partial_{q+2}(f_{q+1}(z_{q+1})) = \underbrace{\partial_{q+2} \circ \partial_{q+1}}_{=0}(z'_q) = 0$$

schließlich, dass bereits $z_{q+1} \in \ker(\partial_{q+2}) = Z_{q+1}(G,A)$ ist.

Wir definieren die Abbildung

$$\delta_q : H^q(G,A'') \longrightarrow H^{q+1}(G,A),\ z_q'' + R_q(G,A'') \longmapsto z_{q+1} + R_{q+1}(G,A)\ .$$

Lemma 2.10. *Ist* $0 \to A \xrightarrow{f} A' \xrightarrow{g} A'' \to 0$ *eine exakte Sequenz von G-Moduln, so ist der zuvor definierte Verbindungshomomorphismus* δ_q *ein wohldefinierter Gruppenhomomorphismus.*

Beweis. [Ne2], *Satz 3.1* auf Seite 22. □

Satz 2.11. *Ist* $0 \to A \xrightarrow{f} A' \xrightarrow{g} A'' \to 0$ *eine exakte Sequenz von G-Moduln, so ist die hieraus entstehende unendliche Sequenz*

$$\ldots \to H^q(G,A) \xrightarrow{\bar{f}_q} H^q(G,A') \xrightarrow{\bar{g}_q} H^q(G,A'') \xrightarrow{\delta_q} H^{q+1}(G,A) \to \ldots$$

ebenfalls exakt. Sie wird auch häufig als die exakte Kohomologiesequenz bezeichnet.

Beweis. [Ne2], *Satz 3.2*, auf Seite 24. □

Satz 2.12 (Dimensionsverschiebung)**.** *Für einen G-Modul A und ein* $m \in \mathbb{Z}$ *setzen wir*

$$A^m := \begin{cases} \underbrace{I_G \otimes_{\mathbb{Z}} \ldots \otimes_{\mathbb{Z}} I_G}_{-m-mal} \otimes_{\mathbb{Z}} A & , m < 0, \\ A & , m = 0, \\ \underbrace{J_G \otimes_{\mathbb{Z}} \ldots \otimes_{\mathbb{Z}} J_G}_{m-mal} \otimes_{\mathbb{Z}} A & , m > 0. \end{cases}$$

Dann liefert die m-malige Hintereinanderschaltung des Verbindungshomomorphismus δ *einen Isomorphismus*

$$\delta^m : H^{q-m}(H,A^m) \to H^q(H,A)$$

für jedes $q \in \mathbb{Z}$ *und jede Untergruppe* $H \leq G$*.*

Beweis. Einen Beweis der Dimensionsverschiebung findet man in [Ne2], *Satz 3.15*, auf Seite 32. □

Definition 2.13. Für eine Gruppe G setzen wir die Kommutatorgruppe G' als die von $\{[g,h] := ghg^{-1}h^{-1} \mid g,h \in G\}$ erzeugte Untergruppe von G. Dann ist G' ein Normalteiler von G und wir definieren $G^{ab} := G/G'$ als den maximalen abelschen Quotienten von G.

Von nun an und für den Rest der gesamten Arbeit betrachten wir $\mathbb{Z}, \mathbb{Q}$ und $\mathbb{Q}/\mathbb{Z}$ als G-Moduln mit der trivialen Operation.

Lemma 2.14. *Aus den beiden kurzen exakten Sequenzen* $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ *und* $0 \to I_G \to \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \to 0$ *erhält man:*

(i) Der Verbindungshomomorphismus $\delta_1 : H^1(G, \mathbb{Q}/\mathbb{Z}) \to H^2(G, \mathbb{Z})$ *ist ein Isomorphismus und wir bezeichnen mit*

$$\chi(G) := Hom(G, \mathbb{Q}/\mathbb{Z}) = H^1(G, \mathbb{Q}/\mathbb{Z}) \cong H^2(G, \mathbb{Z})$$

die sogenannte Charaktergruppe von G;

(ii) $H^{-2}(G, \mathbb{Z}) \cong G^{ab}$.

Beweis. [Ne2], *Korollar 3.18 & Satz 3.19*, auf Seite 33. □

2.4 Inflation, Restriktion und Korestriktion

Im vorherigen Abschnitt haben wir untersucht, wie sich $H^q(G, A)$ verhält, wenn sich A verändert. In diesem Abschnitt möchten untersuchen, was mit $H^q(G, A)$ passiert, wenn wir G variieren.

Sei dafür $H \trianglelefteq G$ ein Normalteiler und A ein G-Modul. Offensichtlich ist dann A^H ein G/H-Modul via $(gH) \cdot a := g \cdot a$ für $a \in A^H, g \in G$. Ist $f \in A_q^H = Maps((G/H)^q, A^H)$ eine sogenannte q-Kokette, so definieren wir für $q \geq 1$

$$\inf_q(f) : G^q \twoheadrightarrow (G/H)^q \xrightarrow{f} A^H \hookrightarrow A \, .$$

Man sieht recht leicht, dass dann $\partial_{q+1} \circ \inf_q = \inf_{q+1} \circ \partial_{q+1}$, also $\inf_q$ die Eigenschaft der q-Kozykel und q-Koränder beibehält.

Definition 2.15. Die zuvor definierte Abbildung $\inf_q : A_q^H \to A_q$ induziert einen Homomorphismus

$$\inf_q : H^q(G/H, A^H) \to H^q(G, A) \text{ für } q \geq 1.$$

Diesen Homomorphismus bezeichnen wir als Inflation.

Auf der anderen Seite wollen wir neben der Inflation nun die Restriktion einführen.

Definition 2.16. Sei A ein G-Modul, $H \leq G$ eine Untergruppe und $q \in \mathbb{Z}$. Wir definieren $\mathrm{res}_q : H^q(G, A) \to H^q(H, A)$ wie folgt:

- $\mathrm{res}_0 : H^0(G, A) = A^G/N_G A \to A^H/N_H A = H^0(H, A), a + N_G A \mapsto a + N_H A$;

- Für $q \in \mathbb{Z}$ definieren wir res_q durch den Dimensionsverschiebungsisomorphismus δ^q als den eindeutigen Homomorphismus, sodass das Diagramm

$$\begin{array}{ccc} H^0(G, A^q) & \xrightarrow{\cong}_{\delta^q} & H^q(G, A) \\ {\scriptstyle \mathrm{res}_0}\downarrow & & \downarrow{\scriptstyle \mathrm{res}_q} \\ H^0(H, A^q) & \xrightarrow{\cong}_{\delta^q} & H^q(H, A) \end{array}$$

  kommutiert.

In quasi umgekehrter Weise zur Restriktion möchten wir nun die Korestriktion definieren.

Definition 2.17. Sei A ein G-Modul, $H \leq G$ eine Untergruppe und $q \in \mathbb{Z}$. Wir definieren $\mathrm{cor}_q : H^q(H, A) \to H^q(G, A)$ wie folgt:

- $\mathrm{cor}_0 : H^0(H, A) = A^H / N_H A \to A^G / N_G A = H^0(G, A), a + N_H A \mapsto \sum_{\sigma \in G/H} \sigma \cdot a + N_G A$;
- Für $q \in \mathbb{Z}$ definieren wir cor_q durch den Dimensionsverschiebungsisomorphismus δ^q als den eindeutigen Homomorphismus, sodass das Diagramm

$$\begin{array}{ccc} H^0(H, A^q) & \xrightarrow{\cong}_{\delta^q} & H^q(H, A) \\ {\scriptstyle \mathrm{cor}_0}\downarrow & & \downarrow{\scriptstyle \mathrm{cor}_q} \\ H^0(G, A^q) & \xrightarrow{\cong}_{\delta^q} & H^q(G, A) \end{array}$$

  kommutiert.

Lemma 2.18. *Sei A ein G-Modul, $H \leq G$ eine Untergruppe und $q \in \mathbb{Z}$. Dann ist*

$$cor_q \circ res_q = (G : H) \cdot id_{H^q(G,A)}.$$

Beweis. [Ne2], *Satz 4.14*, auf Seite 45. □

Lemma 2.19. *Sei A ein G-Modul, $H \trianglelefteq G$ ein Normalteiler von G und $q \geq 1$. Ist $H^i(H, A) = 0$ für alle $i \in \{1, \ldots, q-1\}$, so hat man mit*

$$0 \longrightarrow H^q(G/H, A^H) \xrightarrow{inf_q} H^q(G, A) \xrightarrow{res_q} H^q(H, A)$$

eine exakte Sequenz.

Beweis. [Ne2], *Satz 4.7*, aus Seite 38. □

2.5 Das Cupprodukt

Es seien wie zuvor G eine endliche Gruppe und A, A' G-Moduln. Damit ist auch $A \otimes_{\mathbb{Z}} A'$ ein G-Modul via $\sigma \cdot (a \otimes a') := \sigma \cdot a \otimes \sigma \cdot a'$ und wir haben eine $\mathbb{Z}$-bilineare Abbildung $A^G \times A'^G \to (A \otimes_{\mathbb{Z}} A')^G$, $(a, a') \mapsto a \otimes a'$. Unter dieser Abbildung wird $N_G A \times N_G A'$ in $N_G(A \otimes_{\mathbb{Z}} A')$ abgebildet und induziert damit eine $\mathbb{Z}$-bilineare Abbildung

$$\begin{aligned} H^0(G,A) \times H^0(G,A') &\longrightarrow H^0(G, A \otimes_{\mathbb{Z}} A') \\ (a + N_G A, a' + N_G A') &\longmapsto a \otimes a' + N_G(A \otimes A') \ . \end{aligned}$$

Satz 2.20. *Es gibt eine eindeutig bestimmte Familie von bilinearen Abbildungen*

$$\begin{aligned} \cup : H^p(G,A) \times H^q(G,A') &\longrightarrow H^{p+q}(G, A \otimes_{\mathbb{Z}} A'), \quad p, q \in \mathbb{Z}, \\ (\bar{a}, \bar{a'}) &\longmapsto \bar{a} \cup \bar{a'}, \end{aligned}$$

das sogenannte Cupprodukt, mit den folgenden Eigenschaften:

(i) Für $p = q = 0$ ist das Cupprodukt durch die zuvor definierte Abbildung gegeben;

(ii) Sind die G-Modulsequenzen $0 \to A \to A' \to A'' \to 0$ und $0 \to A \otimes_{\mathbb{Z}} B \to A' \otimes_{\mathbb{Z}} B \to A'' \otimes_{\mathbb{Z}} B \to 0$ beide exakt, so ist das Diagramm

$$\begin{array}{ccc} H^p(G,A'') \times H^q(G,B) & \xrightarrow{\cup} & H^{p+q}(G, A'' \otimes_{\mathbb{Z}} B) \\ \downarrow{\scriptstyle \delta_p \times id} & & \downarrow{\scriptstyle \delta_{p+q}} \\ H^{p+1}(G,A) \times H^q(G,B) & \xrightarrow{\cup} & H^{p+q+1}(G, A \otimes_{\mathbb{Z}} B) \end{array}$$

kommutativ;

(iii) Sind die G-Modulsequenzen $0 \to B \to B' \to B'' \to 0$ und $0 \to A \otimes_{\mathbb{Z}} B \to A \otimes_{\mathbb{Z}} B' \to A \otimes_{\mathbb{Z}} B'' \to 0$ beide exakt, so ist das Diagramm

$$\begin{array}{ccc} H^p(G,A) \times H^q(G,B'') & \xrightarrow{\cup} & H^{p+q}(G, A \otimes_{\mathbb{Z}} B'') \\ \downarrow{\scriptstyle id \times \delta_q} & & \downarrow{\scriptstyle \delta_{p+q}} \\ H^p(G,A) \times H^{q+1}(G,B) & \xrightarrow{\cup} & H^{p+q+1}(G, A \otimes_{\mathbb{Z}} B) \end{array}$$

kommutativ.

Beweis. [Ne2], *Definition 5.1*, auf Seite 49. □

In gewissen Spezialfällen können wir das Cupprodukt auf recht einfache Weise explizit angeben.

Satz 2.21. *Ist $p = 0$ oder $q = 0$, so ist das Cupprodukt explizit gegeben durch*

$$\begin{aligned} \cup : H^p(G,A) \times H^q(G,A') &\longrightarrow H^{p+q}(G, A \otimes_{\mathbb{Z}} A') , \\ (\bar{a_p}, \bar{a'_q}) &\longmapsto \bar{a_p} \cup \bar{a'_q} = \overline{a_p \otimes a'_q} \end{aligned}$$

wobei a_p bzw. a'_q ein Repräsentant von $\bar{a_p}$ bzw. $\bar{a'_q}$ ist.

Beweis. [Ne2], *Satz 5.2*, Seite 51. □

3 Azumaya-Algebren und Brauergruppen

Für das gesamte Kapitel sei durch E ein beliebiger Körper bezeichnet. Die folgenden Ausführungen orientieren sich dabei größtenteils an [Ke]

Definition 3.1. Eine (nicht notwendigerweise kommutative) E-Algebra A mit 1 heißt Azumaya-Algebra über E, wenn

(i) $dim_E(A) < \infty$;

(ii) $Zentrum(A) = \{z \in A \mid z \cdot a = a \cdot z \; \forall a \in A\} = E$;

(iii) A ist einfach, d.h. 0 und A sind die einzigen zweiseitigen Ideale.

Ein einfaches Beispiel für eine Azumaya-Algebra über E ist $A = E^{m\times m}$ für ein $m \in \mathbb{N}$.

Definition 3.2. Zwei Azumaya-Algebren A, B über E heißen ähnlich, wenn $n, m \in \mathbb{N}$ existieren, sodass $A \otimes_E E^{n\times n} \cong B \otimes_E E^{m\times m}$ als E-Algebren. Man schreibt dann auch $A \sim B$.

Wie man in [Ke], *§3.4* genauer nachlesen kann, bildet die zuvor definierte Relation $\sim$ auf den Azumaya-Algebren über E eine Äquivalenzrelation und wir setzen $[A] :=$ Äquivalenzklasse von A bzgl. $\sim$.

Lemma 3.3. *$Br(E) := \{[A] \mid A$ ist eine Azuyama-Algebra über $E\}$ ist eine kommutative Gruppe bzgl. $[A] \cdot [B] := [A \otimes_E B]$ mit Einselement $[E] = [E^{m\times m}]$. $Br(E)$ ist die sogenannte Brauergruppe von E.*

Beweis. Für einen Beweis sei auf [Ke], *§3.5*, Seite 32 verwiesen. □

Satz 3.4. *Es sei $E'|E$ eine Körpererweiterung. Ist A eine Azumaya-Algebra über E, so ist $A \otimes_E E'$ eine Azumaya-Algebra über E' und es gibt einen Gruppenhomomorphismus*

$$r_{E'|E}: Br(E) \to Br(E'), \; [A] \mapsto [A \otimes_E E'].$$

Dabei gilt $r_{E''|E} = r_{E''|E'} \circ r_{E'|E}$ für eine Körperkette $E \subset E' \subset E''$.

Beweis. Einen Beweis der Aussage findet man in [Ke], *§3.7*, auf Seite 33. □

Definition 3.5. Es sei $E'|E$ eine Körpererweiterung. Dann bezeichnen wir mit

$$Br(E'|E) := \ker(r_{E'|E}) = \{[A] \in Br(E) \mid [A \otimes_E E'] = [E']\}$$

die relative Brauergruppe der Körpererweiterung $E'|E$, welche offensichtlich eine Untergruppe von $Br(E)$ ist.

Nach [Ke], *§5.8* ist dann sogar $Br(E) = \bigcup_{\substack{E'|E \text{ endl.} \\ \text{Galois}}} Br(E'|E)$.

Satz 3.6. *Es sei $E'|E$ eine endliche Galoiserweiterung der Ordnung $m = [E' : E]$ mit Galoisgruppe $G_{E'|E}$ und $f : G_{E'|E} \times G_{E'|E} \to (E')^*$ ein 2-Kozyklus, wobei $G_{E'|E}$ kanonisch auf $(E')^*$ operiert, d.h. $\sigma \cdot x = \sigma(x)$ für $\sigma \in G_{E'|E}$ und $x \in (E')^*$. Dann ist der m^2-dimensionale E-Vektorraum $A = A(f) := \bigoplus_{\sigma \in G_{E'|E}} E' \cdot u_\sigma$ (u_σ formale Symbole) mit der durch*

$$\left(\sum_{\sigma \in G_{E'|E}} x_\sigma u_\sigma\right) \cdot \left(\sum_{\tau \in G_{E'|E}} y_\tau u_\tau\right) = \sum_{\sigma \in G_{E'|E}} \sum_{\tau \in G_{E'|E}} x_\sigma \sigma(y_\tau) f(\sigma, \tau) u_{\sigma\tau}$$

für $x_\sigma, y_\tau \in E'$ definierten Multiplikation eine Azumaya-Algebra über E mit Einselement $1_a = (f(1_{G_{E'|E}}, 1_{G_{E'|E}}))^{-1} u_{1_{G_{E'|E}}}$. Ferner gilt:

(i) Durch $x \mapsto x \cdot 1_A$ wird E' in A eingebettet;

(ii) Es ist $u_\sigma \in A^*$ für alle $\sigma \in G_{E'|E}$;

(iii) Es ist $Z_A(E') := \{a \in A \mid x \cdot a = a \cdot x \; \forall x \in E'\} = E'$.

Beweis. Einen Beweis des Satzes findet man in [Ke], *§7.5*, auf den Seiten 59-62. □

Bemerkung 3.7. Mit der zuvor definierten Multiplikation auf $A(f)$ gilt:

(i) $u_\sigma \cdot x = \sigma(x) u_\sigma$ für alle $\sigma \in G_{E'|E}, x \in E'$;

(ii) $u_\sigma \cdot u_\tau = f(\sigma, \tau) u_{\sigma\tau}$ für alle $\sigma, \tau \in G_{E'|E}$.

Beweis. (ii) ist trivial nach Definition der Multiplikation auf $A(f)$. Für (i) erhält man unter Anwendung der 2-Kozykel-Relation von f:

$$\begin{aligned} u_\sigma \cdot x &= u_\sigma \cdot (x(f(1,1))^{-1}) u_1 = \sigma(x(f(1,1))^{-1}) f(\sigma, 1) u_{\sigma \cdot 1} = \sigma(x)\sigma(f(1,1))^{-1} f(\sigma, 1) u_\sigma \\ &= \sigma(x)(\sigma(f(1,1)) f(\sigma, 1 \cdot 1)(f(\sigma, 1 \cdot 1))^{-1})^{-1} f(\sigma, 1) u_\sigma \\ &= \sigma(x)(f(\sigma \cdot 1, 1) f(\sigma \cdot 1, 1)(f(\sigma, 1))^{-1})^{-1} f(\sigma, 1) u_\sigma \\ &= \sigma(x) u_\sigma, \end{aligned}$$

was zu zeigen war. □

Satz 3.8. *Es sei $E'|E$ eine endliche Galoiserweiterung mit Galoisgruppe $G_{E'|E}$. Dann ist die Abbildung*

$$\alpha_{E'|E}: H^2(G_{E'|E}, (E')^*) \to Br(E'|E),\ [f] \mapsto [A(f)],$$

ein Gruppenisomorphismus.

Beweis. Für einen Beweis des Satzes sei auf [Ke], *§8.3* auf Seite 71 verwiesen. □

Beispiel 3.9. Wir betrachten nun eine endliche Galoiserweiterung $E'|E$ mit Galoisgruppe $G_{E'|E}$. Sei $\chi: G_{E'|E} \hookrightarrow \mathbb{Q}/\mathbb{Z}$ ein injektiver Gruppenhomomorphismus und $u \in E^*$. Aufgrund der Injektivität von χ handelt es sich bei $E'|E$ um eine abelsche Erweiterung. Wir setzen $\bar{u} := u \cdot N_{E'|E}(E')^* \in E^*/N_{E'|E}((E')^*) = H^0(G_{E'|E}, (E')^*)$ und bezeichnen mit δ_1 den Verbindungsisomorphismus

$$\delta_1: Hom(G_{E'|E}, \mathbb{Q}/\mathbb{Z}) = H^1(G_{E'|E}|\mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} H^2(G_{E'|E}, \mathbb{Z})$$

aus Lemma 2.14 (i). Mit Hilfe des Cupprodukts

$$\cup: H^0(G_{E'|E}, (E')^*) \times H^2(G_{E'|E}, \mathbb{Z}) \to H^2(G_{E'|E}, (E')^* \otimes_{\mathbb{Z}} \mathbb{Z}) = H^2(G_{E'|E}, (E')^*)$$

erhalten wir das Element $\bar{u} \cup \delta_1(\chi) \in H^2(G_{E'|E}, (E')^*)$. Sei $f: G_{E'|E} \times G_{E'|E} \to (E')^*$ ein 2-Kozykel, welcher $\bar{u} \cup \delta_1(\chi) \in H^2(G_{E'|E}, (E')^*)$ repräsentiert. Wir wollen nun versuchen einen Repräsentanten f explizit anzugeben. Sei dafür $s: \mathbb{Q}/\mathbb{Z} \to \mathbb{Q}$ ein beliebiger Schnitt, d.h. eine Abbildung $s: \mathbb{Q}/\mathbb{Z} \to \mathbb{Q}$, sodass für die kanonische Abbildung $can: \mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$ die Komposition $can \circ s = id_{\mathbb{Q}/\mathbb{Z}}$.

Behauptung: $g: G_{E'|E} \times G_{E'|E} \to \mathbb{Z}, (\sigma, \tau) \mapsto s \circ \chi(\sigma) + s \circ \chi(\tau) - s \circ \chi(\sigma\tau)$ ist ein wohldefinierter 2-Kozykel.
Die Wohldefiniertheit sieht man hierbei leicht, denn für alle $\sigma, \tau \in G_{E'|E}$ gilt:

$$can(g(\sigma, \tau)) = can \circ s \circ \chi(\sigma) + can \circ s \circ \chi(\tau) - can \circ s \circ \chi(\sigma\tau) = \chi(\sigma) + \chi(\tau) - \chi(\sigma\tau) = 0.$$

Damit bleibt nur noch die 2-Kozykel-Relation zu zeigen. Diese ist aber gegeben, denn für $\sigma, \tau, \rho \in G_{E'|E}$ gilt:

$$\begin{aligned} g(\sigma\tau, \rho) + g(\sigma, \tau) &= s \circ \chi(\sigma\tau) + s \circ \chi(\rho) - s \circ \chi(\sigma\tau\rho) + s \circ \chi(\sigma) + s \circ \chi(\tau) - s \circ \chi(\sigma\tau) \\ &= s \circ \chi(\tau) + s \circ \chi(\rho) + s \circ \chi(\sigma) - s \circ \chi(\sigma\tau\rho) \\ &= s \circ \chi(\tau) + s \circ \chi(\rho) - s \circ \chi(\tau\rho) + s \circ \chi(\sigma) + s \circ \chi(\tau\rho) - s \circ \chi(\sigma\tau\rho) \\ &= g(\tau, \rho) + g(\sigma, \tau\rho) \\ &= \sigma \cdot g(\tau, \rho) + g(\sigma, \tau\rho). \end{aligned}$$

Dabei gilt die letzte Gleichheit aufgrund der trivialen Operation von $G_{E'|E}$ auf $\mathbb{Z}$. Nach Konstruktion von δ_1 wird $\delta_1(\chi)$ sogar von g repräsentiert, denn $\partial_2(s \circ \chi) = g$. Dabei ist

∂_2 die Abbildung, welche sich aus dem Homomorphismus d_2 des Standardkomplexes ergibt. Nach Satz 2.21 wird damit $\bar{u} \cup \delta_1(\chi)$ durch den 2-Kozykel

$$f: G_{E'|E} \times G_{E'|E} \to (E')^* \otimes \mathbb{Z} \cong (E')^*,\ (\sigma, \tau) \mapsto u \otimes g(\sigma, \tau) \mapsto u^{g(\sigma,\tau)}$$

repräsentiert. Nach unserer Voraussetzung ist $E'|E$ endlich, d.h. $m := [E' : E] < \infty$. Dann ist $0 = \chi(1) = \chi(\sigma^m) = m\chi(\sigma)$ für alle $\sigma \in G_{E'|E}$. Also ist $\chi(G_{E'|E})$ eine Untergruppe von $\langle \frac{1}{m} + \mathbb{Z} \rangle$. Da auch $|\langle \frac{1}{m} + \mathbb{Z} \rangle| = m = |G_{E'|E}|$ und χ injektiv ist, stimmt die Gruppe $\chi(G_{E'|E})$ mit $\langle \frac{1}{m} + \mathbb{Z} \rangle$ überein. Insbesondere existiert ein $\sigma \in G_{E'|E}$ mit $\chi(\sigma) = \frac{1}{m} + \mathbb{Z}$ und $G_{E'|E} = \langle \sigma \rangle$.

Nun wollen wir den zuvor beliebig gewählten Schnitt $s: \mathbb{Q}/\mathbb{Z} \to \mathbb{Z}$ geschickt wählen, nämlich so, dass $s(\frac{k}{m} + \mathbb{Z}) = \frac{k}{m}$ für alle $k \in \{0, \dots, m-1\}$. Dann ist nämlich

$$g(\sigma^i, \sigma^j) = \begin{cases} 0, & \text{für } i + j < m, \\ 1, & \text{für } i + j \geq m \end{cases}$$

und damit

$$f(\sigma^i, \sigma^j) = \begin{cases} 1, & \text{für } i + j < m, \\ u, & \text{für } i + j \geq m, \end{cases}$$

wobei $i, j \in \{0, \dots, m-1\}$. Damit können wir auch die nach Satz 3.6 zu f gehörige Azumaya-Algebra $A(f)$ explizit angeben. Da $G_{E'|E} = \langle \sigma \rangle$ zyklisch ist mit Erzeuger σ, ist $A(f)$ gegeben durch

$$A(f) = \bigoplus_{\tau \in G_{E'|E}} E' \cdot u_\tau = \bigoplus_{i=0}^{m-1} E' \cdot u_{\sigma^i}.$$

Wegen $f(\sigma^i, \sigma^j) = 1$ für $i + j < m$ und $u_\tau \cdot u_\rho = f(\tau, \rho) u_{\tau\rho}$ für alle $\tau, \rho \in G_{E'|E}$, ist $u_\sigma^i = u_{\sigma^i}$ für alle $i \in \{0, \dots, m-1\}$. Also ist

$$A(f) = \bigoplus_{i=0}^{m-1} E' \cdot u_{\sigma^i} = \bigoplus_{i=0}^{m-1} E' \cdot t^i,$$

wobei $t := u_\sigma$. Außerdem gilt

- $t^m = u_\sigma \cdot u_{\sigma^{m-1}} = f(\sigma, \sigma^{m-1}) u_{\sigma^m} = u \cdot u_1 = u \cdot 1_{A(f)} = u$ und
- $t \cdot \beta = \sigma(\beta) t$ für alle $\beta \in E'$,

unter Berücksichtigung von Bemerkung 3.7.

4 Lokale Klassenkörpertheorie

Für das gesamte Kapitel fixieren wir mit $\tilde{F}|F_0$ eine Galoiserweiterung und setzen $G := Gal(\tilde{F}|F_0)$. Des Weiteren bezeichnen wir mit $F|F_0$ stets eine endliche Erweiterung. Ist zudem $F_0 \subset E \subset \tilde{F}$ ein Zwischenkörper, so sei fortan $G_E := Gal(\tilde{F}|E)$ und $A_E := A^{G_E}$ für einen G-Modul A. Haben wir sogar eine Körperkette $F_0 \subset F \subset E \subset \tilde{F}$ mit $E|F$ Galois, so ist $A_E = A^{G_E}$ auf natürliche Weise ein $G_{E|F} := Gal(E|F)$-Modul, da $G_{E|F} = Gal(E|F) \cong Gal(\tilde{F}|F)/Gal(\tilde{F}|E) = G_F/G_E$. Für eine endliche Galoiserweiterung $E|F$ definieren wir zudem die Notation $H^q(E|F) := H^q(G_{E|F}, A_E)$ für $q \in \mathbb{Z}$.

4.1 Klassenformationen

Definition 4.1. Eine Körperformation ist ein Paar (G, A), wobei A ein G-Modul mit

$$A = \bigcup_{\substack{F_0 \subset E \subset \tilde{F} \\ E|F \text{ endl.}}} A_E$$

ist und für jede Körperkette $F_0 \subset F \subset E \subset \tilde{F}$ mit $E|F$ endlich Galois ist $H^1(E|F) = H^1(G_{E|F}, A_E) = 0$.

Ist nun (G, A) eine Körperformation und $F_0 \subset F \subset E \subset E' \subset \tilde{F}$ eine Körperkette mit $E'|F$ und $E|F$ endlich Galois, so ist $G_{E|F} \cong G_{E'|F}/G_{E'|E}$ und $A_E = A^{G_E} = (A^{G_{E'}})^{G_E/G_{E'}} = A_{E'}^{G_{E'|E}}$. Daher haben wir die Sequenz

$$1 \longrightarrow H^2(E|F) \xrightarrow{\inf_2} H^2(E'|F) \xrightarrow{\text{res}_2} H^2(E'|E)$$

von abelschen Gruppen, welche nach Lemma 2.19 sogar exakt ist.

Definition 4.2. Sei (G, A) eine Körperformation und $F_0 \subset F \subset \tilde{F}$ ein Zwischenkörper. Wir setzen

$$H^2(\tilde{F}|F) := \varinjlim_{E} H^2(E|F)$$

als den induktiven Limes des induktiven Systems $(H^2(E|F), \inf_2 : H^2(E|F) \hookrightarrow H^2(E'|F))$, wobei E alle Zwischenkörper $F_0 \subset F \subset E \subset \tilde{F}$ durchläuft, sodass $E|F$ Galois ist.

Da alle Inflationsabbildungen injektiv sind, kann man leicht zeigen, dass auch die kanonischen Einbettungen

$$H^2(E|F) \overset{\text{can}}{\hookrightarrow} H^2(\tilde{F}|F) = \varinjlim_{E} H^2(E|F)$$

injektiv sind. Daher schreiben wir einfach $H^2(\tilde{F}|F) = \bigcup_E H^2(E|F)$.

Definition 4.3. Eine Klassenformation ist eine Körperformation (G, A) mit der folgenden Eigenschaft: Für jede Körperkette $F_0 \subset F \subset E \subset \tilde{F}$ mit $E|F$ endlich Galois existiert ein Isomorphismus

$$\text{inv}_{E|F} : H^2(E|F) \xrightarrow{\sim} \frac{1}{[E:F]}\mathbb{Z}/\mathbb{Z}$$

von abelschen Gruppen, sodass

(a) Für jede Körperkette $F_0 \subset F \subset E \subset E' \subset \tilde{F}$ mit $E'|F$ und $E|F$ endlich Galois ist $\text{inv}_{E|F} = \text{inv}_{E'|F}|_{H^2(E|F)}$, wobei $H^2(E|F) \subset H^2(E'|F)$ via inf_2 eingebettet wird;

(b) Für jede Körperkette $F_0 \subset F \subset E \subset E' \subset \tilde{F}$ mit $E'|F$ endlich Galois ist das Diagramm

$$\begin{array}{ccc} H^2(E'|F) & \xrightarrow{\text{inv}_{E'|F}} & \frac{1}{[E':F]}\mathbb{Z}/\mathbb{Z} \\ \Big\downarrow{\scriptstyle \text{res}_2} & & \Big\downarrow{\scriptstyle \cdot[E:F]} \\ H^2(E'|E) & \xrightarrow{\text{inv}_{E'|E}} & \frac{1}{[E':E]}\mathbb{Z}/\mathbb{Z} \end{array}$$

kommutativ.

Die Abbildung $\text{inv}_{E|F}$ bezeichnet man dabei als Invariantenabbildung von $E|F$.

Man beachte, dass für eine Klassenformation die Eigenschaft a) aus Definition 4.3 zu einem injektiven Gruppenhomomorphismus

$$\text{inv}_F : H^2(\tilde{F}|F) = \bigcup_E H^2(E|F) \overset{\text{inv}_{E|F}}{\xrightarrow{\sim}} \bigcup_E \frac{1}{[E:F]}\mathbb{Z}/\mathbb{Z} \hookrightarrow \mathbb{Q}/\mathbb{Z}$$

führt.

Definition 4.4. Sei (G, A) eine Klassenformation und $F_0 \subset F \subset E \subset \tilde{F}$ eine Körperkette mit $E|F$ endlich Galois. Das eindeutig bestimmte Element

$$u_{E|F} := \text{inv}_{E|F}^{-1}\left(\frac{1}{[E:F]} + \mathbb{Z}\right) \in H^2(E|F)$$

heißt Fundamentalklasse von $E|F$.

Satz 4.5. *Sei (G, A) eine Klassenformation und $F_0 \subset F \subset E \subset \tilde{F}$ eine Körperkette mit $E|F$ endlich Galois. Dann ist*

$$\begin{aligned} u_{E|F} \cup : H^q(G_{E|F}, \mathbb{Z}) &\longrightarrow H^{q+2}(E|F) \\ \delta &\longmapsto u_{E|F} \cup \delta \end{aligned}$$

ein Isomorphismus von abelschen Gruppen für alle $q \in \mathbb{Z}$.

Beweis. [Ne2], *Hauptsatz 1.7*, Seite 78. □

Korollar 4.6. *Sei (G, A) eine Klassenformation und $F_0 \subset F \subset E \subset \tilde{F}$ eine Körperkette mit $E|F$ endlich Galois. Dann gibt es einen kanonischen Isomorphismus*

$$\vartheta_{E|F} : G_{E|F}^{ab} \longmapsto A_F / N_{E|F} A_E \quad ,$$

wobei $N_{E|F} := N_{G_{E|F}}$.

Beweis. $\vartheta_{E|F}$ ist eindeutig durch das kommutative Diagramm

$$\begin{array}{ccc} H^{-2}(G_{E|F}, \mathbb{Z}) & \xrightarrow[u_{E|F}\cup]{\sim} & H^0(E|F) \\ \downarrow \wr & & \downarrow \mathrm{id} \\ G_{E|F}^{ab} & \xrightarrow[\vartheta_{E|F}]{} & A_F / N_{E|F} A_E \end{array}$$

definiert. Dabei handelt es sich bei dem linken vertikalen Homomorphismus nach Lemma 2.14 (ii) und dem oberen horizontalen Homomorphismus nach Satz 4.5 um Isomorphismen. □

Definition 4.7. Es sei die Situation aus Korollar 4.6 gegeben.

(i) $\vartheta_{E|F}^{-1} : A_F / N_{E|F} A_E \xrightarrow{\sim} G_{E|F}^{ab}$ ist der sogenannte Reziprozitätsisomorphismus der endlichen Galoiserweiterung $E|F$.

(ii) $(\cdot, E|F) : A_F \xrightarrow{\mathrm{can}} A_F / N_{E|F} A_E \xrightarrow{\vartheta_{E|F}^{-1}} G_{E|F}^{ab}$ ist das sogenannte Normrestsymbol der endlichen Galoiserweiterung $E|F$.

Mit dem folgenden Lemma möchten wir zeigen, dass eine gewisse Verbindung zwischen dem Normrestsymbol und der Invariantenabbildung besteht.

Lemma 4.8. *Sei (G, A) eine Klassenformation, $F_0 \subset F \subset E \subset \tilde{F}$ eine Körperkette mit $E|F$ endlich Galois, $a \in A_F$ und $\bar{a} := a + N_{E|F} A_E \in H^0(E|F)$. Dann gilt für jeden Charakter $\chi \in \chi(G_{E|F}) = H^1(G_{E|F}, \mathbb{Q}/\mathbb{Z})$:*

$$\chi((a, E|F)) = inv_{E|F}(\bar{a} \cup \delta_1(\chi)) \in \frac{1}{[E:F]} \mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z},$$

wobei $\delta_1 : H^1(G_{E|F}, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} H^2(G_{E|F}, \mathbb{Z})$ der Verbindungshomomorphismus aus Lemma 2.14 (i) ist.

Beweis. [Ne2], *Lemma 1.10*, Seite 78. □

Definition 4.9. Sei (G, A) eine Körperformation und $F_0 \subset F \subset \tilde{F}$ eine Körperkette. Eine Untergruppe $I \leq A_F$ heißt Normengruppe, falls ein Zwischenkörper $F \subset E \subset \tilde{F}$ mit $E|F$ endlich Galois und $I = N_{E|F}A_E$ existiert.

Satz 4.10. *Sei (G, A) eine Klassenformation und $F_0 \subset F \subset \tilde{F}$ ein Zwischenkörper. Dann ist die Abbildung*

$$\{F \subset E \subset \tilde{F} \text{ mit } E|F \text{ endl. abelsch}\} \to \{\text{Normenuntergruppen } I \leq A_F\}$$
$$E \mapsto I_E := N_{E|F}A_E$$

eine inklusionsumkehrende Bijektion

Beweis. [Ne2], *Satz 1.14*, Seite 82. □

4.2 Hauptsatz der lokalen Klassenkörpertheorie

Es sei $E|F$ eine endliche Galoiserweiterung. Dann ist sowohl die additive Gruppe $(E, +)$, als auch die multiplikative Gruppe $(E^*, \cdot)$ auf kanonische Weise ein $G_{E|F}$-Modul.

Satz 4.11 (Hilbert-Noether)**.** *Es gilt $H^1(G_{E|F}, E^*) = 0$.*

Beweis. [Ne2], *Satz 2.2*, Seite 85. □

Das gesamte Kapitel 2 über Kohomologiegruppen und Abschnitt 4.1 über Klassenformationen richtete sich nach dem Buch [Ne2]. Als nächstes möchten wir gerne die unverzweigten Erweiterungen $E|F$ untersuchen und auch dabei der Vorgehensweise von [Ne2] folgen. Es sei allerdings angemerkt, dass die folgenden Resultate in [Ne2] nur für den Fall $char(F) = 0$ bewiesen werden, obwohl diese auch in allgemeiner Form gelten, ohne Bedingungen an die Charakteristik von F zu stellen. Daher sei für den Fall $char(F) \neq 0$ an das Buch [Ser] verwiesen, welches ebenfalls zu den folgenden Resultaten kommt, allerdings mit einer anderen Herangehensweise als der Unseren.

Sei nun $E|F$ eine endliche, unverzweigte Erweiterung von lokalen Körpern, sowie $\bar{v}_2 : H^2(G_{E|F}, E^*) \to H^2(G_{E|F}, \mathbb{Z})$ der durch $v := v_E : E^* \to \mathbb{Z}$ induzierte Gruppenhomomorphismus. Des Weiteren sei $\delta_1 : H^1(G_{E|F}, \mathbb{Q}/\mathbb{Z}) \to H^2(G_{E|F}, \mathbb{Z})$ der durch die exakte Sequenz $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ induzierte Verbindungshomomorphismus und wir definieren den Gruppenhomomorphismus

$$\varphi: \chi(G_{E|F}) = H^1(G_{E|F}, \mathbb{Q}/\mathbb{Z}) \longrightarrow \frac{1}{[E:F]}\mathbb{Z}/\mathbb{Z}$$
$$\chi \longmapsto \chi(\varphi_{E|F}),$$

wobei $\varphi_{E|F}$ der in Satz 1.33 definierte Frobeniusautomorphismus von $E|F$ ist. Wie man in [Ne2] auf Seite 93 genauer nachlesen kann, handelt es sich bei $\bar{v}_2, \delta_1$ und φ sogar um Gruppenisomorphismen.

Definition 4.12. Ist $E|F$ eine unverzweigte Erweiterung von lokalen Körpern, so sei

$$\mathrm{inv}_{E|F} : H^2(G_{E|F}, E^*) \xrightarrow{\sim} \frac{1}{[E:F]}\mathbb{Z}/\mathbb{Z}$$

der durch $\mathrm{inv}_{E|F} := \varphi \circ \delta_1^{-1} \circ \bar{v}_2$ definierte Isomorphismus.

Satz 4.13. *Sei F_0 ein lokaler Körper, $\tilde{F} := {F_0}^{nr}$ die maximal unverzweigte Erweiterung von F_0, $G := Gal(\tilde{F}|F_0)$ und $A := \tilde{F}^*$. Dann ist (G, A) eine Klassenformation mit den Invariantenabbildungen aus 4.12.*

Beweis. [Ne2], *Satz 4.6*, Seite 94. □

Korollar 4.14. *Es seien alle Notationen wie zuvor in Satz 4.13. Dann ist*

$$H^2({F_0}^{nr}|F_0) = \bigcup_{\substack{F_0 \subset F \subset {F_0}^{nr} \\ F|F_0 \text{ endlich}}} H^2(Gal(F|F_0), F^*) = \bigcup_{\substack{F_0 \subset F \subset {F_0}^{nr} \\ F|F_0 \text{ endlich}}} H^2(F|F_0)$$

isomorph zu $\mathbb{Q}/\mathbb{Z}$ und zwar durch den nach Definition 4.3 eingeführten Homomorphismus $inv_{F_0} : H^2({F_0}^{nr}|F) \hookrightarrow \mathbb{Q}/\mathbb{Z}$.

Beweis. Injektivität folgt bereits aus der Bemerkung nach Definition 4.3. Für die Surjektivität beachte man, dass $\mathbb{Q}/\mathbb{Z} = \bigcup_{n\in\mathbb{N}} \frac{1}{n}\mathbb{Z}/\mathbb{Z}$ und es nach Satz 1.34 für jedes $n \in \mathbb{N}$ genau eine unverzweigte Erweiterung $F_n|F$ vom Grad n gibt. Aufgrund der Definition von inv_{F_0} und da

$$\mathrm{inv}_{F_n|F_0}(H^2(F_n|F_0)) = \frac{1}{[F_n:F_0]}\mathbb{Z}/\mathbb{Z} = \frac{1}{n}\mathbb{Z}/\mathbb{Z},$$

folgt die Surjektivität von inv_{F_0}. □

Definition 4.15. Sei F_0 ein lokaler Körper und ${F_0}^{sep}$ der separable Abschluss von F_0. Dann definieren wir

$$Br(F_0) := H^2({F_0}^{sep}|F_0) = \bigcup_{\substack{F_0 \subset F \subset {F_0}^{sep} \\ F|F_0 \text{ endl. Galois}}} H^2(Gal(F|F_0), F^*)$$

als die sogenannte *Brauergruppe* von F_0.

Satz 4.16. *Sei F_0 ein lokaler Körper, ${F_0}^{sep}$ der separable Abschluss, sowie $F_0 \subset F \subset E \subset {F_0}^{sep}$ eine Körperkette mit $F|F_0$ endlich und $E|F$ endlich Galois. Ist $F_n|F$ die eindeutige unverzweigte Erweiterung von F vom Grad $n := [E:F]$, so stimmen die beiden Gruppen $H^2(E|F)$ und $H^2(F_n|F)$ als Untergruppen von $H^2({F_0}^{sep}|F)$ überein.*

Beweis. In [Ne2], *Satz 5.2* auf Seite 99 wird der allgemeinere Fall mit einem algebraischen Abschluss von F_0 bewiesen. □

Korollar 4.17. *Sei F_0 ein lokaler Körper, dann ist*

$$Br(F_0) = H^2({F_0}^{sep}|F_0) = H^2({F_0}^{nr}|F_0) \cong \mathbb{Q}/\mathbb{Z}.$$

Beweis. Die Behauptung folgt sofort aus Satz 4.16 und Korollar 4.14. □

Definition 4.18. Sei $E|F$ eine endliche Galoiserweiterung von lokalen Körpern wie in Satz 4.16. Dann definieren wir

$$\mathrm{inv}_{E|F} : H^2(E|F) = H^2(F_n|F) \xrightarrow[\sim]{\mathrm{inv}_{F_n|F}} \frac{1}{[F_n : F]}\mathbb{Z}/\mathbb{Z} = \frac{1}{[E : F]}\mathbb{Z}/\mathbb{Z}.$$

Satz 4.19 (Hauptsatz der lokalen Klassenkörpertheorie)**.**
Sei F_0 ein lokaler Körper, $G := Gal({F_0}^{sep}|F_0)$ und $A := ({F_0}^{sep})^*$. Dann ist (G, A) eine Klassenformation mit den Invariantenabbildungen wie in Definition 4.18.

Beweis. Einen Beweis findet man in [Ne2], *Satz 5.6* auf Seite 101. Auch hier sei wieder angemerkt, dass der Beweis für einen algebraischen Abschluss $\overline{F_0}$ von F_0 und $A = (\overline{F_0})^*$ gezeigt wird, aber in völliger Analogie für $A := ({F_0}^{sep})^*$ gilt. □

5 Der Ring der Wittvektoren

Bisher haben wir zu einem diskret bewertetem Körper (F, v) mit Hilfe der diskreten Bewertung den Restklassenkörper k_F konstruiert. In diesem Kapitel stellen wir uns die Frage, ob man zu einem vorgegebenem Körper k der Charakteristik $p > 0$ einen diskret bewerteten Körper F konstruieren kann, welcher als Restklassenkörper $k_F = k$ besitzt. Man sieht sofort, dass $F = k((t))$ ein solcher Körper ist und $char(F) = p > 0$ gilt. Finden wir auch einen Körper F mit $char(F) = 0$?

5.1 Cohen-Ringe

Für das gesamte Kapitel sei p eine positive Primzahl und k ein Körper der Charakteristik p.

Definition 5.1. Ein p-Cohen-Ring für k ist ein vollständiger, diskreter Bewertungsring C mit maximalem Ideal pC und Restklassenkörper $C/pC \cong k$.

Wir haben bereits in Beispiel 1.18 gesehen, dass $\mathbb{Z}_p$ ein p-Cohen-Ring für $\mathbb{F}_p$ ist.

Lemma 5.2. *Es sei C ein p-Cohen-Ring für den Körper k. Dann ist*

$$C' := \left\{ \sum_{n \in \mathbb{Z}} c_n t^n \mid c_n \in C, \lim_{n \to -\infty} v(c_n) = \infty \right\}$$

ein p-Cohen-Ring für $k((t))$. Besitzt zudem C einen Frobenius-Lift φ, so besitzt auch C' einen Frobenius-Lift.

Beweis. Wir müssen zunächst einmal zeigen, dass es sich bei C' überhaupt um einen Ring handelt. Die Addition auf C' ist dabei komponentenweise definiert und die Multiplikation durch

$$\left(\sum_{n \in \mathbb{Z}} c_n t^n \right) \cdot \left(\sum_{m \in \mathbb{Z}} d_m t^m \right) := \sum_{l \in \mathbb{Z}} \left(\sum_{k \in \mathbb{Z}} c_k d_{l-k} \right) t^l \, .$$

Dabei ist $\sum_{k \in \mathbb{Z}} c_k d_{l-k} = \sum_{k \geq 0} c_k d_{l-k} + \sum_{k < 0} c_k d_{l-k}$ mit $\lim_{k \to \pm\infty} c_k d_{l-k} = 0$. Aufgrund der Vollständigkeit von C konvergieren die beiden Reihen in C und somit ist $\sum_{k \in \mathbb{Z}} c_k d_{l-k} \in C$ für alle $l \in \mathbb{Z}$. Außerdem ist wegen

$$v\left(\sum_{k \in \mathbb{Z}} c_k d_{l-k} \right) \geq \min_{k \in \mathbb{Z}} \{ v(c_k) + v(d_{l-k}) \} \, ,$$

$\lim_{k\to-\infty} v(c_k) = \infty$ und $\lim_{k\to\infty} v(d_{l-k}) = \infty$ auch wieder $\lim_{l\to-\infty} v(\sum_{k\in\mathbb{Z}} c_k d_{l-k}) = \infty$. Also ist die Multiplikation wohldefiniert und damit C' ein Ring.

Man betrachte nun den wohldefinierten, surjektiven Ringhomomorphismus

$$\rho\colon C' \longrightarrow k((t)),\ \sum_{n\in\mathbb{Z}} c_n t^n \longmapsto \sum_{n\in\mathbb{Z}} (c_n + pC)t^n\ .$$

Dann ist $\ker(\rho) = pC'$, also $C'/pC' \cong k((t))$ und somit insb. pC ein maximales Ideal von C'.

Als nächstes definieren wir die Abbildung $v'\colon C' \to \mathbb{N}\cup\{\infty\}$, $\sum_{n\in\mathbb{N}} c_n t^n \mapsto \min_{n\in\mathbb{Z}}\{v(c_n)\}$, für die gilt:

$$\begin{aligned} v'\Big(\sum_{n\in\mathbb{Z}} c_n t^n\Big) = m &\Leftrightarrow \forall n \in \mathbb{Z}:\ v(c_n) \geq m \text{ und } \exists n_0 \in \mathbb{Z} \text{ mit } v(c_{n_0}) = m \\ &\Leftrightarrow \forall n \in \mathbb{Z}:\ c_n \in p^m C \text{ und } \exists n_0 \in \mathbb{Z} \text{ mit } c_{n_0} \in p^m C \backslash p^{m+1} C \\ &\Leftrightarrow \sum_{n\in\mathbb{Z}} c_n t^n \in p^m C' \backslash p^{m+1} C'\ . \end{aligned}$$

Also handelt es sich bei v' um die p-adische Bewertung auf C'.

Ein weiterer Punkt, der noch zu zeigen bleibt, ist, dass C' bzgl. der p-adischen Topologie vollständig ist. Sei deshalb mit $f^{(n)} := \sum_{m\in\mathbb{Z}} c_m^{(n)} t^m \in C'$ eine Cauchyfolge gegeben. Für $i \geq 0$ sei entsprechend $N_i \in \mathbb{N}$, sodass für alle $n \geq N_i$:

$$i \leq v'\left(f^{(n)} - f^{(n+1)}\right) = \min_{m\in\mathbb{Z}} \left\{ v\left(c_m^{(n)} - c_m^{(n+1)}\right)\right\}\ . \qquad (*)$$

Fixieren wir nun ein $m \in \mathbb{Z}$, so folgt aus $(*)$, dass für alle $n \geq N_i$: $i \leq v(c_m^{(n)} - c_m^{(n+1)})$. Also ist $(c_m^{(n)})_{n\geq 0}$ eine Cauchyfolge in C und es existiert ein $c_m := \lim_{n\to\infty} c_m^{(n)} \in C$, da C vollständig ist. Wir setzen $f := \sum_{m\in\mathbb{Z}} c_m t^m$.

Behauptung 1: $f \in C'$, d.h. $\lim_{m\to-\infty} c_m = 0$.
Für $i, N_i \in \mathbb{N}$ wie zuvor wählen wir $M \geq N_i$, sodass für alle $m \geq M$: $c_m^{(N_i)} \in p^i C$. Ist nun $n \geq M$, so erhält man aus $(*)$

$$c_m^{(N_i)} - c_m^{(n)} = c_m^{(N_i)} - c_m^{(N_i+1)} + \ldots + c_m^{(n-1)} - c_m^{(n)} \in p^i C\,.$$

Also ist $c_m^{(n)} = c_m^{(N_i)} - (c_m^{(N_i)} - c_m^{(n)}) \in p^i C$ und damit $c_m = \lim_{\substack{n\to\infty \\ n\geq M}} c_m^{(n)} \in p^i C$ für alle $m \geq M$, da $p^i C$ abgeschlossen ist. Die Abgeschlossenheit von $p^i C$ sieht man dabei recht leicht, denn für eine Folge $(x_n)_n$ in $p^i C$ können wir ohne Einschränkung $\lim_{n\to\infty} x_n =: x \neq 0$ annehmen. Dann existiert ein $n \in \mathbb{N}$ mit $v(x - x_n) > v(x)$ und es gilt bereits $v(x) = \min\{v(x_n), v(x - x_n)\} = v(x_n) \geq i$.

Behauptung 2: $f = \lim_{n\to\infty} f^{(n)}$ in C' für die p-adische Topologie.
Seien wieder $i, N_i \in \mathbb{N}, n \geq N_i$ wie in $(*)$, sowie $n' \geq n$ und $m \in \mathbb{Z}$. Dann ist $v(c_m^{(n)} - c_m^{(n')}) = v(c_m^{(n)} - c_m^{(n+1)} + \ldots + c_m^{(n'-1)} - c_m^{(n')}) \geq i$, d.h. $c_m^{(n)} - c_m^{(n')} \in p^i C$. Da $n' \geq n$ beliebig war und $p^i C$ abgeschlossen ist, ist $c_m^{(n)} - c_m \in p^i C$ für alle $n \geq N_i$ und $m \in \mathbb{Z}$. Also gilt $f^{(n)} - f \in p^i C'$ für alle $n \geq N_i$, was nichts anderes bedeutet, als dass $f^{(n)}$ p-adisch gegen f konvergiert.

Als nächstes möchten wir gerne $(C')^* = C' \backslash pC'$ zeigen. Sei deshalb $f \in C'$ mit $f \notin pC' = \ker(\rho)$, d.h. $\rho(f) \neq 0$. Aufgrund der Surjektivität von ρ und da $k((t))$ ein Körper ist, existiert ein $g \in C'$ mit $1 = \rho(f)\rho(g) = \rho(fg)$. Damit ist $fg = 1 - ph$ für ein $h \in C'$. Da aber $1 - ph \in (C')^*$ mit Inversem $\sum_{i=0}^{\infty}(ph)^i$, ist auch f eine Einheit in C' mit $f^{-1} = g\sum_{i=0}^{\infty}(ph)^i$.

Damit bleibt nur noch zu zeigen, dass es sich bei C' auch um einen Hauptidealring handelt. Wie wir zuvor schon gesehen haben, ist für ein $f \in C' \backslash \{0\}$ die p-adische Bewertung wegen $\bigcap_{n\geq 0} p^n C' = 0$ gegeben durch $v'(f) = \max\{j \in \mathbb{N}_0 \mid f \in p^j C'\}$. Man sieht recht leicht, dass dann ein Ideal $I \subset C'$ mit $I \neq 0$ gegeben ist durch $I = p^j C'$, wobei $j := \min\{v(f) \mid f \in I\}$.
Also handelt es sich bei C' tatsächlich um einen p-Cohen-Ring für $k((t))$.

Ist schließlich noch $\varphi: C \to C$ eine Frobenius-Lift, so impliziert Lemma 7.6 weiter unten, wobei man W durch C und F durch φ ersetzen muss, dass auch C' einen Frobenius-Lift besitzt. □

Satz 5.3. *p-Cohen-Ringe sind bis auf Isomorphie eindeutig.*

Beweis. Einen Beweis der Aussage findet man in [Wa], *theorem 22.11* auf Seite 191. □

5.2 Wittvektoren

Wie zuvor sei durch $p > 0$ eine Primzahl fixiert. Die folgenden Ausführungen orientieren sich größtenteils an [Sch].

Definition 5.4. Für $n \in \mathbb{N}_0$ definieren wir durch

$$\Phi_n(X_0, X_1, \ldots, X_n) := \sum_{i=0}^{n} p^i X_i^{p^{n-i}} \in \mathbb{Z}[X_0, X_1, \ldots]$$

das sogenannte n-te Wittpolynom.

Definition 5.5. Sei A ein kommutativer Ring mit Einselement 1_A. Es ist $A^{\mathbb{N}_0} := \prod_{n\geq 0} A$ bzgl. der komponentenweisen Operationen ein Ring und wir definieren die Abbildungen

- $f_A: A^{\mathbb{N}_0} \to A^{\mathbb{N}_0}$, $(a_0, a_1, \ldots) \mapsto (a_1, a_2, \ldots)$;
- $v_A: A^{\mathbb{N}_0} \to A^{\mathbb{N}_0}$, $(a_0, a_1, \ldots) \mapsto (0, p \cdot a_1, p \cdot a_2, \ldots)$;
- $\Phi_n: A^{\mathbb{N}_0} \to A$, $(a_0, a_1, \ldots) \mapsto \Phi_n(a_0, \ldots, a_n)$;
- $\Phi_A: A^{\mathbb{N}_0} \to A^{\mathbb{N}_0}$, $(a_0, a_1, \ldots) \mapsto (\Phi_n(a_0, \ldots, a_n))_{n \geq 0}$.

Lemma 5.6. *Sei A ein kommutativer Ring mit Einselement 1_A.*

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

(ii) Ist $p \cdot 1_A \in A^*$, so ist Φ_A bijektiv.

Beweis. [Sch], *Lemma 5.3* auf Seite 21. □

Satz 5.7. *Sei A ein kommutativer Ring mit Einselement 1_A und $\varphi: A \to A$ ein Ringhomomorphismus mit $\varphi(x) \equiv x^p \mod pA$ für alle $x \in A$. Dann ist $A' := im(\Phi_A)$ ein Unterring von $A^{\mathbb{N}_0}$ mit $v_A(A') \subset A'$, $f_A(A') \subset A'$ und A' selbst ist gegeben durch*

$$A' = \left\{ (u_n)_{n \geq 0} \in A^{\mathbb{N}_0} \mid \forall n \geq 0 : \varphi(u_n) \equiv u_{n+1} \mod p^{n+1}A \right\}.$$

Beweis. [Sch], *Satz 5.5* auf Seite 22. □

Wir betrachten nun den Polynomring $A := \mathbb{Z}[X_0, X_1, \ldots, Y_0, Y_1, \ldots]$ in unendlich abzählbar vielen Variablen $X_0, Y_0, X_1, Y_1, \ldots$ über $\mathbb{Z}$. Des Weiteren definieren wir den Ringhomomorphismus

$$\varphi: A \to A,\ \varphi(f(X_0, X_1, \ldots, Y_0, Y_1, \ldots)) := f(X_0^p, X_1^p, \ldots, Y_0^p, Y_1^p, \ldots).$$

In A ist die Multiplikation mit p offensichtlich injektiv und $A/pA = \mathbb{F}_p[X_0, X_1, \ldots, Y_0, Y_1, \ldots]$. Da die Abbildung $(x \mapsto x^p): \mathbb{F}_p \to \mathbb{F}_p$ die Identität ist, haben wir $\varphi(f) \equiv f^p \mod pA$ und somit die Voraussetzungen von Satz 5.7 erfüllt.

Satz 5.8. *Sei $A = \mathbb{Z}[X_0, \ldots, Y_0, \ldots]$, sowie $X := (X_0, X_1, \ldots) \in A^{\mathbb{N}_0}$ und $Y := (Y_0, Y_1, \ldots) \in A^{\mathbb{N}_0}$. Dann gilt:*

(i) Es existieren eindeutig bestimmte $S = (S_n)_{n \geq 0}$, $P = (P_n)_{n \geq 0}$, $I = (I_n)_{n \geq 0}$ und $F = (F_n)_{n \geq 0}$ in $A^{\mathbb{N}_0}$, sodass
   - $\Phi_A(S) = \Phi_A(X) + \Phi_A(Y)$;
   - $\Phi_A(P) = \Phi_A(X) \cdot \Phi_A(Y)$;
   - $\Phi_A(I) = -\Phi_A(X)$;
   - $\Phi_A(F) = f_A(\Phi_A(X))$;

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

(iii) $\forall n \geq 0 : F_n \equiv X_n^p \mod pA$.

Beweis. [Sch], Seite 23. □

Mittels der Definition von Φ_A und der Eindeutigkeit in Satz 5.8 (i) sieht man sofort, dass $S_0 = X_0 + Y_0$, $P_0 = X_0 \cdot Y_0$, $I_0 = -X_0$ und $F_0 = X_0^p + pX_1$ gelten muss.

Definition 5.9. Sei B ein kommutativer Ring mit Einselement $1 = 1_B$. Wir setzen $W(B) := B^{\mathbb{N}_0}$ und definieren zwei Operationen $\boxplus$ und $\boxdot$ auf $W(B)$ wie folgt:

- $(a_n)_{n\geq 0} \boxplus (b_n)_{n\geq 0} := (S_n(a_0, a_1, \ldots, b_0, b_1, \ldots)_{n\geq 0}$;
- $(a_n)_{n\geq 0} \boxdot (b_n)_{n\geq 0} := (P_n(a_0, a_1, \ldots, b_0, b_1, \ldots)_{n\geq 0}$

für $(a_n)_{n\geq 0}, (b_n)_{n\geq 0} \in W(B)$. Des Weiteren setzen wir $0_{W(B)} := (0_B, 0_B, \ldots)$ und $1_{W(B)} := (1_B, 0_B, 0_B, \ldots)$.

Satz 5.10 (Witt)**.** *Sei B ein kommutativer Ring mit Einselement $1 = 1_B$.*

(i) *$(W(B), \boxplus, \boxdot)$ aus Definition 5.9 ist ein kommutativer Ring mit Nullelement $0_{W(B)}$, Einselement $1_{W(B)}$ und $(I_n(b_0, b_1, \ldots))_{n\geq 0}$ als additivem Inversen von $(b_n)_{n\geq 0}$.*

(ii) *Die Abbildung $\Phi_B : W(B) \to B^{\mathbb{N}_0}$, $(b_n)_{n\geq 0} \mapsto (\Phi_n(b_0, \ldots, b_n))_{n\geq 0}$ ist ein Ringhomomorphismus. Insbesondere ist $\Phi_m : W(B) \to B$, $(b_n)_{n\geq 0} \mapsto \Phi_m(b_0, \ldots, b_m)$ für alle $m \geq 0$ ein Ringhomomorphismus.*

(iii) *Für jeden Ringhomomorphismus $\rho: B_1 \to B_2$ von kommutativen Ringen mit Einselement ist*

$$W(\rho): W(B_1) \to W(B_2),\ (b_n)_{n\geq 0} \mapsto (\rho(b_n))_{n\geq 0},$$

ein Ringhomomorphismus.

Beweis. [Sch], *Satz 5.9*, Seite 25. □

Definition 5.11. Sei B ein kommutativer Ring mit Einselement $1 = 1_B$.

(i) $(W(B), \boxplus, \boxdot)$ nennt man den Ring der Wittvektoren mit Koeffizienten in B.

(ii) Die Abbildung $F: W(B) \to W(B)$, $(b_n)_{n\geq 0} \mapsto (F_n(b_0, b_1, \ldots))_{n\geq 0}$ ist der sogenannte Frobenius.

(iii) Die Abbildung $V: W(B) \to W(B)$, $(b_0, b_1, \ldots) \mapsto (b_1, b_2, \ldots)$ ist die sogenannte Verschiebung.

Lemma 5.12. *Sei B ein kommutativer Ring mit Einselement $1 = 1_B$.*

(i) *$F: W(B) \to W(B)$ ist ein Ringhomomorphismus.*

(ii) *$V: W(B) \to W(B)$ ist ein Homomorphismus von additiven Gruppen.*

(iii) $(F \circ V)(b) = p \cdot b = \underbrace{b \boxplus \ldots \boxplus b}_{p-mal}$ *für alle* $b \in W(B)$.

(iv) $V(a \boxdot F(b)) = V(a) \boxdot b$ *für alle* $a, b \in W(B)$.

(v) $F(b) \equiv b^p = \underbrace{b \boxdot \ldots \boxdot b}_{p-mal} \mod pW(B)$ *für alle* $b \in W(B)$.

Beweis. [Sch], *Satz 5.11* auf Seite 26. □

Definition 5.13. Sei B ein kommutativer Ring mit Einselement $1 = 1_B$. Für $m \geq 0$ setzen wir $V_m(B) := \mathrm{im}(V^m) = \{(b_n)_{n\geq 0} \mid b_0 = \ldots = b_{m-1} = 0\}$. Wegen Lemma 5.12 sind $V_m(B)$ Ideale von $W(B)$. Man bezeichnet mit $W_m(B) := W(B)/V_m(B)$ den Ring der Wittvektoren der Länge m.

Lemma 5.14. *Sei B ein kommutativer Ring mit Einselement $1 = 1_B$.*

(i) Für jedes $m \geq 1$ und jedes $(b_n)_{n\geq 0} \in W(B)$ gilt

$$(b_n)_{n\geq 0} = (b_0, b_1, \ldots, b_{m-1}, 0, \ldots) \boxplus (0, \ldots, 0, b_m, b_{m+1}, \ldots).$$

(ii) Die Abbildung $((b_0, \ldots, b_{m-1}) \mapsto (b_0, b_1, \ldots, b_{m-1}, 0, \ldots) \boxplus V_m(B)) \colon B^m \to W_m(B)$ ist für jedes $m \geq 1$ eine mengentheoretische Bijektion.

(iii) Mittels der Identifikation in (ii) und der Verschiebung $V \colon W(B) \to W(B)$ erhält man einen wohldefinierten Homomorphismus

$$V \colon W_{m-1}(B) \to W_m(B),\ (b_0, \ldots, b_{m-2}) \mapsto (0, b_0, \ldots, b_{m-2})\ .$$

(iv) $W(B)$ ist vollständig und separiert bzgl der durch $(V_m(B))_{m\geq 0}$ definierten Topologie.

Beweis. (i) & (ii) werden in [Sch], *Lemma 5.14* auf Seite 26 bewiesen und *(iii)* ist trivial nach der Definition von V. Für (iv) genügt es nach Satz 1.15 zu zeigen, dass die kanonische Abbildung

$$g \colon W(B) \to \varprojlim_{m\geq 0} W(B)/V_m(B),\ b \mapsto (b \boxplus V_m(B))_{m\geq 0},$$

bijektiv ist. Die Injektivität sieht man dabei aber sofort, da

$$\ker(g) = \bigcap_{m\geq 0} V_m(B) = \{(b_n)_{n\geq 0} \in W(B) \mid b_n = 0\ \forall n \geq 0\} = 0.$$

Für die Surjektivität sei $((b_0^{(m)}, b_1^{(m)}, \ldots) \boxplus V_m(B))_{m\geq 0} \in \varprojlim_{m\geq 0} W_m(B)$. Nach Definition des projektiven Limes gilt dann

$$(b_0^{(m)}, b_1^{(m)}, \ldots) \boxplus V_n(B) = (b_0^{(n)}, b_1^{(n)}, \ldots) \boxplus V_n(B) \text{ für alle } n \leq m.$$

Aus Teil (ii) erhalten wir dann schließlich $b_j^{(n)} = b_j^{(m)}$ für alle $0 \leq j < n \leq m$. Daher ist wegen (i) entsprechend $g(b) = ((b_0^{(m)}, b_1^{(m)}, \ldots) \boxplus V_m(B))_{m\geq 0}$ mit $b := (b_m^{(m+1)})_{m\geq 0} \in W(B)$ und deshalb g surjektiv. □

Lemma 5.15. *Sei B ein kommutativer Ring mit Einselement $1 = 1_B$.*

(i) Es gilt $W_1(B) \cong B$.

(ii) Die Abbildung $\tau\colon B \to W(B)$, $b \mapsto \tau(b) := (b, 0, 0, \ldots)$ ist multiplikativ.

Die in (ii) definierte Abbildung heißt Teichmüller-Lift und wir nennen $\tau(b_0)$ einen Teichmüller-Repräsentant von $b \boxplus V_1(B)$ für $b = (b_0, b_1, \ldots) \in W(B)$.

Beweis. Für (i) betrachte man den surjektiven Ringhomomorphismus $\Phi_0\colon W(B) \to B$, $(b_n)_{n\geq 0} \mapsto \Phi_0((b_n)_{n\geq 0}) = b_0$, mit $\ker(\Phi_0) = V_1(B)$, welcher entsprechend einen Isomorphismus $W_1(B) \cong B$ induziert. Die Multiplikativität in (ii) wird in [Sch], *Lemma 5.16* auf Seite 27 bewiesen. □

Wir sagen, dass ein kommutativer Ring B mit Einselement 1_B die Charakteristik p hat, falls $p \cdot 1_B = 0$ gilt in B. In diesem Fall ist $(b \mapsto b^p)\colon B \to B$ ein Ringhomomorphismus. Wir nennen B zudem perfekt, falls dieser bijektiv ist.

Satz 5.16. *Hat B die Charakteristik p, so gilt:*

(i) Für $b = (b_n)_{n\geq 0} \in W(B)$ ist $F(b) = (b_n^p)_{n\geq 0}$ und $p \cdot b = (F \circ V)(b) = (V \circ F)(b) = (0, b_0^p, b_1^p, \ldots)$;

(ii) Der Ringhomomorphismus

$$W(B) \to \varprojlim_{k\geq 1} W(B)/p^k W(B),\ b \mapsto (b \boxplus p^k W(B))_{k\geq 1}$$

ist bijektiv;

(iii) $V_m(B) \boxdot V_n(B) \subset V_{m+n}(B)$ für alle $n, m \geq 0$;

(iv) $p^k W(B) \subset V_1(B)^k \subset p^{k-1} W(B)$ für alle $k \geq 1$.

Beweis. (i) folgt direkt aus Satz 5.8 (iii) und Lemma 5.12 (iii). Einen ausführlichen Beweis der restlichen Punkte findet man in [Sch], *Satz 5.19* auf Seite 28. □

Satz 5.17. *Ist B ein perfekter Ring der Charakteristik p, so gilt:*

(i) Für $b = (b_n)_{n\geq 0} \in W(B)$ und $m \geq 1$ ist

$$b \boxplus V_m(B) = \sum_{i=0}^{m-1} p^i \tau(b_i^{p^{-i}}) \boxplus V_m(B);$$

(ii) $V_m(B) = p^m W(B) = V_1(B)^m$ *für alle* $m \in \mathbb{N}_0$.

Beweis. [Sch], *Satz 5.20* auf Seite 30. □

Satz 5.18. *Sei B ein Körper der Charakteristik p, dann gilt:*

(i) $W(B)$ *ist ein Integritätsbereich mit genau einem maximalem Ideal, nämlich* $V_1(B)$*;*

(ii) Der Ringhomomorphismus

$$W(B) \to \varprojlim_{k\geq 1} W(B)/V_1(B)^k,\ b \mapsto (b \boxplus V_1(B)^k)_{k\geq 1}$$

ist bijektiv, d.h. $W(B)$ *ist vollständig und separiert bzgl. der* $V_1(B)$*-adischen Topologie;*

(iii) Ist B zudem perfekt, so ist $W(B)$ *ein vollständiger, diskreter Bewertungsring mit maximalem Ideal* $pW(B)$ *und Restklassenkörper B. Für jedes* $b = (b_n)_{n\geq 0} \in W(B)$ *gilt außerdem*

$$b = \sum_{n=0}^{\infty} p^n \tau(b_n^{p^{-n}}) \in W(B).$$

Beweis. [Sch], *Satz 5.22* auf Seite 31. □

Lemma 5.19. *Ist B ein Körper der Charakteristik p, so hat der Quotientenkörper von* $W(B)$ *die Charakteristik 0.*

Beweis. Angenommen $char(Quot(W(B))) = l$ für eine Primzahl $l > 0$. Dann müsste wegen $B \cong W(B)/V_1(B)$ aber auch $l \cdot B = 0$ gelten und dementsprechend bereits $l = p$ sein. Das ist aber ein Widerspruch zu $p \cdot 1_{W(B)} = (0,1,0,\ldots) \neq 0_{W(B)}$ nach Satz 5.16 (i). □

Satz 5.20 (Eindeutigkeit von Wittvektoren)**.** *Sei* $(R, \mathfrak{m})$ *ein vollständiger, diskreter Bewertungsring mit perfektem Restklassenkörper k der Charakteristik* $p > 0$*. Dann gilt:*

(i) Es existiert ein eindeutiger Ringhomomorphismus $\gamma\colon W(k) \to R$ *mit* $\gamma(x) \equiv x_0 \mod \mathfrak{m}$ *für alle* $x = (x_n)_{n\geq 0} \in W(k)$*;*

(ii) γ *ist stetig und erfüllt* $\gamma((x_n)_{n\geq 0}) = \sum_{n=0}^{\infty} p^n s(x_n^{p^{-n}})$ *für alle* $(x_n)_{n\geq 0} \in W(k)$*, wobei* $s\colon k \to R$ *die in Lemma 1.22 definierte Abbildung ist;*

(iii) Ist $p \cdot 1_R \neq 0$*, so ist* γ *injektiv;*

(iv) Gilt sogar $\mathfrak{m} = p \cdot R$*, so ist* γ *bijektiv;*

Beweis. [Sch], *Satz 6.3 & Korollar 6.4* auf den Seiten 34-35. □

Korollar 5.21. *Sei $k = \mathbb{F}_{p^n}$ der endliche Körper mit p^n Elementen, d.h. insbesondere ist $char(k) = p$ und k ist perfekt. Dann ist $Quot(W(\mathbb{F}_{p^n}))$ die eindeutige unverzweigte Erweiterung von $\mathbb{Q}_p$ vom Grad n und Bewertungsring $W(\mathbb{F}_{p^n})$. Insbesondere ist damit $W(\mathbb{F}_p) \cong \mathbb{Z}_p \cong \mathcal{O}_{\mathbb{Q}_p}$.*

Beweis. $\mathbb{Q}_p$ ist ein lokaler Körper mit diskretem Bewertungsring $\mathbb{Z}_p$ und Restklassenkörper $\mathbb{F}_p$. Sei $K_n|\mathbb{Q}_p$ die eindeutige unverzweigte Erweiterung vom Grad n. Ist k_{K_n} der Restklassenkörper von K_n, so muss wegen $[k_{K_n} : \mathbb{F}_p] = [k_{K_n} : k_{\mathbb{Q}_p}] = [K_n : \mathbb{Q}_p] = n$ bereits $k_{K_n} = \mathbb{F}_{p^n}$ gelten. Aufgrund der Unverzweigtheit von $K_n|K$ ist $p\mathcal{O}_{K_n}$ das maximale Ideal des vollständigen diskreten Bewertungsrings $\mathcal{O}_{K_n}$. Also haben wir sowohl mit $\mathcal{O}_{K_n}$, als auch $W(\mathbb{F}_{p^n})$ einen vollständigen diskreten Bewertungsring mit Uniformisierer p und Restklassenkörper $\mathbb{F}_{p^n}$ gegeben. Nach Satz 5.20 ist dann $W(\mathbb{F}_{p^n}) \cong \mathcal{O}_{K_n}$ und daher $Quot(W(\mathbb{F}_{p^n})) \cong Quot(\mathcal{O}_{K_n}) = K_n$ die eindeutige unverzweigte Erweiterung von $\mathbb{Q}_p$ vom Grad n. Für den Spezialfall $n = 1$ erhält man entsprechend $W(\mathbb{F}_p) \cong \mathcal{O}_{K_1} = \mathcal{O}_{\mathbb{Q}_p} = \mathbb{Z}_p$. □

Der Einfachheit halber schreiben wir zukünftig nur noch + und · anstatt ⊞ und ⊡.

6 Fontaines Kategorienäquivalenz für lokale Körper der Charakteristik p

In diesem Kapitel möchten wir die Kategorienäquivalenz von Fontaine untersuchen, welche im Wesentlichen aussagt, dass für bestimmte Körper E die Kategorie der stetigen $\mathbb{Z}_p$-linearen Darstellungen der Galoisgruppe $Gal(E^{sep}|E)$ mit der Kategorie der etalen φ-Moduln über dem Ring $\mathcal{O}_\mathcal{E}$ übereinstimmt. Um diese Äquivalenz verstehen zu können, müssen wir zunächst alle nötigen Begrifflichkeiten erklären.

Wir fixieren für das gesamte Kapiel einen vollständigen diskret bewerteten Körper E der Charakteristik $p > 0$ mit perfektem Restklassenkörper k. In Satz 1.22 haben wir bereits gesehen, dass dann $E \cong k((t))$ gilt.

Mit $W := W(k)$ bezeichnen wir den Ring der Wittvektoren mit Koeffizienten in k, welcher nach Satz 5.18 ein p-Cohen-Ring für k ist. Des Weiteren sei durch $F: W \to W$ wie gewohnt der Frobenius auf W definiert.

In Lemma 5.2 haben wir bereits gezeigt, dass

$$\mathcal{O}_\mathcal{E} := \left\{ \sum_{n\in\mathbb{Z}} a_n t^n \mid a_n \in W, \lim_{n\to-\infty} a_n = 0 \right\}$$

ein p-Cohen-Ring von $E \cong k((t))$ ist und es einen Frobenius-Lift $\varphi: \mathcal{O}_\mathcal{E} \to \mathcal{O}_\mathcal{E}$ gibt, welcher $F: W \to W$ fortsetzt. Damit ist $\mathcal{E} := Quot(\mathcal{O}_\mathcal{E})$ ein vollständiger diskret bewerteter Körper der Charakteristik 0 mit Restklassenkörper $E = \mathcal{O}_\mathcal{E}/p\mathcal{O}_\mathcal{E}$.

Wie bereits zuvor bezeichnen wir mit $\mathcal{E}^{nr}$ die maximal unverzweigte Erweiterung von $\mathcal{E}$, was nach Satz 1.30 wieder ein diskret bewerteter Körper mit Uniformisierer p ist. Außerdem ist $\mathcal{E}^{nr}|\mathcal{E}$ Galois mit Galoisgruppe $Gal(\mathcal{E}^{nr}|\mathcal{E}) \cong Gal(E^{sep}|E) =: G_E$. Unter dieser Identifikation können wir also eine G_E-Operation auf $\mathcal{E}^{nr}$ definieren.

Da $\mathcal{E}^{nr}$ im Allgemeinen nicht vollständig ist, betrachten wir mit $\check{\mathcal{E}} := \widehat{\mathcal{E}^{nr}}$ die nach Satz 1.12 gegebene Vervollständigung von $\mathcal{E}^{nr}$ mit diskretem Bewertungsring $\mathcal{O}_{\check{\mathcal{E}}} = \mathcal{O}_{\widehat{\mathcal{E}^{nr}}} = \widehat{\mathcal{O}_{\mathcal{E}^{nr}}}$. Nach Lemma 1.31 lässt sich der Frobenius-Lift $\varphi: \mathcal{O}_\mathcal{E} \to \mathcal{O}_\mathcal{E}$ auf eindeutige Weise zu einem Frobenius-Lift auf $\mathcal{O}_{\mathcal{E}^{nr}}$ bzw. $\mathcal{O}_{\check{\mathcal{E}}}$ fortsetzen.

Für ein $\sigma \in G_E \cong Gal(\mathcal{E}^{nr}|\mathcal{E})$ ist die Einschränkung $\sigma: \mathcal{O}_{\mathcal{E}^{nr}} \to \mathcal{O}_{\mathcal{E}^{nr}}$ ein Ringhomomorphismus und damit trivialerweise stetig bzgl. der p-adischen Topologie. Also lässt sich σ auch auf die Vervollständigung von $\mathcal{O}_{\mathcal{E}^{nr}}$ fortsetzen und wir erhalten dadurch eine G_E-Operation auf $\mathcal{O}_{\mathcal{E}} = \widehat{\mathcal{O}_{\mathcal{E}^{nr}}}$.

6.1 $\mathbb{Z}_p$-Darstellungen und φ-Moduln

Definition 6.1. (i) Eine stetige $\mathbb{Z}_p$-lineare Darstellung der Galoisgruppe G_E ist ein endlich erzeugter $\mathbb{Z}_p$-Modul V, zusammen mit einer linearen und stetigen G_E-Operation $G_E \times V \to V$. Dabei wird G_E bzgl. der Krull-Topologie, V bzgl. der p-adischen Topologie und $G_E \times V$ bzgl. der Produkttopologie betrachtet.

(ii) Wir bezeichnen mit $Rep^{cont.}_{\mathbb{Z}_p}(G_E)$ die Kategorie der stetigen $\mathbb{Z}_p$-Darstellungen von G_E.

(iii) Eine $\mathbb{Z}_p$-lineare Abbildung $f: V_1 \to V_2$ zwischen zwei stetigen $\mathbb{Z}_p$-Darstellungen V_1 und V_2 von G_E heißt G_E-Homomorphismus, falls $f(\sigma \cdot v) = \sigma \cdot f(v)$ für alle $\sigma \in G_E$ und $v \in V_1$. Wir sagen, dass V_1 isomorph zu V_2 ist, falls ein G_E-Isomorphismus existiert.

Neben den stetigen $\mathbb{Z}_p$-Darstellungen von G_E wollen wir nun noch die φ-Moduln über $\mathcal{O}_{\mathcal{E}}$ einführen.

Definition 6.2. Sei R ein kommutativer Ring mit Einselement und $\varphi: R \to R$ ein Ringhomomorphismus.

(i) Ist M ein R-Modul, so heißt eine Abbildung $f: M \to M$ φ-semilinear, falls

- $f(m + m') = f(m) + f(m')$ und
- $f(r \cdot m) = \varphi(r) \cdot f(m)$

für alle $m, m' \in M$ und $r \in R$.

(ii) Ein φ-Modul über R ist ein Paar (M, f), bestehend aus einem R-Modul M zusammen mit einer φ-semilinearen Abbildung $f: M \to M$.

(iii) Seien (M, f) und (N, g) jeweils φ-Moduln über R. Ein Homomorphismus von φ-Moduln von (M, f) nach (N, g) ist dann eine R-lineare Abbildung $F: M \to N$, sodass $F \circ f = g \circ F$.

Sei wie in der vorherigen Definition R ein Ring mit Einselement, $\varphi: R \to R$ ein Ringendomorphismus und (M, f) ein φ-Modul über R. Wir betrachten nun R selbst als R-Modul via $r \bullet s := \varphi(r)s$ für $r, s \in R$. Man kann leicht zeigen, dass dann das

Tensorprodukt $R \otimes_{(R,\varphi)} M := R \otimes_R M$ via $r * (r' \otimes m) := rr' \otimes m$ auch wieder ein R-Modul ist. Nach der universellen Eigenschaft des Tensorprodukts existiert zudem eine R-lineare Abbildung

$$f_R: R \otimes_{(R,\varphi)} M \to M,\ r \otimes m \mapsto f_R(r \otimes m) := r \cdot f(m).$$

Definition 6.3. Sei R ein kommutativer Ring mit Einselement, $\varphi: R \to R$ ein Ringendomorphismus und (M, f) ein φ-Modul über R.

(i) Die R-lineare Abbildung $f_R: R \otimes_{(R,\varphi)} M \to M$ heißt R-Linearisierung von f.

(ii) Der φ-Modul (M, f) heißt etal, falls M ein endlich erzeugter R-Modul ist und es sich bei der R-Linearisierung f_R von f um eine Bijektion handelt.

(iii) Mit $\Phi_R^{\acute{e}t}$ bezeichnen wir die Kategorie der etalen φ-Moduln über R.

Lemma 6.4. *Sei R ein kommutativer Ring mit Einselement, $\varphi: R \to R$ ein Ringendomorphismus und (M, f) ein φ-Modul über R, dessen unterliegender R-Modul endlich erzeugt und frei ist mit $\{m_1, \dots, m_r\}$ als R-Basis. Ist $A_f := (a_{ij})_{1 \le i,j \le r} \in R^{r \times r}$ die durch $f(m_j) = \sum_{i=0}^{r} a_{ij} m_i$ definierte Matrix, so gilt:*

$$(M, f) \text{ ist etal } \Leftrightarrow A_f \text{ ist invertierbar in } R^{r \times r}.$$

Beweis. Da $\{m_1, \dots, m_r\}$ eine R-Basis von M ist und

$$R \otimes_{(R,\varphi)} M \ \cong\ R \otimes_{(R,\varphi)} \left(\bigoplus_{i=1}^{r} R \right) \ \cong\ \bigoplus_{i=0}^{r} \left(R \otimes_{(R,\varphi)} R \right) \ \cong\ \bigoplus_{i=0}^{r} R \ \cong\ M,$$
$$(r_i \otimes s_i)_{1 \le i \le r} \mapsto (r_i \varphi(s_i))_{1 \le i \le r}$$

ist $\{1 \otimes m_1, \dots, 1 \otimes m_r\}$ eine R-Basis von $R \otimes_{(R,\varphi)} M$. Außerdem ist $f_R(1 \otimes m_j) = 1 \cdot f(m_j) = \sum_{i=0}^{r} a_{ij} m_i$, d.h. f_R hat bzgl. der R-Basen $\{1 \otimes m_1, \dots, 1 \otimes m_r\}$ und $\{m_1, \dots, m_r\}$ die gleiche darstellende Matrix wie f. Daher gilt:

$$(M, f) \text{ ist etal } \Leftrightarrow f_R \text{ ist bijektiv } \Leftrightarrow A_f \text{ ist invertierbar.}$$

□

Von nun an sei wieder $\varphi: \mathcal{O}_\mathcal{E} \to \mathcal{O}_\mathcal{E}$ ein Frobenius-Lift und $\varphi: \mathcal{O}_{\breve{\mathcal{E}}} \to \mathcal{O}_{\breve{\mathcal{E}}}$ seine eindeutige Fortsetzung auf $\mathcal{O}_{\breve{\mathcal{E}}}$. Man beachte, dass $\varphi: \mathcal{O}_{\breve{\mathcal{E}}} \to \mathcal{O}_{\breve{\mathcal{E}}}$ mit allen $\sigma \in Gal(\mathcal{E}^{nr}|\mathcal{E}) \cong G_E$ kommutiert, da sowohl $\varphi: \mathcal{O}_{\breve{\mathcal{E}}} \to \mathcal{O}_{\breve{\mathcal{E}}}$, als auch $\sigma^{-1} \circ \varphi \circ \sigma: \mathcal{O}_{\breve{\mathcal{E}}} \to \mathcal{O}_{\breve{\mathcal{E}}}$ eine Fortsetzung von $\varphi: \mathcal{O}_\mathcal{E} \to \mathcal{O}_\mathcal{E}$ ist, aber eine solche nach Lemma 1.31 eindeutig ist.

Lemma 6.5. *(i)* $\mathcal{O}_{\breve{\mathcal{E}}}{}^{G_E} = \{x \in \mathcal{O}_{\breve{\mathcal{E}}} \mid \forall \sigma \in G_E : \sigma(x) = x\} = \mathcal{O}_\mathcal{E}$ *und* $\breve{\mathcal{E}}^{G_E} = \mathcal{E}$.

(ii) $(\mathcal{O}_{\breve{\mathcal{E}}})^{\varphi=1} = \{x \in \mathcal{O}_{\breve{\mathcal{E}}} \mid \varphi(x) = x\} \cong \mathbb{Z}_p$ *und* $(\breve{\mathcal{E}})^{\varphi=1} = \mathbb{Q}_p$.

Beweis. [Fo1], *Proposition 2.29* auf Seite 34. □

Unser Ziel ist es nun zwei Funktoren

$$\mathbb{D}\colon Rep^{cont.}_{\mathbb{Z}_p}(G_E) \longrightarrow \Phi^{\acute{e}t}_{\mathcal{O}_\mathcal{E}}\,,$$
$$\mathbb{V}\colon \Phi^{\acute{e}t}_{\mathcal{O}_\mathcal{E}} \longrightarrow Rep^{cont.}_{\mathbb{Z}_p}(G_E)$$

zu konstruieren, sodass für ein $V \in Rep^{cont.}_{\mathbb{Z}_p}(G_E)$ und $M \in \Phi_{\mathcal{O}_\mathcal{E}}$

$$\mathbb{V}(\mathbb{D}(V)) \cong V \text{ und } \mathbb{D}(\mathbb{V}(M)) \cong M$$

gilt.

6.2 Konstruktion von $\mathbb{D}$

Wir starten mit einer stetigen $\mathbb{Z}_p$-Darstellung $V \in Rep^{cont.}_{\mathbb{Z}_p}(G_E)$. Dann operiert G_E auf $\mathcal{O}_{\breve{\mathcal{E}}} \otimes_{\mathbb{Z}_p} V$ via $\sigma \otimes \sigma$ für $\sigma \in G_E$ und wir setzen

$$\mathbb{D}(V) := (\mathcal{O}_{\breve{\mathcal{E}}} \otimes_{\mathbb{Z}_p} V)^{G_E} = \{m \in \mathcal{O}_{\breve{\mathcal{E}}} \otimes_{\mathbb{Z}_p} V \mid \forall \sigma \in G_E : \sigma \cdot m = m\}.$$

Wir wollen nun zeigen, dass es sich bei $\mathbb{D}(V)$ um einen φ-Modul über $\mathcal{O}_\mathcal{E}$ und sogar um einen etalen φ-Modul über $\mathcal{O}_\mathcal{E}$ handelt.

Zunächst einmal ist klar, dass es es sich bei $\mathcal{O}_{\breve{\mathcal{E}}} \otimes_{\mathbb{Z}_p} V$ via $s * (r \otimes v) = sr \otimes v$, für $r, s \in \mathcal{O}_{\breve{\mathcal{E}}}$ und $v \in V$, um einen $\mathcal{O}_{\breve{\mathcal{E}}}$-Modul und damit wegen $\mathcal{O}_\mathcal{E} \subset \mathcal{O}_{\breve{\mathcal{E}}}$ insbesondere um einen $\mathcal{O}_\mathcal{E}$-Modul handelt. Nach Lemma 6.5 (i) ist $(\mathcal{O}_{\breve{\mathcal{E}}})^{G_E} = \mathcal{O}_\mathcal{E}$ und die G_E-Operation auf $(\mathcal{O}_{\breve{\mathcal{E}}} \otimes_{\mathbb{Z}_p} V)$ dementsprechend $\mathcal{O}_\mathcal{E}$-linear. Also ist $\mathbb{D}(V) := (\mathcal{O}_{\breve{\mathcal{E}}} \otimes_{\mathbb{Z}_p} V)^{G_E}$ ein $\mathcal{O}_\mathcal{E}$-Untermodul von $\mathcal{O}_{\breve{\mathcal{E}}} \otimes_{\mathbb{Z}_p} V$. Wegen Lemma 6.5 (ii) erhalten wir einen Gruppenhomomorphismus

$$\varphi \otimes \mathrm{id}\colon \mathcal{O}_{\breve{\mathcal{E}}} \otimes_{\mathbb{Z}_p} V \to \mathcal{O}_{\breve{\mathcal{E}}} \otimes_{\mathbb{Z}_p} V\,.$$

Ist nun $m = \sum_i \beta_i \otimes v_i \in \mathbb{D}(V)$ und $\sigma \in G_E$, so gilt

$$\begin{aligned}\sigma \cdot (\varphi \otimes \mathrm{id})(m) &= \sigma \cdot \left(\sum_i \varphi(\beta_i) \otimes v_i\right) = \sum_i \sigma \circ \varphi(\beta_i) \otimes \sigma(v_i) \\ &= \sum_i \varphi \circ \sigma(\beta_i) \otimes \sigma(v_i) = (\varphi \otimes \mathrm{id}) \left(\sum_i \sigma(\beta_i) \otimes \sigma(v_i)\right) \\ &= (\varphi \otimes \mathrm{id})(\sigma \cdot m) = (\varphi \otimes \mathrm{id})(m), \text{ da } m \in \mathbb{D}(V).\end{aligned}$$

Damit ist die Einschränkung $f := f_{\mathbb{D}(V)} := \varphi \otimes \mathrm{id}_{|_{\mathbb{D}(V)}} : \mathbb{D}(V) \to \mathbb{D}(V)$ wohldefiniert. f ist sogar φ-semilinear, denn für ein $\alpha \in \mathcal{O}_\mathcal{E}$ und $m = \sum_i \beta_i \otimes v_i \in \mathbb{D}(V)$ haben wir

$$\begin{aligned} f(\alpha m) &= (\varphi \otimes \mathrm{id}) \left(\sum_i \alpha\beta_i \otimes v_i \right) = \sum_i \varphi(\alpha\beta_i) \otimes v_i \\ &= \sum_i \varphi(\alpha)\varphi(\beta_i) \otimes v_i = \varphi(\alpha) \sum_i \varphi(\beta_i) \otimes v_i \\ &= \varphi(\alpha)(\varphi \otimes \mathrm{id}) \left(\sum_i \beta_i \otimes v_i \right) = \varphi(\alpha) f(m). \end{aligned}$$

Also haben wir für $V \in Rep^{cont.}_{\mathbb{Z}_p}(G_E)$ durch $(\mathbb{D}(V), f)$ einen φ-Modul über $\mathcal{O}_\mathcal{E}$ konstruiert.

Satz 6.6. *(i) Für $V \in Rep^{cont.}_{\mathbb{Z}_p}(G_E)$ ist die natürliche Abbildung*

$$\mathcal{O}_{\check{\mathcal{E}}} \otimes_{\mathcal{O}_\mathcal{E}} \mathbb{D}(V) \to \mathcal{O}_{\check{\mathcal{E}}} \otimes_{\mathbb{Z}_p} V, \beta \otimes \left(\sum_i \alpha_i \otimes v_i \right) \mapsto \sum_i \beta\alpha_i \otimes v_i,$$

ein Isomorphismus.

(ii) Für eine exakte Sequenz $0 \to V' \xrightarrow{g} V \xrightarrow{h} V'' \to 0$ in $Rep^{cont.}_{\mathbb{Z}_p}(G_E)$ ist auch

$$0 \longrightarrow \mathbb{D}(V') \xrightarrow{id_{\mathcal{O}_{\check{\mathcal{E}}}} \otimes g} \mathbb{D}(V) \xrightarrow{id_{\mathcal{O}_{\check{\mathcal{E}}}} \otimes h} \mathbb{D}(V'') \longrightarrow 0$$

eine wohldefinierte exakte Sequenz von φ-Moduln über $\mathcal{O}_\mathcal{E}$.

Beweis. Einen Beweis der Aussage findet man in [Fo1], *Proposition 2.30* auf Seite 34. Teil (ii) des Satzes wird dabei im Beweis selbst gezeigt. □

6.3 Konstruktion von $\mathbb{V}$

Wir starten nun von der anderen Seite, nämlich mit einem etalen φ-Modul $(M, f) \in \Phi^{ét}_{\mathcal{O}_\mathcal{E}}$. Da f entsprechend φ-semilinear ist, erhalten wir einen Gruppenhomomorphismus

$$\varphi \otimes f : \mathcal{O}_{\check{\mathcal{E}}} \otimes_{\mathcal{O}_\mathcal{E}} M \longrightarrow \mathcal{O}_{\check{\mathcal{E}}} \otimes_{\mathcal{O}_\mathcal{E}} M.$$

Wie man sofort sieht, ist auch dieser φ-semilinear, d.h. man hat mit $(\mathcal{O}_{\check{\mathcal{E}}} \otimes_{\mathcal{O}_\mathcal{E}} M, \varphi \otimes f)$ einen φ-Modul über $\mathcal{O}_{\check{\mathcal{E}}}$ gegeben. Wir setzen

$$\mathbb{V}(M) := (\mathcal{O}_{\check{\mathcal{E}}} \otimes_{\mathcal{O}_\mathcal{E}} M)^{\varphi=1} = \{x \in \mathcal{O}_{\check{\mathcal{E}}} \otimes_{\mathcal{O}_\mathcal{E}} M \mid (\varphi \otimes f)(x) = x\}$$

und wollen nun zeigen, dass es sich bei $\mathbb{V}(M)$ um eine $\mathbb{Z}_p$-Darstellung von G_E handelt.

Nach Lemma 6.5 (*ii*) ist $\mathbb{Z}_p = (\mathcal{O}_{\check{\mathcal{E}}})^{\varphi=1} \subset \mathcal{O}_{\check{\mathcal{E}}}$ und damit $\mathbb{V}(M)$ ein $\mathbb{Z}_p$-Untermodul von $\mathcal{O}_{\check{\mathcal{E}}} \otimes_{\mathcal{O}_\mathcal{E}} M$. Aus Teil (*i*) von Lemma 6.5 wissen wir, dass $\mathcal{O}_\mathcal{E} = \mathcal{O}_{\check{\mathcal{E}}}^{G_E}$, wodurch wir für jedes $\sigma \in G_E$ einen Gruppenhomomorphismus

$$\sigma \otimes \mathrm{id}_M \colon \mathcal{O}_{\check{\mathcal{E}}} \otimes_{\mathcal{O}_\mathcal{E}} M \to \mathcal{O}_{\check{\mathcal{E}}} \otimes_{\mathcal{O}_\mathcal{E}} M$$

erhalten. Damit haben wir durch $\sigma \otimes \mathrm{id}_M$ eine Gruppenoperation von G_E auf $\mathcal{O}_{\check{\mathcal{E}}} \otimes_{\mathcal{O}_\mathcal{E}} M$.

Ist nun $\sigma \in G_E$ und $m = \sum_i \beta_i \otimes m_i \in \mathbb{V}(M) = (\mathcal{O}_{\check{\mathcal{E}}} \otimes_{\mathcal{O}_\mathcal{E}} M)^{\varphi=1}$, so gilt wegen der Vertauschbarkeit von φ und σ schließlich

$$\begin{aligned}(\varphi \otimes f)(\sigma \cdot m) &= (\varphi \otimes f)\left(\sum_i \sigma(\beta_i) \otimes m_i\right) = \sum_i \varphi \circ \sigma(\beta_i) \otimes f(m_i) \\ &= \sum_i \sigma \circ \varphi(\beta_i) \otimes f(m_i) = \sigma \cdot \left(\sum_i \varphi(\beta_i) \otimes f(m_i)\right) \\ &= \sigma \cdot (\varphi \otimes f)(m) = \sigma \cdot m, \text{ da } m \in \mathbb{V}(M).\end{aligned}$$

Also schränkt sich die G_E-Operation auf $\mathcal{O}_{\check{\mathcal{E}}} \otimes_{\mathcal{O}_\mathcal{E}} M$ zu einer G_E-Operation auf $\mathbb{V}(M) = (\mathcal{O}_{\check{\mathcal{E}}} \otimes_{\mathcal{O}_\mathcal{E}} M)^{\varphi=1}$ ein.

Satz 6.7. *(i) Für $(M, f) \in \Phi^{\acute{e}t}_{\mathcal{O}_\mathcal{E}}$ ist die natürliche Abbildung*

$$\mathcal{O}_{\check{\mathcal{E}}} \otimes_{\mathbb{Z}_p} \mathbb{V}(M) \to \mathcal{O}_{\check{\mathcal{E}}} \otimes_{\mathcal{O}_\mathcal{E}} M,\ \beta \otimes \left(\sum_i \alpha_i \otimes m_i\right) \mapsto \sum_i \beta\alpha_i \otimes m_i$$

ein Isomorphismus.

(ii) Für eine exakte Sequenz $0 \to M' \xrightarrow{G} M \xrightarrow{H} M'' \to 0$ in $\Phi^{\acute{e}t}_{\mathcal{O}_\mathcal{E}}$ ist auch

$$0 \longrightarrow \mathbb{V}(M') \xrightarrow{id_{\mathcal{O}_{\check{\mathcal{E}}}} \otimes G} \mathbb{V}(M) \xrightarrow{id_{\mathcal{O}_{\check{\mathcal{E}}}} \otimes H} \mathbb{V}(M'') \longrightarrow 0$$

eine wohldefinierte exakte Sequenz von $\mathbb{Z}_p$-Moduln mit G_E-äquivarianten Homomorphismen.

Beweis. Einen Beweis der Aussage findet man in [Fo1], *Proposition 2.31* auf Seite 36. Teil (*ii*) des Satzes wird dabei im Beweis selbst gezeigt. □

6.4 Kategorienäquivalenz

Als Schlussfolgerung der vorherigen Resultate erhält man die Kategorienäquivalenz von Fontaine.

Satz 6.8 (Kategorienäquivalenz von Fontaine)**.** *Die Funktoren*

$$\mathbb{D}\colon Rep^{cont.}_{\mathbb{Z}_p}(G_E) \longrightarrow \Phi^{\acute{e}t}_{\mathcal{O}_\mathcal{E}} \qquad \textit{und} \qquad \mathbb{V}\colon \Phi^{\acute{e}t}_{\mathcal{O}_\mathcal{E}} \longrightarrow Rep^{cont.}_{\mathbb{Z}_p}(G_E)$$

sind wohldefinierte, zueinander inverse Äquivalenzen von Kategorien, d.h.

(i) für $V \in Rep^{cont.}_{\mathbb{Z}_p}(G_E)$ *ist* $V \cong \mathbb{V}(\mathbb{D}(V))$*;*

(ii) für $M \in \Phi^{\acute{e}t}_{\mathcal{O}_\mathcal{E}}$ *ist* $M \cong \mathbb{D}(\mathbb{V}(M))$*.*

Beweis. Einen Beweis der Kategorienäquivalenz findet man in [Fo1] auf Seite 36. □

7 Explizites Reziprozitätsgesetz von Fontaine-Witt für lokale Körper der Charakteristik p

7.1 Existenz eines Frobenius-Lifts auf $\mathcal{O}_\mathcal{E}$

Es sei wie in Kapitel 6 zuvor $E \cong k((t))$ ein vollständiger, diskret bewerteter Körper der Charakteristik p mit perfektem Restklassenkörper k. Wie wir bereits gesehen haben, ist dann $W := W(k)$ ein p-Cohen-Ring von k und $\mathcal{O}_\mathcal{E} = \{\sum_{n\in\mathbb{Z}} a_n t^n \mid a_n \in W, \lim_{n\to-\infty} a_n = 0\}$ ein p-Cohen-Ring von E. Den Ring $\mathcal{O}_\mathcal{E}$ haben wir bisher immer bezüglich der p-adischen Topologie betrachtet, wollen im Folgenden aber $\mathcal{O}_\mathcal{E}$ mittels der schwachen Topologie untersuchen.

Definition 7.1. Die schwache Topologie auf $\mathcal{O}_\mathcal{E}$ ist definiert durch:

$$U \subset \mathcal{O}_\mathcal{E} \text{ ist offen } \Leftrightarrow \forall u \in U\, \exists n, m \in \mathbb{N}_0 :\ u + p^n\mathcal{O}_\mathcal{E} + t^m W[[t]] \subset U\,.$$

Man sieht dabei recht leicht, dass es sich bei der schwachen Topologie tatsächlich um eine Topologie auf $\mathcal{O}_\mathcal{E}$ handelt.

Lemma 7.2. *Die schwache Topologie auf $\mathcal{O}_\mathcal{E}$ besitzt die folgenden Eigenschaften:*

(i) $(U_{nm} := p^n\mathcal{O}_\mathcal{E} + t^m W[[t]])_{n,m\geq 0}$ *ist eine offene Umgebungsbasis von* $0 \in \mathcal{O}_\mathcal{E}$*;*

(ii) $\mathcal{O}_\mathcal{E}$ *ist bzgl. der schwachen Topologie ein topologischer Ring;*

(iii) die schwache Topologie ist gröber als die p-adische Topologie;

(iv) $\mathcal{O}_\mathcal{E}$ *ist bzgl. der schwachen Topologie vollständig und separiert.*

Beweis. (i) ist klar mit der Definition der schwachen Topologie. Für (ii) setzen wir

- $P\colon \mathcal{O}_\mathcal{E} \times \mathcal{O}_\mathcal{E} \to \mathcal{O}_\mathcal{E}$, $(\alpha, \beta) \mapsto \alpha \cdot \beta$;
- $S\colon \mathcal{O}_\mathcal{E} \times \mathcal{O}_\mathcal{E} \to \mathcal{O}_\mathcal{E}$, $(\alpha, \beta) \mapsto \alpha + \beta$;
- $I\colon \mathcal{O}_\mathcal{E} \to \mathcal{O}_\mathcal{E}$, $\alpha \mapsto -\alpha$.

Um zu zeigen, dass $\mathcal{O}_\mathcal{E}$ ein topologischer Ring ist, müssen wir die Stetigkeit von I, S und P nachweisen. Sei deshalb $U \subset \mathcal{O}_\mathcal{E}$ eine bzgl. der schwachen Topologie offene Teilmenge von $\mathcal{O}_\mathcal{E}$. Damit ist aber auch trivialerweise $-U = I^{-1}(U)$ offen und entsprechend I stetig bzgl. der schwachen Topologie.
Wähle nun ein $(u,v) \in S^{-1}(U) \subset \mathcal{O}_\mathcal{E} \times \mathcal{O}_\mathcal{E}$, d.h. $u+v \in U$. Also existieren $n, m \in \mathbb{N}_0$, sodass $(u+v) + U_{nm} \subset U$. Wir setzen $W_u := u + U_{nm}$ und $W_v := v + U_{nm}$ und haben damit jeweils eine offene Umgebung von u bzw. v. Insbesondere gilt für $x = u + p^n a_u + t^m f_u \in W_u$ und $y = v + p^n a_v + t^m f_v \in W_v$, mit $a_u, a_v \in \mathcal{O}_\mathcal{E}$, $f_u, f_v \in W[[t]]$:

$$x + y = (u+v) + p^n(a_u + a_v) + t^m(f_u + f_v) \in (u+v) + U_{nm} \subset U.$$

Somit ist $(u,v) \in W_u \times W_v \subset S^{-1}(U)$, also $S^{-1}(U)$ offen und schließlich S stetig.
Um letztlich noch die Stetigkeit von P zu zeigen, sei $(u,v) \in P^{-1}(U)$, d.h. $u \cdot v \in U$. Es existieren $n, m \in \mathbb{N}_0$, sodass $u \cdot v + U_{nm} \subset U$. Da $u, v \in \mathcal{O}_\mathcal{E}$, lassen sich u und v in der Form $u = \sum_{k\in\mathbb{Z}} a_k t^k$ und $v = \sum_{k\in\mathbb{Z}} b_k t^k$ schreiben und es existieren $N_u, N_v \in \mathbb{Z}$, sodass $Q_u := \sum_{k<N_u} a_k t^k = p^n H_u \in p^n\mathcal{O}_\mathcal{E}$ und $Q_v := \sum_{k<N_v} b_k t^k = p^n H_v \in p^n\mathcal{O}_\mathcal{E}$ für geeignete $H_u, H_v \in \mathcal{O}_\mathcal{E}$. Wir setzen $P_u := \sum_{k\geq N_u} a_k t^k$, $P_v := \sum_{k\geq N_v} b_k t^k$, $M := \max\{m + |N_u|, m + |N_v|\}$, $W_u := u + U_{nM}$ und $W_v := v + U_{nM}$. Nach Wahl von M ist dann $t^{M-m}P_u \in W[[t]]$ und $t^{M-m}P_v \in W[[t]]$. Für $(x,y) \in W_u \times W_v$ existieren jeweils $g_u, g_v \in \mathcal{O}_\mathcal{E}$, $f_u, f_v \in W[[t]]$ mit $x = u + p^n g_u + t^M f_u$ und $y = v + p^n g_v + t^M f_v$. Damit gilt:

$$\begin{aligned}
P(x,y) = x \cdot y &= (u + p^n g_u + t^M f_u) \cdot (v + p^n g_v + t^M f_v) \\
&= u \cdot v + p^n \underbrace{(ug_v + g_u v + p^n g_u g_v + g_u t^M f_v + t^M f_u g_v)}_{=:G\in\mathcal{O}_\mathcal{E}} + t^M(vf_u + uf_v + t^M f_u f_v) \\
&= u \cdot v + p^n(G + H_v f_u t^M + H_u f_v t^M) + t^m(t^{M-m}P_v f_u + t^{M-m}P_u f_v + t^M f_u f_v) \\
&\in u \cdot v + p^n\mathcal{O}_\mathcal{E} + t^m W[[t]] = u \cdot v + U_{nm} \subset U.
\end{aligned}$$

Also ist $(u,v) \in W_u \times W_v \subset P^{-1}(U)$, damit $P^{-1}(U)$ offen und entsprechend P stetig bezüglich der schwachen Topologie.

Für (iii) sei $U \subset \mathcal{O}_\mathcal{E}$ offen bezüglich der schwachen Topologie. Wegen $p^n\mathcal{O}_\mathcal{E} \subset U_{nm}$ für alle $n, m \in \mathbb{N}_0$ sieht man aber sofort, dass U auch bzgl. der p-adischen Topologie offen sein muss, also die schwache Topologie gröber ist als die p-adische Topologie.

Für (iv) zeigen wir zunächst die Separiertheit von $\mathcal{O}_\mathcal{E}$. Sei dafür $\sum_{k\in\mathbb{Z}} a_k t^k \in \mathcal{O}_\mathcal{E}\backslash\{0\}$, d.h. es existiert ein $k_0 \in \mathbb{Z}$ mit $0 \neq a_{k_0} = (a_{k_0}^{(r)})_{r\geq 0} \in W = W(k)$. Also muss es ein $r_0 \geq 0$ geben, sodass $a_{k_0}^{(r_0)} \neq 0$, d.h. insbesondere $a_{k_0} \notin V_{r_0}(k) = p^{r_0}W(k)$. Angenommen $\sum_{k\in\mathbb{Z}} a_k t^k \in U_{r_0 m}$ für $m := \max\{k_0 + 1, 0\}$. Dann gäbe es für alle $k < m$ geeignete $c_k \in W(k)$ mit $a_k = p^{r_0}c_k$. Insbesondere wäre damit $a_{k_0} = p^{r_0}c_{k_0} \in p^{r_0}W$, da $k_0 < m$. Das ist jedoch ein Widerspruch und somit kann $\sum_{k\in\mathbb{Z}} a_k t^k$ kein Element von $U_{r_0 m}$ sein. Also ist $\bigcap_{n,m\in\mathbb{N}_0} U_{nm} = \{0\}$, was äquivalent zu der Separiertheit von $\mathcal{O}_\mathcal{E}$ ist.

Um die Vollständigkeit von $\mathcal{O}_\mathcal{E}$ zu zeigen, wählen wir mit $(f_r)_{r\in\mathbb{N}}$ eine Cauchyfolge in $\mathcal{O}_\mathcal{E}$. Damit gilt:

$$\forall n, m \in \mathbb{N}\ \exists R \in \mathbb{N}\ \forall r \geq R: \quad f_r - f_R \in U_{nm}.$$

Für die Koeffizienten von $f_r := \sum_{k\in\mathbb{Z}} a_k^{(r)} t^k \in \mathcal{O}_\mathcal{E}$ gilt dann

$$a_k^{(r)} - a_k^{(R)} \in p^n W \text{ für alle } r \geq R \text{ und } k < m.$$

Da wir $m \in \mathbb{N}$ beliebig groß wählen können, ist $(a_k^{(r)})_{r\in\mathbb{N}}$ für jedes $k \in \mathbb{Z}$ eine Cauchyfolge in W. Nach Lemma 5.18 (*iii*) ist W vollständig bzgl. der p-adischen Topologie und dementsprechend existiert ein $a_k \in W$ mit $a_k = \lim_{r\to\infty} a_k^{(r)}$. Wir setzen $f := \sum_{k\in\mathbb{Z}} a_k t^k$.

Behauptung 1: $f \in \mathcal{O}_\mathcal{E}$, d.h. $\lim_{k\to-\infty} a_k = 0$.
Für $n \in \mathbb{N}$ existiert ein $R \in \mathbb{N}$, sodass $f_r - f_R \in U_{n0}$ für alle $r \geq R$. Insbesondere ist dann $a_k^{(r)} - a_k^{(R)} \in p^n W$ für alle $k < 0$. Da $f_R \in \mathcal{O}_\mathcal{E}$, existiert zudem ein $M \geq R$, sodass $a_k^{(R)} \in p^n W$ für alle $k \leq -M$. Also gilt

$$\forall r \geq M,\ \forall k \leq -M: \quad a_k^{(r)} = a_k^{(R)} + a_k^{(r)} - a_k^{(R)} \in p^n W$$

und man erhält daraus

$$\forall k \leq -M: \quad a_k = \lim_{\substack{r\to\infty \\ r\geq M}} a_k^{(r)} \in p^n W,$$

da $p^n W$ abgeschlossen ist. Somit gilt $\lim_{k\to-\infty} a_k = 0$, d.h. $f \in \mathcal{O}_\mathcal{E}$.

Behauptung 2: f_r konvergiert bzgl. der schwachen Topologie gegen f.
Für $n, m \in \mathbb{N}$ existiert ein $R \in \mathbb{N}$, sodass für alle $M, N \geq R$

$$f_N - f_M = \sum_{k\in\mathbb{Z}} (a_k^{(N)} - a_k^{(M)}) t^k \in p^n \mathcal{O}_\mathcal{E} + t^m W[[t]].$$

Somit ist $a_k^{(N)} - a_k^{(M)} \in p^n W$ für alle $k < m$ und $N, M \geq R$. Da wir M beliebig groß wählen können und $p^n W$ abgeschlossen ist, gilt

$$a_k^{(N)} - a_k = \lim_{M\to\infty} a_k^{(N)} - a_k^{(M)} \in p^n W \text{ für alle } N \geq R \text{ und } k < m,$$

woraus

$$f_N - f = \underbrace{\sum_{k<m} (a_k^{(N)} - a_k) t^k}_{\in p^n \mathcal{O}_\mathcal{E}} + \underbrace{\sum_{k\geq m} (a_k^{(N)} - a_k) t^k}_{t^m W[[t]]} \in p^n \mathcal{O}_\mathcal{E} + t^m W[[t]]$$

für alle $N \geq R$ folgt. Also gilt $\lim_{r\to\infty} f_r = f$ in der schwachen Topologie und dementsprechend ist $\mathcal{O}_\mathcal{E}$ auch bzgl. der schwachen Topologie vollständig. □

Lemma 7.3. *Sei $s \in \mathcal{O}_\mathcal{E}$, sodass $s \mod p\mathcal{O}_\mathcal{E} \in (t \cdot k[[t]]) \backslash \{0\}$. Dann existiert genau ein bzgl. der schwachen Topologie stetiger Ringhomomorphismus $\varphi_s : \mathcal{O}_\mathcal{E} \to \mathcal{O}_\mathcal{E}$ mit $\varphi_s(t) = s$ und $\varphi_{s|_W} = id_W$.*

Beweis. Da $s = \sum_{n\in\mathbb{Z}} a_n t^n$ modulo p in $(t \cdot k[[t]]) \backslash \{0\}$ liegt, existiert ein $K \in \mathbb{N}$ mit $a_K \in W^* = W \backslash pW$ und $a_n \in pW$ für alle $n < K$. Also lässt sich s schreiben als $s = p \cdot v + t^K \cdot u$ mit geeignetem $v \in \mathcal{O}_\mathcal{E}$ und $u := \sum_{n=K}^{\infty} a_n t^{n-K} \in W[[t]]^*$. Setzen wir $r := v \cdot t^{-K} \cdot u^{-1} \in \mathcal{O}_\mathcal{E}$, so ist $s = (1 + p \cdot r)t^K u$.

Behauptung 1: $(s^m)_{m\in\mathbb{N}}$ ist eine Nullfolge in der schwachen Topologie.
Es seien N, M zwei beliebige natürliche Zahlen. Da r ein Element von $\mathcal{O}_\mathcal{E}$ ist, existieren $L \in \mathbb{N}$, $r' \in \mathcal{O}_\mathcal{E}$ und $r'' \in W[[t]]$, sodass $r = p^N r' + t^{-L} r''$. Wählen wir nun $m \geq M + (N-1)L$, so gilt

$$\begin{aligned} s^m = (1+pr)^m t^{Km} u^m &= \sum_{i=0}^{m} \binom{m}{i} p^i r^i t^{Km} u^m \\ &\equiv \sum_{i=0}^{N-1} \binom{m}{i} p^i t^{-Li} r''^i t^{Km} u^m \mod p^N \mathcal{O}_\mathcal{E} \\ &\equiv \underbrace{\sum_{i=0}^{N-1} \binom{m}{i} p^i r''^i t^{Km-Li} u^m}_{\in t^{Km-L(N-1)} W[[t]] \subset t^M W[[t]]} \mod p^N \mathcal{O}_\mathcal{E}. \end{aligned}$$

Also ist $s^m \in U_{NM}$ und damit $(s^m)_{m\in\mathbb{N}}$ eine schwache Nullfolge in $\mathcal{O}_\mathcal{E}$.

Nach unseren Voraussetzungen ist $s \mod p\mathcal{O}_\mathcal{E} \neq 0$ und damit $s \in \mathcal{O}_\mathcal{E} \backslash p\mathcal{O}_\mathcal{E} = \mathcal{O}_\mathcal{E}^*$. Daher macht es Sinn von s^{-1} zu sprechen. Haben wir nun ein $f = \sum_{k\in\mathbb{Z}} a_k t^k \in \mathcal{O}_\mathcal{E}$ gegeben, so setzen wir $f_N := \sum_{k=-N}^{N} a_k s^k$.

Behauptung 2: $(f_N)_{N\in\mathbb{N}}$ ist eine Cauchyfolge in $\mathcal{O}_\mathcal{E}$.
Seien dafür wieder n, m zwei beliebige natürliche Zahlen. Da $(s^k)_{k\in\mathbb{N}}$ eine Nullfolge ist, existiert ein $R_1 \in \mathbb{N}$ mit $s^k \in U_{nm}$ für alle $k \geq R_1$. Zudem gibt es wegen $f \in \mathcal{O}_\mathcal{E}$ ein $R_2 \in \mathbb{N}$ mit $a_k \in p^n W$ für alle $k \leq -R_2$. Damit gilt für alle $N, M \geq R := \max\{R_1, R_2\}$:

$$f_M - f_N = \sum_{k=-M}^{-N} a_k s^k + \sum_{k=N}^{M} a_k s^k \in U_{nm},$$

wobei wir o.B.d.A. $M \geq N$ vorausgesetzt haben. Also handelt es sich bei $(f_N)_{N\in\mathbb{N}}$ um eine Cauchyfolge in $\mathcal{O}_\mathcal{E}$. Wie wir bereits in Lemma 7.2 (iv) gezeigt haben, existiert ein eindeutiger Grenzwert $\sum_{k\in\mathbb{Z}} a_k s^k$ von $(f_N)_{N\in\mathbb{N}}$ in $\mathcal{O}_\mathcal{E}$. Damit ist die Abbildung

$$\varphi_s : \mathcal{O}_\mathcal{E} \to \mathcal{O}_\mathcal{E};\ \sum_{k\in\mathbb{Z}} a_k t^k \mapsto \sum_{k\in\mathbb{Z}} a_k s^k,$$

wohldefiniert. Da zudem $\mathcal{O}_\mathcal{E}$ ein topologischer Ring ist, sind die Grenzwertbildung und Ringoperationen vertauschbar und es handelt sich bei φ_s um einen Ringhomomorphismus.

Behauptung 3: φ_s ist stetig bzgl. der schwachen Topologie auf $\mathcal{O}_\mathcal{E}$.
Sei dafür $U \subset \mathcal{O}_\mathcal{E}$ offen und $f \in {\varphi_s}^{-1}(U)$, d.h. $f(s) \in U$. Somit existieren $N, M \in \mathbb{N}_0$ mit $f(s) + U_{NM} \subset U$. Wie zuvor schreiben wir $s = (1+pr)t^K u$ und $r = p^N r' + t^{-L} r''$, wobei ohne Einschränkung $L \geq K$ sein soll. Da $(s^k)_{k\geq 0}$ eine Nullfolge ist, gibt es ein $m \in \mathbb{N}$, sodass $s^m \in p^N\mathcal{O}_\mathcal{E} + t^{M+L(N-1)}W[[t]]$. Es gibt also ein $G \in W[[t]]$ mit $s^m \equiv t^{M+L(N-1)}G \mod p^N\mathcal{O}_\mathcal{E}$. Sei nun $f + p^N g + t^m h \in f + U_{Nm}$ mit $g \in \mathcal{O}_\mathcal{E}$ und $h = \sum_{n\geq 0} b_n t^n \in W[[t]]$. Man beachte:

$$\begin{aligned} h(s) &= \sum_{n\geq 0} b_n s^n = \sum_{n\geq 0} b_n (1+pr)^n t^{Kn} u^n \\ &= \sum_{n\geq 0}\sum_{k=0}^{n} \binom{n}{k} p^k r^k t^{Kn} u^n \equiv \sum_{n\geq 0}\sum_{\substack{k=0 \\ k<N}}^{n} \binom{n}{k} p^k r^k t^{Kn} u^n \mod p^N\mathcal{O}_\mathcal{E} \\ &= \underbrace{\sum_{n\geq 0}\sum_{\substack{k=0 \\ k<N}}^{n} \binom{n}{k} p^k r''^k t^{Kn-Lk} u^n}_{\in t^{K(N-1)-L(N-1)}W[[t]]} \mod p^N\mathcal{O}_\mathcal{E}. \end{aligned}$$

Also existiert ein $H \in W[[t]]$ mit $h(s) \equiv t^{K(N-1)-L(N-1)}H \mod p^N\mathcal{O}_\mathcal{E}$. Zusammen mit $s^m \equiv t^{M+L(N-1)}G \mod p^n\mathcal{O}_\mathcal{E}$ erhält man dann

$$s^m h(s) \equiv \underbrace{t^{M+K(N-1)}GH}_{\in t^M W[[t]]} \mod p^N\mathcal{O}_\mathcal{E}. \qquad (*)$$

Damit folgt schließlich

$$\varphi_s(f + p^N g + t^m h) = f(s) + p^N g(s) + s^m h(s) \in \underbrace{f(s) + p^N\mathcal{O}_\mathcal{E} + t^M W[[t]]}_{\subset U} \text{ nach } (*),$$

woraus die Stetigkeit von φ_s folgt.

Behauptung 4: $W[t][t^{-1}]$ liegt dicht in $\mathcal{O}_\mathcal{E}$ bzgl. der schwachen Topologie.
Dafür wählen wir eine offene Menge $U \subset \mathcal{O}_\mathcal{E}, U \neq \varnothing$, und ein $F = \sum_{k\in\mathbb{Z}} b_k t^k \in U$. Dann existieren $N, M \in \mathbb{N}$ mit $F + U_{NM} \subset U$. Da $F \in \mathcal{O}_\mathcal{E}$, existiert zudem ein $R \in \mathbb{Z}$, sodass $\sum_{k<R} b_k t^k \in p^N\mathcal{O}_\mathcal{E}$. Schließlich erhalten wir daraus

$$\underbrace{\sum_{k=R}^{M} b_k t^k}_{\in W[t][t^{-1}]} = F - \underbrace{\sum_{k<R} b_k t^k}_{\in p^N\mathcal{O}_\mathcal{E}} + \underbrace{\sum_{k>M} b_k t^k}_{\in t^M W[[t]]} \in F + U_{NM} \subset U.$$

Also ist $U \cap W[t][t^{-1}] \neq \varnothing$ und somit $W[t][t^{-1}]$ dicht in $\mathcal{O}_\mathcal{E}$ bzgl. der schwachen Topologie.

Behauptung 5: φ_s ist eindeutig.
Angenommen es existiert ein weiterer stetiger Ringhomomorphismus $\psi: \mathcal{O}_\mathcal{E} \to \mathcal{O}_\mathcal{E}$ mit $\psi(t) = s = \varphi_s(t)$ und $\psi_{|_W} = id_W$. Aufgrund der W-Linearität von ψ und φ_s ist dann bereits $\varphi_{s|_{W[t][t^{-1}]}} = \psi_{|_{W[t][t^{-1}]}}$. Da $\mathcal{O}_\mathcal{E}$ separiert ist, ist $\{0\}$ abgeschlossen in $\mathcal{O}_\mathcal{E}$. Wegen der Stetigkeit von ψ und φ_s ist dann auch $\ker(\psi - \varphi_s) = (\psi - \varphi_s)^{-1}(\{0\})$ abgeschlossen mit $W[t][t^{-1}] \subset \ker(\psi - \varphi_s)$. Wie wir aber zuvor gezeigt haben, liegt $W[t][t^{-1}]$ dicht in $\mathcal{O}_\mathcal{E}$ und somit gilt bereits $\mathcal{O}_\mathcal{E} = \overline{W[t][t^{-1}]} \subset \ker(\psi - \varphi_s) \subset \mathcal{O}_\mathcal{E}$ bzw. $\psi = \varphi_s$. □

Wir wissen also jetzt, dass wir für ein gegebenes $s \in \mathcal{O}_\mathcal{E}$ mit $s \mod p\mathcal{O}_\mathcal{E} \in (t \cdot k[[t]]) \backslash \{0\}$ einen Ringhomomorphismus $\varphi_s: \mathcal{O}_\mathcal{E} \to \mathcal{O}_\mathcal{E}$ konstruieren können, sodass $\varphi_s(t) = s$ gilt. Im nächsten Schritt möchten wir gerne zeigen, dass es sich bei φ_s sogar um einen Isomorphismus handelt, falls $s \mod p\mathcal{O}_\mathcal{E}$ ein Uniformisierer von $E \cong k((t))$ ist.

Satz 7.4. *Für $g = \sum_{n\geq 1} \alpha_n t^n \in t \cdot k[[t]]$ existiert genau ein Ringhomomorphismus $\varphi_g: k[[t]] \to k[[t]]$, $\sum_{k\geq 0} a_k t^k \mapsto \sum_{k\geq 0} a_k g^k$, für den gilt:*

$$\varphi_g \text{ ist ein Isomorphismus } \Leftrightarrow \alpha_1 \neq 0.$$

Beweis. Der Fall $g = 0$ ist hierbei trivial und wir können ohne Einschränkung $g \neq 0$ annehmen. Da $k[[t]]$ bzgl. der t-adischen Topologie vollständig und separiert ist und $g \in t \cdot k[[t]]$, handelt es sich bei $(a_m g^m)_{m\geq 0}$ um eine t-adische Nullfolge in $k[[t]]$ für beliebige $a_m \in k$. Also konvergiert die Reihe $\sum_{m\geq 0} a_m g^m$ eindeutig in $k[[t]]$ und wir erhalten eine wohldefinierte Abbildung

$$\varphi_g: k[[t]] \to k[[t]], \sum_{m\geq 0} a_m t^m \mapsto \sum_{m\geq 0} a_m g^m.$$

Da es sich zudem bei $\varphi_{g_{|_{k[t]}}}$ um einen Ringhomomorphismus handelt und $k[t]$ dicht in $k[[t]]$ liegt, ist auch φ_g ein Ringhomomorphismus, denn $k[[t]]$ ist ein topologischer Ring. Aufgrund der Dichtheit von $k[t] \subset k[[t]]$ ist φ_g eindeutig durch $\varphi_g(t) = g$ und $\varphi_{g_{|_k}} = id$ bestimmt. Setzen wir $s := \sum_{n\geq 1} \tau(\alpha_n) t^n \in t \cdot W[[t]]$, wobei $\tau: k \to W$ der Teichmüller-Lift ist, so gilt $s \mod p\mathcal{O}_\mathcal{E} = g$. Wegen der Eindeutigkeit von φ_g muss dann $\varphi_g = (\varphi_s \mod p\mathcal{O}_\mathcal{E})$ gelten, wobei φ_s der nach Lemma 7.3 konstruierte Ringhomomorphismus ist.

Wir nehmen nun an, dass φ_g ein Isomorphismus ist, d.h. es existiert ein $f = \sum_{r\geq 0} a_r t^r \in k[[t]]$ mit $t = \varphi_g(f) = \sum_{r\geq 0} a_r g^r =: \sum_{n\geq 0} b_n t^n$. Dabei ist $1 = b_1 = a_1 \cdot \alpha_1$, also $\alpha_1 \in k^* = k \backslash \{0\}$.

Sei nun umgekehrt $\alpha_1 \neq 0$. Ist $f \in k[[t]] \backslash \{0\}$, so lässt sich f schreiben als $f = t^n u$ mit $n \geq 0$ und $u \in k[[t]]^*$. Dann ist aber auch $\varphi_g(u) \in k[[t]]^*$, $g^n \neq 0$, da $\alpha_1 \neq 0$ und somit

$\varphi_g(f) = g^n \cdot \varphi_g(u) \neq 0$. Also gilt $\ker(\varphi_g) = \{0\}$ bzw. φ_g ist injektiv.
Um die Surjektivität von φ_g zu zeigen, wählen wir ein beliebiges $b = \sum_{n\geq 0} b_n t^n \in k[[t]]$ und zeigen zunächst die folgende Aussage:

$$\text{Es existieren } a_0, a_1, \ldots \in k, \text{ sodass } \sum_{n=0}^{m} b_n t^n \equiv \sum_{n=0}^{m} a_n g^n \mod t^{m+1} \text{ für alle } m \in \mathbb{N}_0.$$

Wir zeigen die Behauptung per Induktion über m. Für $m = 0$ ist die Kongruenz mit $a_0 := b_0$ gegeben und wir nehmen im Folgenden an, dass die Aussage für ein $m \in \mathbb{N}$ erfüllt ist. Das bedeutet, es existieren $a_0, \ldots, a_m \in k$ und ein $h := \sum_{n\geq 0} c_n t^n \in k[[t]]$ mit

$$\sum_{n=0}^{m} b_n t^n = \sum_{n=0}^{m} a_n g^n + t^{m+1} h.$$

Da $\alpha_1 \neq 0$ vorausgesetzt ist, setzen wir $a_{m+1} := \alpha_1^{-(m+1)}(b_{n+1} + c_0)$. Damit gilt:

$$\begin{aligned}
\sum_{n=0}^{m+1} a_n g^n &= \sum_{n=0}^{m} a_n g^n + a_{m+1} g^{m+1} = \sum_{n=0}^{m} b_n t^n - t^{m+1} h + a_{m+1} g^{m+1} \\
&= \sum_{n=0}^{m} b_n t^n + t^{m+1} \left(a_{m+1} \left(\sum_{k\geq 1} \alpha_k t^{k-1} \right)^{m+1} - \sum_{k\geq 0} c_k t^k \right) \\
&\equiv \sum_{n=0}^{m} b_n t^n + t^{m+1}(a_{m+1}\alpha_1^{m+1} - c_0) \mod t^{m+2} \\
&\equiv \sum_{n=0}^{m+1} b_n t^n \mod t^{m+2}, \text{ nach Wahl von } a_{m+1}.
\end{aligned}$$

Also gilt die Behauptung und es ist $\sum_{n\geq 0} b_n t^n - \varphi_g(\sum_{n\geq 0} a_n t^n) \in \bigcap_{m\geq 0} t^{m+1} k[[t]] = \{0\}$. Damit ist φ_g surjektiv und schließlich insgesamt ein Isomorphismus. □

Korollar 7.5. *Sei $s \in \mathcal{O}_\mathcal{E}$, sodass $s \mod p\mathcal{O}_\mathcal{E}$ ein Uniformisierer in $E \cong k((t))$ ist. Dann ist der Ringhomomorphismus $\varphi_s \colon \mathcal{O}_\mathcal{E} \to \mathcal{O}_\mathcal{E}$, $\sum_{n\in\mathbb{Z}} a_n t^n \mapsto \sum_{n\in\mathbb{Z}} a_n s^n$, ein Isomorphismus.*

Beweis. Da $s \mod p\mathcal{O}_\mathcal{E}$ ein Uniformisierer in $k((t))$ ist, ist $\bar{s} := s \mod p\mathcal{O}_\mathcal{E} = \sum_{n\geq 1} \alpha_n t^n \in t \cdot k[[t]]$ mit $\alpha_1 \neq 0$. Nach Satz 7.4 ist dann $\varphi_{\bar{s}} = (\varphi_s \mod p\mathcal{O}_\mathcal{E})_{|k[[t]]} \colon k[[t]] \to k[[t]]$ ein Isomorphismus, welcher sich zu einem Körperautomorphismus $\varphi_{\bar{s}} \colon k((t)) \to k((t))$ fortsetzt. Damit erhalten wir das kommutative Diagramm

$$\begin{array}{ccc}
\mathcal{O}_\mathcal{E} & \xrightarrow{\varphi_s} & \mathcal{O}_\mathcal{E} \\
\downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi_2} \\
k((t)) & \xrightarrow{\varphi_{\bar{s}}} & k((t)),
\end{array}$$

wobei π_1 und π_2 jeweils die kanonischen Restklassenabbildungen sind.
Die Injektivität von φ_s sieht man recht leicht, denn für ein $x \in \mathcal{O}_\mathcal{E} \backslash \{0\}$ existiert ein

$n \in \mathbb{N}_0$ und $u \in \mathcal{O}_\mathcal{E}^*$ mit $x = p^n u$. Daraus folgt aber, dass auch $\varphi_s(x) = p^n \varphi_s(u) \neq 0$, da φ_s W-linear und $\varphi_s(u)$ auch wieder eine Einheit in $\mathcal{O}_\mathcal{E}$ ist. Dementsprechend muss $\ker(\varphi_s) = \{0\}$ gelten und somit φ_s injektiv sein.

Für die Surjektivität von φ_s wählen wir uns ein beliebiges $y \in \mathcal{O}_\mathcal{E}$. Wegen der Surjektivität von $\varphi_{\bar{s}}$ und π_1 existiert ein $x_0 \in \mathcal{O}_\mathcal{E}$ mit $\varphi_s(x_0) \mod p = \varphi_{\bar{s}}(x_0 \mod p) = y \mod p$, d.h. $y - \varphi_s(x_0) \in p\mathcal{O}_\mathcal{E}$. Es gibt also ein $y_1 \in \mathcal{O}_\mathcal{E}$ für das $y - \varphi_s(x_0) = py_1$ gilt. Mit der gleichen Begründung wie zuvor gibt es auch für y_1 Elemente $x_1, y_2 \in \mathcal{O}_\mathcal{E}$ mit $y_1 - \varphi_s(x_1) = py_2$. Induktiv erhält man dadurch $x_n, y_n \in \mathcal{O}_\mathcal{E}$, sodass für alle $N \geq 0$

$$y = \sum_{n=0}^{N} p^n \varphi_s(x_n) + p^{N+1} y_{N+1} = \varphi_s\left(\sum_{n=0}^{N} p^n x_n\right) + p^{N+1} y_{N+1}.$$

Da $(p^n x_n)_n$ eine p-adische Nullfolge in $\mathcal{O}_\mathcal{E}$ ist und $\mathcal{O}_\mathcal{E}$ vollständig ist, konvergiert die Reihe $\sum_{n=0}^{\infty} p^n x_n$ p-adisch gegen ein $x \in \mathcal{O}_\mathcal{E}$. In Lemma 7.2 (iii) haben wir gezeigt, dass die schwache Topologie gröber ist als die p-adische Topologie. Daher muss $\sum_{n=0}^{\infty} p^n x_n$ auch bzgl. der schwachen Topologie gegen x konvergieren. Da zudem φ_s bzgl. der schwachen Topologie stetig ist und es sich bei $(p^{N+1} y_{N+1})_{N \geq 0}$ um eine Nullfolge handelt, folgt

$$y = \lim_{N \to \infty} y = \lim_{N \to \infty} \left(\varphi_s\left(\sum_{n=0}^{N} p^n x_n\right) + p^{N+1} y_{N+1}\right) = \varphi_s\left(\lim_{N \to \infty} \sum_{n=0}^{N} p^n x_n\right) + \lim_{N \to \infty} p^{N+1} y_{N+1} = \varphi_s(x).$$

Also ist φ_s auch surjektiv und damit insgesamt ein Isomorphismus. □

Korollar 7.6 (Existenz von Frobenius-Lifts)**.** *Es sei wie gewohnt $F: W \to W$ der Frobenius in W.*

(i) Die Abbildung $\Phi_F: \mathcal{O}_\mathcal{E} \to \mathcal{O}_\mathcal{E}$, $\sum_{n \in \mathbb{Z}} a_n t^n \mapsto \sum_{n \in \mathbb{Z}} F(a_n) t^n$ ist ein stetiger Isomorphismus.

(ii) Die Komposition $\varphi := \varphi_{((1+t)^p - 1)} \circ \Phi_F: \mathcal{O}_\mathcal{E} \to \mathcal{O}_\mathcal{E}$, $\sum_{n \in \mathbb{Z}} a_n t^n \mapsto \sum_{n \in \mathbb{Z}} F(a_n)((1+t)^p - 1)^n$ ist ein stetiger Frobenius-Lift.

(iii) Für ein $s \in \mathcal{O}_\mathcal{E}$, dessen Restklasse $s \mod p\mathcal{O}_\mathcal{E}$ ein Uniformisierer in E ist, wird durch $\varphi_s \circ \Phi_F: \mathcal{O}_\mathcal{E} \to \mathcal{O}_\mathcal{E}$ ein Isomorphismus gegeben.

Beweis. Zu (i): Wegen $\mathrm{char}(k) = p$ ist nach Lemma 5.16 (i) $F(b) = (b_n^p)_{n \geq 0}$ für alle $b = (b_n)_{n \geq 0} \in W$. Da zusätzlich k perfekt ist, also $(x \mapsto x^p): k \to k$ eine Bijektion ist, wird wegen 5.12 (i) durch $F: W \to W$ ein Isomorphismus gegeben. Damit handelt es sich bei Φ_F insbesondere um einen wohldefinierten Ringhomomorphismus, da F selbst ein Ringhomomorphismus ist. Außerdem ist wegen

$$\Phi_F(p^n \mathcal{O}_\mathcal{E} + t^m W[[t]]) = p^n \underbrace{\Phi_F(\mathcal{O}_\mathcal{E})}_{\subset \mathcal{O}_\mathcal{E}} + t^m \underbrace{\Phi_F(W[[t]])}_{\subset W[[t]]} \subset p^n \mathcal{O}_\mathcal{E} + t^m W[[t]],$$

Φ_F stetig bzgl. der schwachen Topologie. Da F ein Isomorphismus ist und jedes Element in $\mathcal{O}_\mathcal{E}$ eindeutig durch seine Koeffizienten bestimmt ist, wird auch durch Φ_F ein Isomorphismus gegeben.

(iii) folgt damit sofort aus (i) und Korollar 7.5. Für (ii) wähle ein Element $\sum_{n\in\mathbb{Z}} a_n t^n \in \mathcal{O}_\mathcal{E}$ und wende φ darauf an. Es gilt dann nämlich

$$\begin{aligned}\varphi\left(\sum_{n\in\mathbb{Z}} a_n t^n\right) &= \sum_{n\in\mathbb{Z}} F(a_n)((1+t)^p - 1)^n \equiv \sum_{n\in\mathbb{Z}} a_n^p (t^n)^p \mod p\mathcal{O}_\mathcal{E} \\ &\equiv \left(\sum_{n\in\mathbb{Z}} a_n t^n\right)^p \mod p\mathcal{O}_\mathcal{E}, \text{ da } \operatorname{char}(k((t))) = p.\end{aligned}$$

Die Stetigkeit von φ folgt dann direkt aus (i) und Lemma 7.3. □

7.2 Derivationen und Differentialformen

Definition 7.7. Sei $S|R$ eine Erweiterung kommutativer Ringe und M ein S-Modul. Wir bezeichnen mit

$$Der_R(S,M) := \{\delta\colon S \to M \mid \delta \text{ ist } R\text{-linear}, \delta(s_1 s_2) = s_1\delta(s_2) + s_2\delta(s_1) \text{ für alle } s_1, s_2 \in S\}$$

die sogenannten *R-Derivationen von S nach M*.

Für den Spezialfall $\mathcal{O}_\mathcal{E}|W$ setzen wir

$$Der_W^{cont.}(\mathcal{O}_\mathcal{E}, \mathcal{O}_\mathcal{E}) := \{\delta \in Der_W(\mathcal{O}_\mathcal{E}, \mathcal{O}_\mathcal{E}) \mid \delta \text{ ist stetig bzgl. der schwachen Topologie}\}.$$

Wie man durch einfaches Nachrechnen sehen kann, wird $Der_R(S,M)$ durch $(\alpha\bullet\delta)(\beta) := \alpha\cdot\delta(\beta)$ zu einem S-Modul. Da $\mathcal{O}_\mathcal{E}$ ein topologischer Ring ist, schränkt sich diese Modulstruktur sogar auf $Der_W^{cont.}(\mathcal{O}_\mathcal{E}, \mathcal{O}_\mathcal{E})$ ein. Wie der nächste Satz zeigen wird, ist $Der_W^{cont.}(\mathcal{O}_\mathcal{E}, \mathcal{O}_\mathcal{E})$ dabei sogar von recht einfacher Form.

Satz 7.8. *Der $\mathcal{O}_\mathcal{E}$-Modul $Der_W^{cont.}(\mathcal{O}_\mathcal{E}, \mathcal{O}_\mathcal{E})$ ist frei vom Rang 1 mit Erzeuger $\delta_t := t\frac{d}{dt}$, wobei $\frac{d}{dt}$ die formelle Ableitung nach t bedeutet.*

Beweis. Zunächst einmal müssen wir zeigen, dass δ_t überhaupt ein Element von $Der_W^{cont.}(\mathcal{O}_\mathcal{E}, \mathcal{O}_\mathcal{E})$ ist. Die W-Linearität folgt dabei sofort aus der W-Linearität von $\frac{d}{dt}$. Wählen wir nun $s_1 := \sum_{n\in\mathbb{Z}} a_n t^n, s_2 := \sum_{n\in\mathbb{Z}} b_n t^n \in \mathcal{O}_\mathcal{E}$, so ist das Produkt der beiden Elemente gegeben durch $s_1 \cdot s_2 = \sum_{l\in\mathbb{Z}} c_l t^l$ mit $c_l = \sum_{n\in\mathbb{Z}} a_n b_{l-n}$. Damit erhalten wir

$$s_1\delta_t(s_2) + s_2\delta_t(s_1) = \sum_{l\in\mathbb{Z}}\Big(\sum_{n\in\mathbb{Z}}(l-n)a_n b_{l-n}\Big)t^l + \sum_{l\in\mathbb{Z}}\Big(\sum_{n\in\mathbb{Z}} n a_n b_{l-n}\Big)t^l = \sum_{l\in\mathbb{Z}} l c_l t^l = \delta_t(s_1\cdot s_2).$$

Des Weiteren sieht man leicht, dass aufgrund der Definition von δ_t schließlich auch $\delta_t(p^n\mathcal{O}_\mathcal{E} + t^m W[[t]]) \subset p^n\mathcal{O}_\mathcal{E} + t^m W[[t]]$ gilt. Damit ist δ_t stetig bzgl. der schwachen Topologie, also ein Element von $Der_W^{cont.}(\mathcal{O}_\mathcal{E}, \mathcal{O}_\mathcal{E})$. Um zu sehen, dass δ_t sogar ein Erzeuger von $Der_W^{cont.}(\mathcal{O}_\mathcal{E}, \mathcal{O}_\mathcal{E})$ ist, untersuchen wir zunächst die Eigenschaften einer stetigen W-Derivation $\delta \in Der_W^{cont.}(\mathcal{O}_\mathcal{E}, \mathcal{O}_\mathcal{E})$.

Behauptung 1: $\delta(t^n) = nt^{n-1}\delta(t)$ für alle $n \in \mathbb{Z}$.
Für $n = 0$ ist die Aussage wegen $\delta(1) = \delta(1 \cdot 1) = 1 \cdot \delta(1) + 1 \cdot \delta(1) = \delta(1) + \delta(1)$ gegeben. Betrachtet man nun ein $n \geq 0$, so folgt die Behauptung induktiv durch

$$\delta(t^{n+1}) = t \cdot \delta(t^n) + t^n \cdot \delta(t) = t \cdot (nt^{n-1}\delta(t)) + t^n\delta(t) = (n+1)t^n\delta(t).$$

Auf der anderen Seite lässt sich durch $0 = \delta(1) = \delta(t^n \cdot t^{-n}) = t^n\delta(t^{-n}) + t^{-n}\delta(t^n)$ die Aussage auch für negative Zahlen zeigen, denn

$$\delta(t^{-n}) = -t^{-n} \cdot t^{-n} nt^{n-1}\delta(t) = -nt^{-n-1}\delta(t) \text{ für } n \geq 0,$$

wodurch die Behauptung gezeigt ist. Aufgrund der Stetigkeit und W-Linearität von δ folgt schließlich

$$\delta\left(\sum_{n\in\mathbb{Z}} a_n t^n\right) = \sum_{n\in\mathbb{Z}} a_n\delta(t^n) = \sum_{n\in\mathbb{Z}} n \cdot a_n t^{n-1}\delta(t) = t^{-1}\delta(t)\delta_t\left(\sum_{n\in\mathbb{Z}} a_n t^n\right).$$

Also ist δ_t ein Erzeuger des $\mathcal{O}_\mathcal{E}$-Moduls $Der_W^{cont.}(\mathcal{O}_\mathcal{E}, \mathcal{O}_\mathcal{E})$. Angenommen es existiert ein $\alpha = \sum_{n\in\mathbb{Z}} a_n t^n \in \mathcal{O}_\mathcal{E}\backslash\{0\}$ mit $\alpha \bullet \delta_t = 0$. Dann müsste aber insbesondere $0 = (\alpha \bullet \delta_t)(t) = \alpha \cdot \delta_t(t) = \alpha \cdot t = \sum_{n\in\mathbb{Z}} a_n t^{n+1}$ gelten, woraus schließlich $a_n = 0$ für alle $n \in \mathbb{Z}$ folgt. Das ist aber offensichtlich ein Widerspruch zu $\alpha \neq 0$.
Also ist $\delta_t = t \cdot \frac{d}{dt}$ eine $\mathcal{O}_\mathcal{E}$-Basis von $Der_W^{cont.}(\mathcal{O}_\mathcal{E}, \mathcal{O}_\mathcal{E})$. □

Definition 7.9. Wir bezeichnen mit $\Omega_{\mathcal{O}_\mathcal{E}|W} := \mathcal{O}_\mathcal{E} \cdot dt$ den freien $\mathcal{O}_\mathcal{E}$-Modul vom Rang 1 mit Basiselement dt, die sogenannten Differentialformen von $\mathcal{O}_\mathcal{E}$ über W.

Bemerkung 7.10. Für die Differentialformen von $\mathcal{O}_\mathcal{E}$ über W sieht man leicht, dass die folgenden Anmerkungen gelten.

1. Die Abbildung $Der_W^{cont.}(\mathcal{O}_\mathcal{E}, \mathcal{O}_\mathcal{E}) \xrightarrow{\sim} Hom_{\mathcal{O}_\mathcal{E}}(\Omega_{\mathcal{O}_\mathcal{E}|W}, \mathcal{O}_\mathcal{E})$, $\delta \mapsto (f \cdot dt \mapsto f \cdot \delta(t))$ ist $\mathcal{O}_\mathcal{E}$-linear.

2. Die Abbildung $d\colon \mathcal{O}_\mathcal{E} \to \Omega_{\mathcal{O}_\mathcal{E}|W}$, $f \mapsto df := \frac{df}{dt} \cdot dt$ ist W-linear.

3. Da $t \in \mathcal{O}_\mathcal{E}$ eine Einheit ist, bildet auch $d_{log}t := t^{-1} \cdot dt \in \Omega_{\mathcal{O}_\mathcal{E}|W}$ eine Basis des $\mathcal{O}_\mathcal{E}$-Moduls $\Omega_{\mathcal{O}_\mathcal{E}|W}$.

4. Für ein $s \in \mathcal{O}_\mathcal{E}$ mit $s \equiv t \mod p\mathcal{O}_\mathcal{E}$ ist auch $d_{log}s := s^{-1} \cdot ds \in \Omega_{\mathcal{O}_\mathcal{E}|W}$ eine $\mathcal{O}_\mathcal{E}$-Basis von $\Omega_{\mathcal{O}_\mathcal{E}|W}$.

Zum letzten Punkt sei noch angemerkt, dass für ein $s \in \mathcal{O}_\mathcal{E}$ von der Form $s = t + pr$ mit $r \in \mathcal{O}_\mathcal{E}$ die formelle Ableitung $\frac{ds}{dt} = 1 + p\frac{dr}{dt}$ eine Einheit in $\mathcal{O}_\mathcal{E}$ ist. Daher ist auch $s^{-1} \cdot \frac{ds}{dt}$ eine Einheit in $\mathcal{O}_\mathcal{E}$ und somit $d_{log}s = s^{-1} \cdot \frac{ds}{dt} \cdot dt$ eine $\mathcal{O}_\mathcal{E}$-Basis von $\Omega_{\mathcal{O}_\mathcal{E}|W}$.

Die zuvor angegebene Definition der Differentialformen von $\mathcal{O}_\mathcal{E}$ über W lässt sich auch auf die Quotientenkörper $K := Quot(W) = W[\frac{1}{p}]$ und $\mathcal{E} := Quot(\mathcal{O}_\mathcal{E}) = \mathcal{O}_\mathcal{E}[\frac{1}{p}]$ fortsetzen.

Definition 7.11. Analog zur Definition zuvor bezeichnen wir mit $\Omega_{\mathcal{E}|K} := \mathcal{E} \cdot dt = \mathcal{E} \cdot d_{log}t$ die sogenannten Differentialformen von $\mathcal{E}$ über K.

Wir wollen nun den Quotientenkörper $\mathcal{E}$ von $\mathcal{O}_\mathcal{E}$ etwas genauer untersuchen und hoffen, diesen in einer ähnlich expliziten Form wie $\mathcal{O}_\mathcal{E}$ angeben zu können. Zunächst wählen wir dafür ein $f \in \mathcal{E}$. Da $\mathcal{E} = \mathcal{O}_\mathcal{E}[\frac{1}{p}]$, existieren $g = \sum_{n\in\mathbb{Z}} a_n t^n \in \mathcal{O}_\mathcal{E}$ und $m \geq 0$ mit

$$f = gp^{-m} = \sum_{n\in\mathbb{Z}} \underbrace{(a_n p^{-m})}_{=:c_n \in W[\frac{1}{p}]=K} t^n = \sum_{n\in\mathbb{Z}} c_n t^n.$$

Für die Koeffizienten c_n gilt dann

$$v_p(c_n) = v_p(a_n p^{-m}) = v_p(a_n) - m.$$

Da aber $\lim_{n\to-\infty} a_n = 0$, muss schließlich auch $\lim_{n\to-\infty} c_n = 0$ gelten. Außerdem gilt wegen $v_p(a_n) \geq 0$ und der obigen Abschätzung $v_p(c_n) \geq -m$ für alle $n \in \mathbb{Z}$. Also muss auch $\inf_{n\in\mathbb{Z}}\{v_p(c_n)\} \geq -m > -\infty$ und damit

$$\mathcal{E} \subset \left\{ \sum_{n\in\mathbb{Z}} c_n t^n \mid c_n \in K, \lim_{n\to-\infty} c_n = 0, \inf_{n\in\mathbb{Z}}\{v_p(c_n)\} > -\infty \right\}.$$

gelten. Auf der anderen Seite können wir sogar Gleichheit der beiden Mengen zeigen, denn für ein Element $\sum_{n\in\mathbb{Z}} c_n t^n$ aus der rechten Menge ist

$$p^{-r} \sum_{n\in\mathbb{Z}} c_n t^n = \sum_{n\in\mathbb{Z}} \underbrace{p^{-r}c_n}_{\in W} t^n \in \mathcal{O}_\mathcal{E} \text{ und } \lim_{n\to-\infty} p^{-r}c_n = 0,$$

wobei $r := \inf_{n\in\mathbb{Z}}\{v_p(c_n)\}$. Also ist $\sum_{n\in\mathbb{Z}} c_n t^n$ ein Element von $p^r\mathcal{O}_\mathcal{E} \subset \mathcal{O}_\mathcal{E}[\frac{1}{p}] = \mathcal{E}$, womit die Gleichheit der beiden Mengen gezeigt ist. Mit dieser Darstellung der Elemente von $\mathcal{E}$ können wir die Abbildung $d\colon \mathcal{O}_\mathcal{E} \to \Omega_{\mathcal{O}_\mathcal{E}|W}$ fortsetzen zu $d\colon \mathcal{E} \to \Omega_{\mathcal{E}|K}$, $f \mapsto df = \frac{df}{dt} \cdot dt$.

Im nächsten Schritt möchten wir gerne über die schwache Topologie auf $\mathcal{O}_\mathcal{E}$ die schwache Topologie auf $\mathcal{E}$ definieren. Dazu wählen wir uns zunächst ein beliebiges

$n \in \mathbb{N}$ und definieren die schwache Topologie auf $p^{-n}\mathcal{O}_\mathcal{E}$ wie folgt:

$$\begin{aligned} U \subset p^{-n}\mathcal{O}_\mathcal{E} \text{ offen } &\Leftrightarrow p^n U \subset \mathcal{O}_\mathcal{E} \text{ offen} \\ &\Leftrightarrow \forall x \in p^n U\ \exists N, M \geq 0 :\ x + p^N \mathcal{O}_\mathcal{E} + t^M W[[t]] \subset p^n U \\ &\Leftrightarrow \forall x \in U\ \exists N, M \geq 0 :\ x + p^{-n}(p^N \mathcal{O}_\mathcal{E} + t^M W[[t]]) \subset U. \end{aligned}$$

Ähnlich wie auf $\mathcal{O}_\mathcal{E}$ bilden die Mengen $(U_{NM}^{(n)} := p^{-n}(p^N\mathcal{O}_\mathcal{E} + t^M W[[t]]))_{N,M\in\mathbb{N}_0}$ eine offene Umgebungsbasis der 0 in $p^{-n}\mathcal{O}_\mathcal{E}$. Mit dieser Definition der schwachen Topologie auf $p^{-n}\mathcal{O}_\mathcal{E}$ ist $(x \mapsto p^{-n}x)\colon \mathcal{O}_\mathcal{E} \to p^{-n}\mathcal{O}_\mathcal{E}$ ein Homöomorphismus.

Die schwache Topologie auf $\mathcal{E}$ definieren wir schließlich durch

$$\begin{aligned} &U \subset \mathcal{E} = \bigcup_{n\geq 0} p^{-n}\mathcal{O}_\mathcal{E} \text{ ist offen} \\ &\Leftrightarrow \forall n \geq 0 :\ U \cap p^{-n}\mathcal{O}_\mathcal{E} \subset p^{-n}\mathcal{O}_\mathcal{E} \text{ ist offen} \\ &\Leftrightarrow \forall n \geq 0\ \forall x \in U \cap p^{-n}\mathcal{O}_\mathcal{E}\ \exists N, M \geq 0 :\ x + p^{-n}(p^N\mathcal{O}_\mathcal{E} + t^M W[[t]]) \subset U \cap p^{-n}\mathcal{O}_\mathcal{E} \\ &\Leftrightarrow \forall n \geq 0\ \forall x \in U\ \exists N, M \geq 0 :\ x + p^{-n}(p^N\mathcal{O}_\mathcal{E} + t^M W[[t]]) \subset U, \end{aligned}$$

wobei wir auf die letzte Äquivalenz noch etwas genauer eingehen sollten. Die Rückrichtung ist dabei leicht zu sehen, indem man einfach mit $p^{-n}\mathcal{O}_\mathcal{E}$ schneidet. Für die Hinrichtung sei $x \in U$ und $n \geq 0$. Für den Fall $x \in p^{-n}\mathcal{O}_\mathcal{E}$ ist nichts zu zeigen und wir können ohne Einschränkung $x \notin p^{-n}\mathcal{O}_\mathcal{E}$ bzw. $v_p(x) < -n$ annehmen. Allerdings existieren wegen $x \in U \cap p^{v_p(x)}\mathcal{O}_\mathcal{E}$ natürliche Zahlen $N, M \geq 0$ mit

$$x + p^{-n}(p^N\mathcal{O}_\mathcal{E} + t^M W[[t]]) \subset x + p^{v_p(x)}(p^N\mathcal{O}_\mathcal{E} + t^M W[[t]]) \subset U \cap p^{v_p(x)}\mathcal{O}_\mathcal{E} \subset U,$$

womit die Hinrichtung gezeigt wäre. Die Mengen $(U_{NM}^{(n)} := p^{-n}(p^N\mathcal{O}_\mathcal{E} + t^M W[[t]]))_{n,N,M\in\mathbb{N}_0}$ bilden damit eine offene Umgebungsbasis der 0 in $\mathcal{E}$ bzgl. der schwachen Topologie. Führen wir auf analoge Weise die p-adische Topologie aus W fort zu einer Topologie auf K, so ist eine Menge $U \subset K$ genau dann offen, wenn für jedes $x \in U$ ein $m \geq 0$ mit $x + p^m W \subset U$ existiert, was genau die Bewertungstopologie auf K ergibt.

7.3 Die Residuenabbildung

Im Folgenden sei durch $s \in \mathcal{O}_\mathcal{E}$ stets ein Element mit $s \equiv t \mod p\mathcal{O}_\mathcal{E}$ gegeben. Wie wir in Korollar 7.5 gesehen haben, ist dann $\varphi_s\colon \mathcal{O}_\mathcal{E} \to \mathcal{O}_\mathcal{E}$ ein Isomorphismus, welcher sich zu einem Körperautomorphismus $\varphi_s\colon \mathcal{E} \to \mathcal{E}$ fortsetzt. Dieser Körperautomorphismus ist sogar stetig bzgl. der schwachen Topologie auf $\mathcal{E}$. Ist nämlich $U \subset \mathcal{E}$ offen und $n \geq 0$ eine beliebige natürliche Zahl, so ist $p^n U \cap \mathcal{O}_\mathcal{E} \subset \mathcal{O}_\mathcal{E}$ offen. Da $\varphi_{s|_{\mathcal{O}_\mathcal{E}}}$ ein stetiger Ringautomorphismus ist, ist auch

$$p^n\varphi_s^{-1}(U) \cap \mathcal{O}_\mathcal{E} = \varphi_s^{-1}(p^n U \cap \mathcal{O}_\mathcal{E}) = \varphi_{s|_{\mathcal{O}_\mathcal{E}}}^{-1}(p^n U \cap \mathcal{O}_\mathcal{E}) \subset \mathcal{O}_\mathcal{E} \text{ offen.}$$

Nach Definition der schwachen Topologie auf $\mathcal{E}$ und der beliebigen Wahl von $n \geq 0$ folgt schließlich die Stetigkeit von $\varphi_s: \mathcal{E} \to \mathcal{E}$.

Definition 7.12. Für ein $w = (\sum_{n\in\mathbb{Z}} a_n t^n) \cdot d_{log}t \in \Omega_{\mathcal{E}|K}$ setzen wir $res_t(w) := a_0 \in K$.

Durch diese Definition erhalten wir ein K-lineare Abbildung $res_t: \Omega_{\mathcal{E}|K} \to K$ mit $res_t(\Omega_{\mathcal{O}_\mathcal{E}|W}) \subset W$. Definiert man auf $\Omega_{\mathcal{E}|K}$ die schwache Topologie durch $\mathcal{E} \cong \Omega_{\mathcal{E}|K}$, $f \mapsto f \cdot dt$, so handelt es sich bei res_t sogar um eine stetige Abbildung. Um dies zu zeigen wählen wir eine offene Menge $U \subset K$ und ein $x \cdot dt = (\sum_{k\in\mathbb{Z}} a_k t^k) \cdot dt \in res_t^{-1}(U)$. Es existiert also ein $m \geq 0$ mit $a_{-1} + p^m W = res_t(x \cdot dt) + p^m W \subset U$. Sei nun $n \geq 0$ eine beliebige natürliche Zahl und setze $N := m + n$ und $M := 1$. Dann gilt aufgrund der K-Linearität von res_t:

$$\begin{aligned} res_t((x + U_{NM}^{(n)}) \cdot dt) &= \underbrace{res_t(x \cdot dt)}_{=a_{-1}} + p^{N-n} \underbrace{res_t(\mathcal{O}_\mathcal{E} \cdot dt)}_{=W} + p^{-n} \underbrace{res_t(t^M W[[t]] \cdot dt)}_{=0} \\ &= a_{-1} + p^m W \subset U. \end{aligned}$$

Also ist $res_t^{-1}(U)$ offen in $\Omega_{\mathcal{E}|K}$ und damit $res_t: \Omega_{\mathcal{E}|K} \to K$ stetig.

Satz 7.13. *Wie gewohnt sei $s \in \mathcal{O}_\mathcal{E}$ mit $s \equiv t \mod p\mathcal{O}_\mathcal{E}$ und schreibe $w = (\sum_{n\in\mathbb{Z}} a_n t^n) \cdot d_{log}t \in \Omega_{\mathcal{E}|K}$ bzw. $w = (\sum_{n\in\mathbb{Z}} b_n s^n) \cdot d_{log}s \in \Omega_{\mathcal{E}|K}$ bezüglich der Basen $d_{log}t$ bzw. $d_{log}s$. Dann ist $res_t(w) = a_0 = b_0 =: res_s(w)$.*

Beweis. Wir setzen $f(t) := \sum_{n\in\mathbb{Z}\setminus\{-1\}} b_{n+1} t^n \in \mathcal{E}$ und schreiben

$$w = \left(\sum_{n\in\mathbb{Z}} b_n s^n\right) \cdot d_{log}s = b_0 \cdot d_{log}s + \left(\sum_{n\in\mathbb{Z}\setminus\{0\}} b_n s^n\right) s^{-1} \cdot ds = b_0 \cdot d_{log}s + f(s) \cdot ds.$$

Des Weiteren setzen wir $F_m(t) := \sum_{\substack{|n|\leq m \\ n\neq -1}} b_{n+1} t^n \in \mathcal{E}$ für $m \in \mathbb{N}$.

Behauptung: $\lim_{m\to\infty} F_m(t) = f(t)$ in $\mathcal{E}$ bzgl. der schwachen Topologie.
Sei dafür $U \subset$ eine offene Umgebung von 0 und setze

$$k := \max\{0, -v_p(f)\} = \max\{0, -\min\{v_p(b_{n+1}) \mid n \in \mathbb{Z}\setminus\{-1\}\}\} \in \mathbb{N}_0,$$

was wohldefiniert ist, da $f \in \mathcal{E}$ und damit die p-adische Bewertung der Koeffizienten nach unten beschränkt ist. Damit existieren $N, M \in \mathbb{N}$ mit $p^{-k}(p^N\mathcal{O}_\mathcal{E} + t^M W[[t]]) \subset U$. Des Weiteren existiert für $f \in \mathcal{E}$ ein $m_1 \in \mathbb{Z}$, sodass $b_{n+1} \in p^{N-k}\mathcal{O}_\mathcal{E}$ für alle $n < m_1$. Dann gilt schließlich für alle $m \geq \max\{|m_1|, M\}$:

$$f - F_m = \sum_{\substack{|n|>m \\ n\neq -1}} b_{n+1} t^n = \underbrace{\sum_{n<-m} b_{n+1} t^n}_{\in p^{N-k}\mathcal{O}_\mathcal{E}} + \underbrace{\sum_{n>m} b_{n+1} t^n}_{\in t^M p^{-k} W[[t]]},$$

nach Wahl von k und m. Also ist $f - F_m \in U_{NM}^{(k)} \subset U$ und damit gilt $\lim_{m\to\infty} F_m(t) = f(t)$ in $\mathcal{E}$. Da $\varphi_s\colon \mathcal{E} \to \mathcal{E}$ stetig ist , erhalten wir sogar

$$\lim_{m\to\infty} F_m(s) = \lim_{m\to\infty} \varphi_s(F_m(t)) = \varphi_s(\lim_{m\to\infty} F_m(t)) = \varphi_s(f(t)) = f(s).$$

Aus der Bemerkung zu Beginn dieses Abschnitts wissen wir, dass es sich bei φ_s um einen Körperautomorphismus handelt. Somit existiert für jedes $g = g(t) \in \mathcal{E}$ ein $h(t) \in \mathcal{E}$ mit $g(t) = h(s(t))$. Schreiben wir $s(t) := \sum_{n\in\mathbb{Z}} d_n t^n$ und $h(t) := \sum_{n\in\mathbb{Z}} c_n t^n$, so gilt

$$\begin{aligned}
dg &= \frac{dg}{dt}\cdot dt = \frac{d}{dt}(h(s(t)))\cdot dt = \left(\frac{d}{dt}\sum_{n\in\mathbb{Z}} c_n\left(\sum_{k\in\mathbb{Z}} d_k t^k\right)^n\right)\cdot dt \\
&= \left(\sum_{n\in\mathbb{Z}} c_n \frac{d}{dt}\left(\sum_{k\in\mathbb{Z}} d_k t^k\right)^n\right)\cdot dt \\
&= \left(\sum_{n\in\mathbb{Z}} c_n n \underbrace{\left(\sum_{k\in\mathbb{Z}} d_k t^k\right)}_{=s(t)}{}^{n-1} \underbrace{\left(\sum_{k\in\mathbb{Z}} d_k k t^{k-1}\right)}_{=\frac{d}{dt}s(t)}\right)\cdot dt \\
&= \underbrace{\left(\sum_{n\in\mathbb{Z}} c_n n s^{n-1}\right)}_{=\frac{d}{ds}h(s)} \cdot \underbrace{\frac{ds}{dt}\cdot dt}_{=ds} \\
&= \frac{dh}{ds}\cdot ds.
\end{aligned}$$

Daher ist sowohl $res_s(dg) = 0$, als auch $res_t(\frac{dh}{ds}\cdot ds) = 0$.

setzen wir $G_m := \sum_{\substack{|n|<m \\ n\neq -1}} \frac{b_{n+1}}{n+1} s^{n+1} \in \mathcal{E}$ für $m \geq 0$, so erhält man $\frac{dG_m}{ds}\cdot ds = (\sum_{\substack{|n|<m \\ n\neq -1}} b_{n+1}s^n)\cdot ds = F_m(s)\cdot ds$. Wie wir gerade herausgefunden haben ist dann $res_t(F_m(s)\cdot ds) = res_t(\frac{dG_m}{ds}\cdot ds) = 0$ für alle $m \geq 0$. Aufgrund der Stetigkeit von res_t ergibt sich damit

$$res_t(f(s)\cdot ds) = \lim_{m\to\infty} res_t(F_m(s)\cdot ds) = 0.$$

Des Weiteren erhalten wir durch die K-Linearität von res_t auch

$$res_t(w) = res_t(b_0\cdot d_{log}s) + res_t(f(s)\cdot ds) = b_0 res_t(d_{log}s).$$

Also bleibt nur noch zu zeigen, dass $res_t(d_{log}s) = 1$ gilt.

Sei wie gewohnt $r \in \mathcal{O}_\mathcal{E}$ mit $s = (1+pr)t$. Dann lässt sich $d_{log}s$ schreiben als

$$\begin{aligned} d_{log}s = s^{-1} \cdot ds &= t^{-1}(1+pr)^{-1}\frac{ds}{dt} \cdot dt \\ &= (1+pr)^{-1}((1+pr) + t\frac{d}{dt}(1+pr))t^{-1} \cdot dt \\ &= d_{log}t + ((1+pr)^{-1}p\frac{d}{dt}r) \cdot dt. \end{aligned}$$

Wir setzen $G := \sum_{i=0}^{\infty} \frac{1}{i+1}(-p)^i r^{i+1} \in \mathcal{O}_\mathcal{E}$. Zunächst einmal muss man sich dabei klar machen, dass G tatsächlich ein Element von $\mathcal{O}_\mathcal{E}$ ist. Für $i+1 \in \mathbb{N}$ schreiben wir $i+1 = p^{n_{i+1}}u_{i+1}$ mit $n_{i+1} \geq 0, u_{i+1} \geq 1$ und p teilt nicht u_{i+1}. Dann gilt $i+1 \geq p^{n_{i+1}}$ und wegen der Monotonie des Logarithmus $\log_p$ zur Basis p schließlich auch $\log_p(i+1) \geq n_{i+1}$. Aufgrund von $\lim_{i\to\infty} \frac{p^i}{i+1} = \infty$ und $\lim_{x\to\infty} \log_p(x) = \infty$ ist damit auch $\lim_{i\to\infty} \log_p(\frac{p^i}{i+1}) = \infty$. Da u_{i+1} nicht durch p teilbar ist, muss $u_{i+1} = u_{i+1} \cdot 1_W$ eine Einheit in W sein. Wegen der Ungleichung $i+1 \leq p^i$ ist insbesondere $n_{i+1} \leq i$. Wegen $r \in \mathcal{O}$ muss damit auch

$$\frac{1}{i+1}(-p)^i r^{i+1} = u_{i+1}^{-1}(-1)^i p^{i-n_{i+1}} r^{i+1}$$

in $\mathcal{O}_\mathcal{E}$ liegen. Des Weiteren muss es sich wegen

$$\begin{aligned} v_p\left(\frac{1}{i+1}(-p)^i r^{i+1}\right) &= i - v_p(i+1) + (i+1)v_p(r) \geq i - v_p(i+1) = i - n_{i+1} \\ &\geq i - \log_p(i+1) = \log_p\left(\frac{p^i}{i+1}\right) \end{aligned}$$

bei $(\frac{1}{i+1}(-p)^i r^{i+1})_{i\geq 0}$ um eine p-adische Nullfolge handeln, d.h. die Reihe $\sum_{i=0}^{\infty} \frac{1}{i+1}(-p)^i r^{i+1}$ konvergiert p-adisch in $\mathcal{O}_\mathcal{E}$. Da die schwache Topologie auf $\mathcal{O}_\mathcal{E}$ gröber ist als die p-adische Topologie, konvergiert die Reihe auch bzgl. der schwachen Topologie. Für G gilt dann:

$$dG = \frac{dG}{dt} \cdot dt = \left(\sum_{i=0}^{\infty}(-p)^i r^i \frac{d}{dt}r\right) \cdot dt = \underbrace{\left(\sum_{i=0}^{\infty}(-pr)^i\right)}_{=(1+pr)^{-1}} \frac{d}{dt}r \cdot dt = (1+pr)^{-1}\frac{d}{dt}r \cdot dt.$$

Aufgrund der K-Linearität von res_t erhalten wir schließlich

$$res_t(d_{log}s) = res_t(d_{log}t) + p \cdot res_t((1+pr)^{-1}\frac{d}{dt}rdt) = 1 + p \cdot res_t(dG) = 1,$$

womit die Behauptung gezeigt wäre. □

Korollar 7.14. *$res := res_\mathcal{E} := res_t : \Omega_{\mathcal{E}|K} \to K$ hängt nur von der Restklasse $t \mod p\mathcal{O}_\mathcal{E}$ ab.*

Beweis. Die Aussage folgt sofort aus dem vorherigen Satz 7.13. □

7.4 Der Coleman-Isomorphismus

Sei wie in Lemma 7.6 (ii) $\varphi: \mathcal{O}_\mathcal{E} \to \mathcal{O}_\mathcal{E}$ ein Frobenius-Lift mit $\varphi(t) = (1+t)^p - 1$. Wir fixieren eine beliebige Nullstelle t' von $\varphi(X) - t = (1+X)^p - 1 - t$ in $\mathcal{E}^{sep}$ und setzen $\mathcal{E}' := \mathcal{E}[t']$.

Lemma 7.15. *Die endliche Körpererweiterung $\mathcal{E}'|\mathcal{E}$ hat die folgenden Eigenschaften:*

(i) *$\mathcal{E}'$ ist vollständig diskret bewertet;*

(ii) *$\varphi(X) - t = (1+X)^p - 1 - t$ ist irreduzibel über $\mathcal{E}$;*

(iii) *$\mathcal{O}_{\mathcal{E}'} = \mathcal{O}_\mathcal{E}[t']$;*

(iv) *$e(\mathcal{E}'|\mathcal{E}) = 1$, d.h. $p\mathcal{O}_{\mathcal{E}'}$ ist das maximale Ideal von $\mathcal{O}_{\mathcal{E}'}$;*

(v) *Bezeichnen wir mit E' den Restklassenkörper von $\mathcal{E}'$, so ist die Körpererweiterung $E'|E$ rein inseparabel, d.h. für jedes $x \in EE'$ ist das charakteristische Polynom in einem algebraischen Abschluss gleich $\chi_x(T) = (T-x)^p = T^p - x^p$.*

Insbesondere ist $\mathcal{E}'|\mathcal{E}$ wegen (v) nicht unverzweigt.

Beweis. (i) folgt hierbei sofort aus Satz 1.24. Für (ii) nehmen wir an, dass $\varphi(X) - t = g \cdot h$ in $\mathcal{O}_\mathcal{E}[X]$ zerfällt, wobei $g, h \in \mathcal{O}_\mathcal{E}[X]$ nach dem Gauß-Lemma normiert sind. Insbesondere zerfällt damit auch $X^p - t = \varphi(X) - t \mod p = \bar{g} \cdot \bar{h}$ mit $\bar{g} = g \mod p, \bar{h} = h \mod p \in \mathcal{O}_\mathcal{E}/p\mathcal{O}_\mathcal{E}[X] = E[X] \cong k((t))[X]$. Da aber $X^p - t \in k[[t]][X]$ ein Eisensteinpolynom bzgl. des Primelements t ist, muss $X^p - t = \bar{g}\bar{h}$ irreduzibel über $k((t))$ sein und damit bereits $0 = \deg(\bar{g}) = \deg(g)$ oder $0 = \deg(\bar{h}) = \deg(h)$ gelten. Schließlich ist dann auch $\varphi(X) - t$ irreduzibel über $\mathcal{E}$.

Für einen Uniformisierer $\pi' \in \mathcal{O}_{\mathcal{E}'}$ setzen wir $t_p := t' \mod \pi'\mathcal{O}_{\mathcal{E}'}$, was eine Nullstelle des irreduziblen Polynoms $X^p - t \in E[X]$ ist. Wegen der Irreduzibilität von $\varphi(X) - t$ über $\mathcal{E}$ erhält man dann

$$p = [E[t_p] : E] \leq [E' : E] \leq [\mathcal{E}' : \mathcal{E}] = p.$$

Also gilt sogar Gleichheit und damit wegen Lemma 1.26 (i) $e(\mathcal{E}'|\mathcal{E}) = 1$, d.h. p ist ein Uniformisierer von $\mathcal{O}_{\mathcal{E}'}$. Des Weiteren folgt aus Lemma 1.26 (iii) und $E' = E[t_p] = E[t' \mod p\mathcal{O}_{\mathcal{E}'}]$ auch $\mathcal{O}_{\mathcal{E}'} = \mathcal{O}_\mathcal{E}[t']$, womit (iii) und (iv) gezeigt sind.

Für (v) sei $x \in E' = E[t_p]$ und $m_x(T) \in E[T]$ das Minimalpolynom von x über E. Liegt x bereits in E, so ist $m_x(T) = T - x$ und damit $\chi_x = (T-x)^p$. Daher bleibt nur noch der Fall $x \notin E$ zu zeigen. Wie wir zuvor bereits gesehen haben, ist $[E' : E] = p$ und daher muss auch $\deg(m_x) = p$ gelten, also das Minimalpolynom bereits mit dem charakteristischen Polynom übereinstimmen. Außerdem existieren wegen $E' = E[t_p]$

eindeutig bestimmte $a_0, \dots, a_{p-1} \in E$ mit $x = \sum_{i=0}^{p-1} a_i t_p^i$. Da t_p eine Nullstelle von $X^p - t$ und $\mathrm{char}(E') = p$ ist, liegt $x^p = \sum_{i=0}^{p-1} a_i^p t^i$ bereits in E. Aus Gradgründen ist das Minimalpolynom von x daher gegeben durch $m_x(T) = T^p - x^p = (T-x)^p$ in $E'[T]$. □

Wir behalten weiterhin die Bezeichnung $t_p := t' \bmod p\mathcal{O}_{\mathcal{E}'}$ bei und haben $E' := E[t_p] \cong k((t_p))$. Aus dem Beweis des vorherigen Lemmas wissen wir bereits, dass $\mathcal{O}_{\mathcal{E}'}$ ein vollständiger diskreter Bewertungsring mit Uniformisierer p ist. Also handelt es sich bei $\mathcal{O}_{\mathcal{E}'}$ um einen p-Cohen-Ring für E'. Aufgrund der Eindeutigkeit von p-Cohen-Ringen nach Satz 5.3 und wegen Lemma 5.2 ist

$$\mathcal{O}_{\mathcal{E}'} = \left\{ \sum_{n\in\mathbb{Z}} a_n t'^n \mid a_n \in W, \lim_{n\to-\infty} v(a_n) = \infty \right\}.$$

Die vorherigen Resultate für $\mathcal{O}_{\mathcal{E}}$ gelten also auch völlig analog für den Ring $\mathcal{O}_{\mathcal{E}'}$ und dementsprechend gilt

$$\mathcal{E}' = \left\{ \sum_{n\in\mathbb{Z}} c_n t'^n \mid c_n \in K, \lim_{n\to-\infty} c_n = 0, \inf_{n\in\mathbb{Z}}\{v(c_n)\} > -\infty \right\}$$

und wir haben durch Lemma 7.6 auch einen Frobenius-Lift

$$\varphi = \varphi_{((1+t')^p-1)} \circ \Phi_F \colon \mathcal{O}_{\mathcal{E}'} \to \mathcal{O}_{\mathcal{E}'}, \sum_{n\in\mathbb{Z}} a_n t'^n \mapsto \sum_{n\in\mathbb{Z}} F(a_n)((1+t')^p - 1)^n = \sum_{n\in\mathbb{Z}} F(a_n) t^n.$$

Außerdem gilt $\varphi(t) = \varphi((1+t')^p - 1) = (1+\varphi(t'))^p - 1 = (1+t)^p - 1$, d.h. φ schränkt sich auf $\mathcal{O}_{\mathcal{E}} \subset \mathcal{O}_{\mathcal{E}'}$ zu unserem ursprünglichen Frobenius-Lift ein. Man beachte zudem, dass $\varphi(\mathcal{O}_{\mathcal{E}'}) \subset \mathcal{O}_{\mathcal{E}}$ und die Einschränkung $\varphi \colon \mathcal{O}_{\mathcal{E}'} \to \mathcal{O}_{\mathcal{E}}$ sogar ein Isomorphismus ist. Dies sieht man recht leicht, da nach Lemma 7.6 Φ_F ein Isomorphismus ist und aufgrund der Definitionen von $\mathcal{O}_{\mathcal{E}'}$ und $\mathcal{O}_{\mathcal{E}}$ auch

$$\varphi_{((1+t')^p-1)} \colon \mathcal{O}_{\mathcal{E}'} \to \mathcal{O}_{\mathcal{E}}, \sum_{n\in\mathbb{Z}} a_n t'^n \mapsto \sum_{n\in\mathbb{Z}} a_n((1+t')^p - 1)^n = \sum_{n\in\mathbb{Z}} a_n t^n,$$

offensichtlich bijektiv ist. Daher setzt sich $\varphi \colon \mathcal{O}_{\mathcal{E}'} \to \mathcal{O}_{\mathcal{E}}$ zu einem Körperautomorphismus $\varphi \colon \mathcal{E}' \xrightarrow{\sim} \mathcal{E}$ fort.

Definition 7.16. Wir bezeichnen mit $N_{\mathcal{E}'|\mathcal{E}} \colon \mathcal{E}' \to \mathcal{E}$ die Körpernorm und mit $Tr_{\mathcal{E}'|\mathcal{E}} \colon \mathcal{E}' \to \mathcal{E}$ die Spur der endlichen Körpererweiterung $\mathcal{E}'|\mathcal{E}$. Da $\varphi \colon \mathcal{E}' \to \mathcal{E}$ ein Isomorphismus ist, haben wir die wohldefinierten Abbildungen

$$N_\varphi \colon \mathcal{E} \to \mathcal{E}, x \mapsto N_{\mathcal{E}'|\mathcal{E}}(\varphi^{-1}(x)) \quad \text{und} \quad Tr_\varphi \colon \mathcal{E} \to \mathcal{E}, x \mapsto Tr_{\mathcal{E}'|\mathcal{E}}(\varphi^{-1}(x)).$$

Satz 7.17. *Die Reduktionsabbildung $\mathcal{O}_{\mathcal{E}}^* \to (\mathcal{O}_{\mathcal{E}}/p\mathcal{O}_{\mathcal{E}})^* = E^*$ schränkt sich zu einem Gruppenisomorphismus $(\mathcal{O}_{\mathcal{E}}^*)^{N_\varphi} \xrightarrow{\sim} E^*$ ein, wobei $(\mathcal{O}_{\mathcal{E}}^*)^{N_\varphi} = \{x \in \mathcal{O}_{\mathcal{E}}^* \mid N_\varphi(x) = x\}$.*

Beweis. Wir zeigen zunächst die Isomorphie $\mathcal{O}_\mathcal{E}^*/(1+p\mathcal{O}_\mathcal{E}) \cong E^*$ und betrachten dafür die kanonische Abbildung $\eta: \mathcal{O}_\mathcal{E}^* \hookrightarrow \mathcal{O}_\mathcal{E} \to (\mathcal{O}_\mathcal{E}/p\mathcal{O}_\mathcal{E}) = E$. Wegen $\mathcal{O}_\mathcal{E}^* = \mathcal{O}_\mathcal{E} \backslash p\mathcal{O}_\mathcal{E}$ ist die Einschränkung $\eta: \mathcal{O}_\mathcal{E}^* \to E^*$ ein wohldefinierter, surjektiver Gruppenhomomorphismus mit $\ker(\eta) = 1 + p\mathcal{O}_\mathcal{E}$. Also ist $E^* \cong \mathcal{O}_\mathcal{E}^*/\ker(\eta) = \mathcal{O}_\mathcal{E}^*/(1+p\mathcal{O}_\mathcal{E})$ und wir erhalten die exakte Sequenz

$$0 \longrightarrow 1 + p\mathcal{O}_\mathcal{E} \longrightarrow \mathcal{O}_\mathcal{E}^* \longrightarrow E^* \longrightarrow 0.$$

Behauptung 1: $N_\varphi(1+p\mathcal{O}_\mathcal{E}) \subset 1 + p\mathcal{O}_\mathcal{E}$.
Sei dafür $x = 1 + px' \in 1 + p\mathcal{O}_\mathcal{E}$, $y' := \varphi^{-1}(x')$ und $y := \varphi^{-1}(x) = 1 + py' \in 1 + p\mathcal{O}_{\mathcal{E}'}$. Nach Lemma 7.15 ist $\{y_1 := 1, y_2 := t', \dots, y_p := t'^{p-1}\}$ sowohl eine $\mathcal{O}_\mathcal{E}$-Basis von $\mathcal{O}_{\mathcal{E}'}$, als auch eine $\mathcal{E}$-Basis von $\mathcal{E}'$. Daher existieren eindeutig bestimmte $a_{ij} \in \mathcal{O}_\mathcal{E}$ mit

$$y \cdot y_i = y_i + p(y' \cdot y_i) = y_i + p\sum_{j=1}^{p} a_{ij} y_j \text{ für alle } i \in \{1, \dots, p\}.$$

Also ist die darstellende Matrix der Multiplikation mit y gegeben durch $I_p + pA$, wobei $A = (a_{ij})_{1\le i,j\le p} \in \mathcal{O}_\mathcal{E}{}^{p\times p}$ die darstellende Matrix der Multiplikation mit y' ist. Für $B := I_p + pA = (b_{ij})_{1\le i,j\le} \in \mathcal{O}_\mathcal{E}{}^{p\times p}$ gilt dann nach der Leibniz-Formel für Determinanten:

$$N_\varphi(x) = \det(B) = \sum_{\tau\in S_p} sign(\tau) \underbrace{\prod_{i=1}^{p} b_{i\tau(i)}}_{\substack{\equiv 0 \bmod p, \\ \text{falls } \tau \neq 1_{S_p}}} \equiv \prod_{i=1}^{p} b_{ii} \bmod p \equiv \prod_{i=0}^{p} (1+pa_{ii}) \bmod p \equiv 1 \bmod p.$$

Also gilt $N_\varphi(1+p\mathcal{O}_\mathcal{E}) \subset 1 + p\mathcal{O}_\mathcal{E}$ und damit wird durch die Abbildung $\mathcal{O}_\mathcal{E}^* \xrightarrow{N_\varphi} \mathcal{O}_\mathcal{E}^* \to \mathcal{O}_\mathcal{E}^*/(1+p\mathcal{O}_\mathcal{E}) \cong E^*$ ein Gruppenhomomorphismus $N_\varphi: E^* \to E^*$, $x \cdot (1+p\mathcal{O}_\mathcal{E}) \to N_\varphi(x) \cdot (1+p\mathcal{O}_\mathcal{E})$ induziert.

Behauptung 2: $N_\varphi: E^* \to E^*$ ist die Identität.
Sei dafür wieder $x \in \mathcal{O}_\mathcal{E}$ und setze $y = \varphi^{-1}(x) \in \mathcal{O}_{\mathcal{E}'}$. Zudem bezeichnen wir mit $\chi_y \in \mathcal{E}[T]$ das charakteristische Polynom von y über $\mathcal{E}$. Man beachte dabei, dass χ_y bereits in $\mathcal{O}_\mathcal{E}[T]$ liegt, da $y \in \mathcal{O}_{\mathcal{E}'}$. Des Weiteren setzen wir $\bar{y} = y \mod p\mathcal{O}_{\mathcal{E}'} \in E'$ und $\chi_{\bar{y}} \in E[T]$ bezeichne das charakteristische Polynom von $\bar{y}$.
Beachte: Ist $\mu_y: \mathcal{E}' \to \mathcal{E}'$ die Multiplikation mit y und $\mu_{\bar{y}}: E' \to E'$ die Multiplikation mit $\bar{y}$, so gilt $\mu_{\bar{y}} = \mu_{y_{|\mathcal{O}_{\mathcal{E}'}}} \mod p\mathcal{O}_{\mathcal{E}'}$. Daher ist die darstellende Matrix von $\mu_{\bar{y}}$ gleich der darstellenden Matrix von μ_y modulo p. Insbesondere gilt:

$$\begin{aligned}
\chi_{\bar{y}} &= \det(T \cdot I_p - \text{ darstellende Matrix von } \mu_{\bar{y}}) \\
&= \det(T \cdot I_p - \text{ darstellende Matrix von } (\mu_y \mod p)) \\
&= \det(T \cdot I_p - \text{ darstellende Matrix von } \mu_y) \mod p \\
&= \chi_y \mod p.
\end{aligned}$$

Nach Lemma 7.15 (v) ist das charakteristische Polynom von $\bar{y}$ gegeben durch $\chi_{\bar{y}}(T) = T^p - \bar{y}^p$. Da φ ein Frobenius-Lift ist, folgt damit

$$\chi_y \mod p = \chi_{\bar{y}} = T^p - \bar{y}^p = T^p - \varphi(y) \mod p = T^p - x \mod p.$$

Wegen $(-1)^{p+1} \equiv 1 \mod p$ ist dann $N_\varphi(x) \equiv x \mod p$ und $T_\varphi(x) \equiv 0 \mod p$, womit Behauptung 2 gezeigt wäre.

Betrachte nun den Gruppenhomomorphismus $(N_\varphi - 1)\colon \mathcal{O}_\mathcal{E}^* \to \mathcal{O}_\mathcal{E}^*$, $x \mapsto \frac{N_\varphi(x)}{x}$ und das kommutative Diagramm

$$\begin{array}{ccccccccc} 0 & \longrightarrow & 1 + p\mathcal{O}_\mathcal{E} & \longrightarrow & {\mathcal{O}_\mathcal{E}}^* & \longrightarrow & E^* & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f=(N_\varphi-1)} & & \downarrow{\scriptstyle g=(N_\varphi-1)} & & \downarrow{\scriptstyle h=(N_\varphi-1)} & & \\ 0 & \longrightarrow & 1 + p\mathcal{O}_\mathcal{E} & \longrightarrow & {\mathcal{O}_\mathcal{E}}^* & \longrightarrow & E^* & \longrightarrow & 0 \end{array}$$

mit exakten Reihen. Durch das Schlangenlemma erhalten wir nun die exakte Sequenz

$$0 \to \ker(f) \to \ker(g) \to \ker(h) \to \operatorname{coker}(f) \to \operatorname{coker}(g) \to \operatorname{coker}(h) \to 0.$$

Insbesondere hat man wegen $N_\varphi\colon E^* \to E^* = id_{E^*}$ eine exakte Sequenz

$$0 \to (1 + p\mathcal{O}_\mathcal{E})^{N_\varphi} \to (\mathcal{O}_\mathcal{E}^*)^{N_\varphi} \to E^* \to (1 + p\mathcal{O}_\mathcal{E})/(N_\varphi - 1)(1 + p\mathcal{O}_\mathcal{E}) \,,$$

denn h ist der triviale Homomorphismus.

Behauptung 3: $(1 + p\mathcal{O}_\mathcal{E})^{N_\varphi} = (1 + p\mathcal{O}_\mathcal{E})/(N_\varphi - 1)(1 + p\mathcal{O}_\mathcal{E}) = 1$.
Als erstes zeigen wir, dass $(1 + p\mathcal{O}_\mathcal{E})^{N_\varphi}$ nur das Element 1 enthält. Sei deshalb $x = 1 + p^r x' \in 1 + p^r\mathcal{O}_\mathcal{E}$, $y' = \varphi^{-1}(x') \in \mathcal{O}_{\mathcal{E}'}$ und $y = \varphi^{-1}(x) = 1 + p^r y' \in 1 + p^r\mathcal{O}_{\mathcal{E}'}$ für $r \geq 1$. Wie bereits zuvor gesehen, ist die darstellende Matrix der Multiplikation mit y gegeben durch $B := I_p + p^r A = (b_{ij})_{1\leq i,j\leq p} \in {\mathcal{O}_\mathcal{E}}^{p\times p}$, wobei $A = (a_{ij})_{1\leq i,j\leq p} \in {\mathcal{O}_\mathcal{E}}^{p\times p}$ die darstellende Matrix der Multiplikation mit y' ist. Durch die Leibniz-Formel für Determinanten ergibt sich dann

$$N_\varphi(x) = \det(B) = \sum_{\tau\in S_p} sign(\tau) \cdot \underbrace{\prod_{i=1}^{p} b_{i\tau(i)}}_{\substack{\equiv 0 \bmod p^{r+1},\\ \text{falls } \tau\neq 1_{S_p}}} \equiv \prod_{i=0}^{p} b_{ii} \mod p^{r+1} \equiv \prod_{i=0}^{p}(1 + p^r a_{ii}) \mod p^{r+1}$$

$$\equiv 1 + p^r \sum_{i=0}^{p} a_{ii} \mod p^{r+1} \equiv 1 + p^r T_\varphi(x') \mod p^{r+1} \equiv 1 \mod p^{r+1},$$

da, wie wir bereits zuvor gesehen haben, $T_\varphi(x') \equiv 0 \mod p$ für alle $x' \in \mathcal{O}_\mathcal{E}$. Wegen

$$(1 + p\mathcal{O}_\mathcal{E})\backslash\{1\} = \bigcup_{r\geq 1} ((1 + p^r\mathcal{O}_\mathcal{E})\backslash(1 + p^{r+1}\mathcal{O}_\mathcal{E})) \quad \text{und} \quad N_\varphi(1 + p^r\mathcal{O}_\mathcal{E}) \subset 1 + p^{r+1}\mathcal{O}_\mathcal{E}$$

ist dann $N_\varphi(x) \neq x$ für alle $x \in (1+p\mathcal{O}_\mathcal{E})\backslash\{1\}$ und damit $(1+p\mathcal{O}_\mathcal{E})^{N_\varphi} = \{1\}$.

Als nächstes zeigen wir die Surjektivität von $(N_\varphi - 1)\colon 1+p\mathcal{O}_\mathcal{E} \to 1+p\mathcal{O}_\mathcal{E}$, was gleichbedeutend zu $\operatorname{coker}(N_\varphi - 1) = \{1\}$ ist. Sei dafür $x = 1+py \in 1+p\mathcal{O}_\mathcal{E}$ mit $y \in \mathcal{O}_\mathcal{E}$. Dann ist aufgrund der Vollständigkeit von $\mathcal{O}_\mathcal{E}$ auch

$$x^{-1} = \sum_{n=0}^{\infty}(-py)^n \in (1+p\mathcal{O}_\mathcal{E}).$$

Damit ist $(N_\varphi^n(x^{-1}))_{n\geq 0}$ eine konvergente Folge in $1+p\mathcal{O}_\mathcal{E}$ mit $\lim_{n\to\infty} N_\varphi^n(x^{-1}) = 1$, denn $N_\varphi(1+p^r\mathcal{O}_\mathcal{E}) \subset 1+p^{r+1}\mathcal{O}_\mathcal{E}$ für alle $r \geq 1$.

Behauptung 4: Für $a_n \in (1+p\mathcal{O}_\mathcal{E})$ gilt $\lim_{n\to\infty} a_n = 1$ genau dann, wenn $\prod_{n=0}^{\infty} a_n$ in $1+p\mathcal{O}_\mathcal{E}$ konvergiert.
Da alle a_n Einheiten sind, ist die Bewertung von $\prod_{n=0}^{m} a_n$ gleich 0 für alle $m \geq 0$. Zusammen mit der Abgeschlossenheit von $1+p\mathcal{O}_\mathcal{E}$ und der Vollständigkeit von $\mathcal{O}_\mathcal{E}$ folgt dann

$$\begin{aligned}
\lim_{n\to\infty} a_n = 1 &\Leftrightarrow \forall C \geq 0\ \exists N \in \mathbb{N}\ \forall m \geq N\colon\ v(a_m - 1) \geq C \\
&\Leftrightarrow \forall C \geq 0\ \exists N \in \mathbb{N}\ \forall m \geq N\colon\ v(a_m - 1) + v\left(\prod_{n=0}^{m} a_n\right) \geq C \\
&\Leftrightarrow \forall C \geq 0\ \exists N \in \mathbb{N}\ \forall m \geq N\colon\ v\left(\prod_{n=0}^{m+1} a_n - \prod_{n=0}^{m} a_n\right) \geq C \\
&\Leftrightarrow \left(\prod_{n=0}^{m} a_n\right)_{m\geq 0} \text{ ist eine Cauchyfolge in } 1+p\mathcal{O}_\mathcal{E} \\
&\Leftrightarrow \prod_{n=0}^{\infty} a_n \text{ konvergiert in } 1+p\mathcal{O}_\mathcal{E}.
\end{aligned}$$

Also konvergiert insbesondere $z := \prod_{n=0}^{\infty} N_\varphi^n(x^{-1})$ in $1+p\mathcal{O}_\mathcal{E}$.

Behauptung 5: $x = \frac{N_\varphi(z)}{z}$.
Es genügt zu zeigen, dass $N_\varphi(z) = \prod_{n=1}^{\infty} N_\varphi^n(x^{-1})$. Wir setzen $z_m := \prod_{n=0}^{m} N_\varphi^n(x^{-1})$ und wählen für $C > 0$ ein $N \in \mathbb{N}$, sodass für alle $m \geq N$: $v(z - z_m) \geq C$, d.h. $z_m^{-1}z = 1 + p^C\tilde{y}$ für ein $\tilde{y} \in \mathcal{O}_\mathcal{E}$. Aufgrund der Multiplikativität von N_φ, $N_\varphi(1+p^r\mathcal{O}_\mathcal{E}) \subset 1+p^{r+1}\mathcal{O}_\mathcal{E}$ für alle $r \geq 1$ und $N_\varphi(1) = 1$ gilt dann

$$N_\varphi(z_m)^{-1}N_\varphi(z) = N_\varphi(z_m^{-1}z) = 1 + p^{C+1}\tilde{z} \text{ für ein } \tilde{z} \in \mathcal{O}_\mathcal{E}.$$

Damit gilt für alle $m \geq N$:

$$v(N_\varphi(z) - \prod_{n=1}^{m+1} N_\varphi^n(x^{-1})) = v(N_\varphi(z) - N_\varphi(z_m)) = v(p^{C+1}\tilde{z}N_\varphi(z_m)) \geq C+1.$$

Also ist $N_\varphi(z) = \prod_{n=1}^{\infty} N_\varphi^n(x^{-1}) = x\prod_{n=0}^{\infty} N_\varphi^n(x^{-1}) = x \cdot z$, woraus schließlich die Behauptung und damit die Surjektivität von $N_\varphi - 1$ folgt.

Zusammengefasst hat man also die exakte Sequenz

$$1 \longrightarrow (\mathcal{O}_\mathcal{E}^*)^{N_\varphi} \longrightarrow E^* \longrightarrow 1$$

und damit die zu zeigende Isomorphie. □

Definition 7.18. Der Isomorphismus $Col\colon E^* \xrightarrow{\sim} (\mathcal{O}_\mathcal{E}^*)^{N_\varphi}$, der invers zum Isomorphismus aus Satz 7.17 ist, heißt Coleman-Isomorphismus.

Korollar 7.19. *Der Gruppenhomomorphismus* $(\mathcal{O}_\mathcal{E}^*)^{N_\varphi} \times (1 + p\mathcal{O}_\mathcal{E}) \to \mathcal{O}_\mathcal{E}^*$, $(x, y) \mapsto x \cdot y$ *ist ein Isomorphismus.*

Beweis. Die Sequenz $0 \to 1 + p\mathcal{O}_\mathcal{E} \to \mathcal{O}_\mathcal{E}^* \to E^* \to 0$ ist exakt und $Col\colon E^* \xrightarrow{\sim} (\mathcal{O}_\mathcal{E}^*)^{N_\varphi} \hookrightarrow \mathcal{O}_\mathcal{E}^*$ nach Satz 7.17 ein Schnitt der Projektion $\mathcal{O}_\mathcal{E}^* \to E^*$. □

Der Coleman-Isomorphismus wird uns im Folgenden noch sehr nützlich sein, wir wollen diesen jedoch kurz vernachlässigen und uns stattdessen die Körpererweiterung $\mathcal{E}'|\mathcal{E}$ etwas genauer anschauen. Dazu bezeichnen wir mit ζ eine primitive p-te Einheitswurzel. Wir haben bereits gesehen, dass das Polynom $f(X) = (1+X)^p - 1 - t \in \mathcal{O}_\mathcal{E}[X]$ irreduzibel über $\mathcal{E}$ ist. Damit ist aber auch trivialerweise $f(X-1) = X^p - 1 - t$ irreduzibel über $\mathcal{E}$. Da $\mathcal{E}' = \mathcal{E}[t'] = \mathcal{E}[1+t']$ und $X^p - 1 - t = \prod_{n=0}^{p-1}(X - \zeta^n(1+t'))$, ist $\mathcal{E}'[\zeta]$ der Zerfällungskörper von $X^p - 1 - t$ über $\mathcal{E}$. Also ist $\mathcal{E}'[\zeta]|\mathcal{E}$ Galois und damit insbesondere auch $\mathcal{E}'[\zeta]|\mathcal{E}[\zeta]$.

Man mache sich zunächst einmal klar, dass ganz allgemein ein diskret bewerteter Körper (L, v) mit Uniformisierer p die primitive p-te Einheitswurzel ζ genau dann enthält, wenn $p = 2$ gilt. Für $p = 2$ ist nämlich $\zeta = -1 \in L$. Nehmen wir umgekehrt an, dass ζ bereits in L liegt, so muss wegen $\zeta^p = 1$ auch $v(\zeta) = 0$ gelten. Betrachte nun das Polynom

$$\frac{X^p - 1}{X - 1} = X^{p-1} + \ldots + X + 1 = \prod_{i=1}^{p-1}(X - \zeta^i),$$

woraus wir $p = \prod_{i=1}^{p-1}(1 - \zeta^i)$ erhalten. Somit ist $1 = v(p) = \sum_{i=1}^{p-1} v(1 - \zeta^i)$, d.h. also es existiert genau ein $i_0 \in \{1, \ldots, p-1\}$ mit $v(1 - \zeta^{i_0}) = 1$. Aus $1 \leq v((1 - \zeta^{i_0})(1 + \zeta^{i_0})) = v(1 - \zeta^{2i_0})$ folgt aufgrund der Eindeutigkeit von i_0 entweder $i_0 \equiv 2i_0 \mod p$ oder aber $2i_0 \equiv 0 \mod p$. In beiden Fällen erhält man wegen $1 \leq i_0 \leq p - 1$ schließlich $2 \equiv 0 \mod p$, was $p = 2$ ergibt.

In unserem Fall bedeutet dies, dass entweder ζ kein Element von $\mathcal{E}$ und $\mathcal{E}'$ sein kann oder $p = 2$ gilt. In beiden Fällen ist dann $p - 1 = [\mathcal{E}'[\zeta] : \mathcal{E}'] = [\mathcal{E}[\zeta] : \mathcal{E}]$ und damit

$$p = [\mathcal{E}' : \mathcal{E}] = \frac{[\mathcal{E}'[\zeta] : \mathcal{E}'] \cdot [\mathcal{E}' : \mathcal{E}]}{p-1} = \frac{[\mathcal{E}'[\zeta] : \mathcal{E}]}{p-1} = \frac{[\mathcal{E}'[\zeta] : \mathcal{E}[\zeta]] \cdot [\mathcal{E}[\zeta] : \mathcal{E}]}{p-1} = [\mathcal{E}'[\zeta] : \mathcal{E}[\zeta]].$$

Hieraus sieht man auch sofort, dass dann $X^p - 1 - t$ das Minimalpolynom von $t' + 1$ über $\mathcal{E}[\zeta]$ ist und dieses daher irreduzibel sein muss.

Lemma 7.20. *(i)* $1 - \zeta$ *ist ein Uniformisierer von* $K[\zeta]$ *und* $\mathcal{O}_{K[\zeta]} = \mathcal{O}_K[\zeta] = W[\zeta]$ *ist in der Bewertungstheorie vollständig.*

(ii) $1-\zeta$ *ist ein Uniformisierer von* $\mathcal{E}[\zeta]$ *und* $\mathcal{O}_{\mathcal{E}[\zeta]}$ *ist in der Bewertungstopologie vollständig. Jedes Element* $f \in \mathcal{O}_{\mathcal{E}[\zeta]}$ *besitzt eine Darstellung der Form* $f = \sum_{n\in\mathbb{Z}} a_n t^n$ *mit eindeutig bestimmten Elementen* $a_n \in W[\zeta]$*, sodass* $\lim_{n\to-\infty} a_n = 0$ *in* $W[\zeta]$*.*

(iii) $\mathcal{E}[\zeta] = \mathcal{O}_{\mathcal{E}[\zeta]}[\frac{1}{1-\zeta}] = \{\sum_{n\in\mathbb{Z}} c_n t^n \mid c_n \in K[\zeta], \lim_{n\to-\infty} c_n = 0, \inf_{n\in\mathbb{Z}}\{v(c_n)\} > -\infty\}$.

Beweis. Wie wir zuvor gezeigt haben handelt es sich bei $K[\zeta]|K$ um eine Körpererweiterung vom Grad $p-1$. Sei $(K[\zeta], v)$ die eindeutige Fortsetzung von (K, v_p) nach Satz 1.24. Aufgrund der Eindeutigkeit von v ist $v \circ \sigma = v$ für alle $\sigma \in G_K := Gal(K[\zeta]|K)$. Da sich die Primzahl p schreiben lässt als

$$p = 1^{p-1} + \ldots + 1^1 + 1 = \prod_{n=1}^{p-1}(1-\zeta^n) = \prod_{\sigma\in G_K} \sigma(1-\zeta)$$

erhalten wir

$$e(K[\zeta]|K) = v(p) = v(\prod_{\sigma\in G_K} \sigma(1-\zeta)) = \sum_{\sigma\in G_K} v\circ\sigma(1-\zeta) = \sum_{\sigma\in G_K} v(1-\zeta) = |G_K|\cdot v(1-\zeta).$$

Bei $e(K[\zeta]|K)$ handelt es sich jedoch um eine positive natürliche Zahl mit $e(K[\zeta]|K) \leq [K[\zeta] : K] = p-1$. Also muss zum einen $v(1-\zeta) \geq 1$ und zum anderen

$$v(1-\zeta) = \frac{e(K[\zeta]|K)}{|G_K|} \leq \frac{p-1}{p-1} = 1$$

gelten. Somit ist $e(K[\zeta]|K) = [K[\zeta] : K] = p-1$ und $1-\zeta$ ein Uniformisierer von $K[\zeta]$. Nach Lemma 1.26 *(iii)* ist dann $\mathcal{O}_{K[\zeta]} = \mathcal{O}_K[1-\zeta] = \mathcal{O}_K[\zeta] = W[\zeta]$ und wegen Lemma 1.11 auch vollständig.

Für *(ii)* folgt völlig analog zu *(i)*, dass $1-\zeta$ ein Uniformisierer von $\mathcal{E}[\zeta]$ ist und $\mathcal{O}_{\mathcal{E}[\zeta]} = \mathcal{O}_{\mathcal{E}}[\zeta]$ vollständig ist. Dementsprechend bleibt nur noch zu zeigen, dass jedes Element $f \in \mathcal{O}_{\mathcal{E}[\zeta]}$ eine Darstellung der Form $f = \sum_{n\in\mathbb{Z}} a_n t^n$ mit eindeutig bestimmten Elementen $a_n \in W[\zeta]$ besitzt, sodass $\lim_{n\to-\infty} a_n = 0$ in $W[\zeta]$. Wir zeigen zunächst, dass überhaupt $W[\zeta][[t]] \subset \mathcal{O}_{\mathcal{E}}[\zeta]$ gilt. Aufgrund der t-adischen Vollständigkeit von $W[\zeta][[t]]$ lässt sich jedes Element $f = \sum_{n\geq 0} a_n t^n \in W[\zeta][[t]]$ mit $a_n = \sum_{k=0}^{p-2} a_{nk}\zeta^k \in W[\zeta]$ umordnen zu $f = \sum_{k=0}^{p-2}(\sum_{n\geq 0} a_{nk}t^n)\,\zeta^k$. Ähnlich wie zuvor definieren wir eine schwache Topologie auf $\mathcal{O}_{\mathcal{E}}[\zeta]$ mit Basis offener Nullumgebungen $((1-\zeta)^n\mathcal{O}_{\mathcal{E}} + t^m W[\zeta][[t]])_{n,m\geq 0}$. Völlig analog zu Lemma 7.2 zeigt man, dass $\mathcal{O}_{\mathcal{E}}[\zeta]$ bzgl. der schwachen Topologie

vollständig ist. Damit ergeben Reihen der Form $\sum_{n\in\mathbb{Z}} a_n t^n$ mit $\lim_{n\to-\infty} a_n = 0$ in $W[\zeta]$ überhaupt einen Sinn und wir können diese beliebig umordnen. Sei nun $f \in \mathcal{O}_\mathcal{E}[\zeta]$, d.h. es existieren $f_k = \sum_{n\in\mathbb{Z}} a_{nk} t^n \in \mathcal{O}_\mathcal{E}$ mit

$$f = \sum_{k=0}^{p-2} f_k \zeta^k = \sum_{k=0}^{p-2} \sum_{n\in\mathbb{Z}} a_{nk} t^n \zeta^k = \sum_{n\in\mathbb{Z}} \underbrace{\left(\sum_{k=0}^{p-2} a_{nk} \zeta^k \right)}_{=:a_n \in W[\zeta]} t^n = \sum_{n\in\mathbb{Z}} a_n t^n.$$

Für die Koeffizienten a_n gilt dann

$$\begin{aligned} v(a_n) &\geq \min\{v(a_{nk}\zeta^k) \mid 0 \leq k \leq p-2\} \\ &= \min\{e(K[\zeta]|K) v_p(a_{nk}) + kv(\zeta) \mid 0 \leq k \leq p-2\} \\ &= \min\{(p-1) \underbrace{v_p(a_{nk})}_{\xrightarrow{n\to-\infty}\infty} \mid 0 \leq k \leq p-2\} \xrightarrow{n\to-\infty} \infty. \end{aligned}$$

Ist insbesondere $f = 0$, so muss $f_k = 0$ für alle $k \in \{0, \dots, p-2\}$ gelten, denn $\mathcal{O}_\mathcal{E}[\zeta]$ ist ein freier $\mathcal{O}_\mathcal{E}$-Modul vom Rang $p-1$. Aufgrund der eindeutigen Schreibweise von f_k in $\mathcal{O}_\mathcal{E}$ muss $a_{nk} = 0$ und damit auch $a_n = 0$ für alle $n \in \mathbb{Z}$ gelten.

Nach (i) und (ii) ist $1-\zeta$ ein Uniformisierer von $\mathcal{E}[\zeta]$ und $K[\zeta]$, d.h. $\mathcal{E}[\zeta] = \mathcal{O}_{\mathcal{E}[\zeta]}[\frac{1}{1-\zeta}]$ und $K[\zeta] = \mathcal{O}_{K[\zeta]}[\frac{1}{1-\zeta}]$. Völlig analog zur Vorgehensweise nach Definition 7.11 erhält man

$$\mathcal{E}[\zeta] = \mathcal{O}_{\mathcal{E}[\zeta]}\left[\frac{1}{1-\zeta}\right] = \left\{ \sum_{n\in\mathbb{Z}} c_n t^n \mid c_n \in K[\zeta], \lim_{n\to-\infty} c_n = 0, \inf_{n\in\mathbb{Z}}\{v(c_n)\} > -\infty \right\},$$

wobei man den dortigen Uniformisierer p durch den neuen Uniformisierer $1-\zeta$ ersetzen muss. □

Bemerkung 7.21. Da $E' \cong k((t_p)) = k((t'))$ und $\mathcal{O}_{\mathcal{E}'} = \mathcal{O}_\mathcal{E}[t']$ ein p-Cohen-Ring von E' ist, folgt in absoluter Analogie:

- $\mathcal{O}_{\mathcal{E}'[\zeta]} = \mathcal{O}_{\mathcal{E}'}[\zeta] = \{\sum_{n\in\mathbb{Z}} a_n t'^n \mid a_n \in W[\zeta], \lim_{n\to-\infty} a_n = 0\}$;
- $\mathcal{E}'[\zeta] = \{\sum_{n\in\mathbb{Z}} c_n t'^n \mid c_n \in K[\zeta], \lim_{n\to-\infty} c_n = 0, \inf_{n\in\mathbb{Z}}\{v(c_n)\} > -\infty\}$.

Mit dieser eindeutigen Darstellung der Elemente von $\mathcal{E}[\zeta]$ und $\mathcal{E}'[\zeta]$ können wir analog zur Abbildung $d\colon \mathcal{E} \to \Omega_{\mathcal{E}|K}$ die Abbildungen

$$d\colon \mathcal{E}[\zeta] \to \mathcal{E}[\zeta] \cdot dt =: \Omega_{\mathcal{E}[\zeta]|K[\zeta]},\ f \mapsto \frac{df}{dt} \cdot dt$$

und

$$d\colon \mathcal{E}'[\zeta] \to \mathcal{E}'[\zeta] \cdot dt' =: \Omega_{\mathcal{E}'[\zeta]|K[\zeta]},\ f \mapsto \frac{df}{dt'} \cdot dt'$$

definieren. Wir wollen uns nun verdeutlichen, dass die Galoisgruppe $G := Gal(\mathcal{E}'[\zeta]|\mathcal{E}[\zeta])$ auf $\Omega_{\mathcal{E}'[\zeta]|K[\zeta]}$ durch $\sigma(f \cdot dt') := \sigma(f) \cdot d\sigma(t')$ operiert. Die Operation von 1_G ist dabei offensichtlich trivial. Da $\mathcal{E}'[\zeta]$ der Zerfällungskörper von $X^p - 1 - t$ ist, zerfällt dieses Polynom komplett in Linearfaktoren

$$X^p - 1 - t = \prod_{n=0}^{p-1}(X - \zeta^n(1+t')) = \prod_{\sigma\in G}(X - \sigma(1+t')).$$

Somit erhält man einen Gruppenisomorphismus $\chi: G \to \mathbb{Z}/p\mathbb{Z}$, welcher durch $\sigma(1 + t') = \zeta^{\chi(\sigma)}(1 + t')$ charakterisiert ist. Daher gilt $\sigma(t') = \zeta^{\chi(\sigma)}(1 + t') - 1$ für alle $\sigma \in G$ und man erhält dadurch

$$d\sigma(t') = \frac{d\sigma(t')}{dt'} \cdot dt' = \frac{d}{dt'}(\zeta^{\chi(\sigma)}(1+t') - 1) \cdot dt' = \zeta^{\chi(\sigma)} \cdot dt'.$$

Sind nun $\tau, \sigma \in G$, so hat man für $f \in \mathcal{E}'[\zeta]$ schließlich

$$\begin{aligned}
\tau(\sigma(f \cdot dt')) &= \tau(\sigma(f) \cdot d\sigma(t')) = \tau(\zeta^{\chi(\sigma)}\sigma(f) \cdot dt') \\
&= \tau(\zeta^{\chi(\sigma)})\tau \circ \sigma(f) \cdot d\tau(t') = \zeta^{\chi(\sigma)}\zeta^{\chi(\tau)}(\tau \circ \sigma)(f) \cdot dt' \\
&= \zeta^{\chi(\sigma)+\chi(\tau)}(\tau \circ \sigma)(f)dt' = (\tau \circ \sigma)(f)\zeta^{\chi(\tau\circ\sigma)} \cdot dt' \\
&= (\tau \circ \sigma)(f)d(\tau \circ \sigma)(t') = (\tau \circ \sigma)(f \cdot dt').
\end{aligned}$$

Also operiert G auf $\Omega_{\mathcal{E}'[\zeta]|K[\zeta]}$ und die Operation ist wegen $\sigma_{|_{\mathcal{E}[\zeta]}} = id_{\mathcal{E}[\zeta]}$ für alle $\sigma \in G$ auch $\mathcal{E}[\zeta]$-linear.

Mittels der kanonischen G-Operation auf $\mathcal{E}'[\zeta]$ ist $d: \mathcal{E}'[\zeta] \to \Omega_{\mathcal{E}'[\zeta]|K[\zeta]}$ sogar G-äquivariant. Dazu müssen wir zunächst zeigen, dass jedes $\sigma \in G$ bzgl. der schwachen Topologie auf $\mathcal{E}'[\zeta]$ stetig ist. Dafür genügt es die schwache Stetigkeit von $\sigma_{|_{\mathcal{O}_{\mathcal{E}'}[\zeta]}}: \mathcal{O}_{\mathcal{E}'}[\zeta] \to \mathcal{O}_{\mathcal{E}'}[\zeta]$ zu beweisen. Für $\sigma = id$ ist die Stetigkeit trivial. Sei deshalb $\sigma \neq id$ und für $n, m \geq 0$ setzen wir $U := (1-\zeta)^n\mathcal{O}_{\mathcal{E}'}[\zeta] + t'^{n+m}W[\zeta][[t']]$. Dann gilt wegen $\sigma(t') = \zeta^{\chi(\sigma)}t' + \zeta^{\chi(\sigma)} - 1$ schließlich

$$\begin{aligned}
\sigma(U) &= \sigma(1-\zeta)^n\sigma(\mathcal{O}_{\mathcal{E}'}[\zeta]) + \sigma(t')^{n+m}\sigma(W[\zeta][[t']]) \\
&\subset (1-\zeta)^n\mathcal{O}_{\mathcal{E}'}[\zeta] + (\zeta^{\chi(\sigma)}t' + \zeta^{\chi(\sigma)} - 1)^{n+m}W[\zeta][[t']] \\
&= (1-\zeta)^n\mathcal{O}_{\mathcal{E}'}[\zeta] + \left(\sum_{j=0}^{n+m}\binom{n+m}{j}\zeta^{\chi(\sigma)j}t'^j(\zeta^{\chi(\sigma)} - 1)^{n+m-j}\right)W[\zeta][[t']] \\
&\subset (1-\zeta)^n\mathcal{O}_{\mathcal{E}'}[\zeta] + (\zeta^{\chi(\sigma)} - 1)^nW[\zeta][[t']] + t'^mW[\zeta][[t']] \\
&\subset (1-\zeta)^n\mathcal{O}_{\mathcal{E}'}[\zeta] - (1-\zeta)^n(\zeta^{\chi(\sigma)-1} + \ldots + \zeta + 1)^n\mathcal{O}_{\mathcal{E}'}[\zeta] + t'^mW[\zeta][[t']] \\
&\subset (1-\zeta)^n\mathcal{O}_{\mathcal{E}'}[\zeta] + t'^mW[\zeta][[t']],
\end{aligned}$$

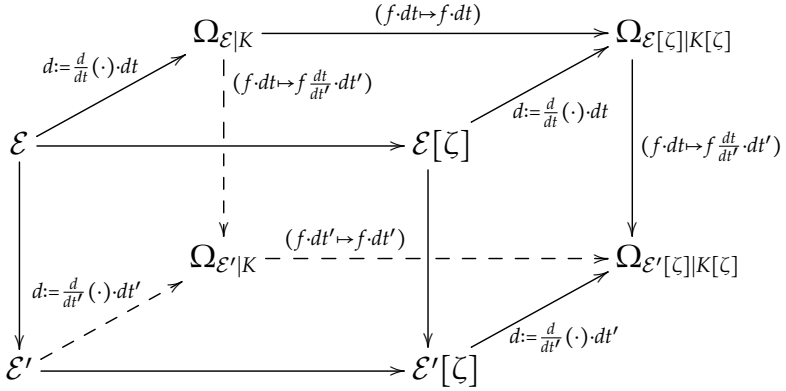
woraus man die schwache Stetigkeit von σ erhält. Sind nun $f = \sum_{n\in\mathbb{Z}} c_n t'^n \in \mathcal{E}'[\zeta]$ und $\sigma \in G$, so gilt wegen der schwachen Stetigkeit von σ schließlich

$$\begin{aligned} d(\sigma(f)) &= d\left(\sum_{n\in\mathbb{Z}} c_n \sigma(t')^n\right) = \left(\sum_{n\in\mathbb{Z}} c_n n \sigma(t')^{n-1} \frac{d\sigma(t')}{dt'}\right) \cdot dt' \\ &= \sigma\left(\sum_{n\in\mathbb{Z}} c_n n t'^{n-1}\right) \frac{d\sigma(t')}{dt'} \cdot dt' = \sigma\left(\frac{df}{dt'}\right) \cdot d\sigma(t') \\ &= \sigma\left(\frac{df}{dt'} \cdot dt'\right) = \sigma(df). \end{aligned}$$

Aufgrund der Gleichung $t = (1+t')^p - 1$ ergibt sich

$$dt = \frac{dt}{dt'} \cdot dt' = \frac{d((1+t')^p - 1)}{dt'} \cdot dt' = p(1+t')^{p-1} \cdot dt'$$

und wir erhalten den kommutativen Würfel



(7.22)

Lemma 7.23. *(i)* $(\Omega_{\mathcal{E}'[\zeta]|K[\zeta]})^G = \Omega_{\mathcal{E}[\zeta]|K[\zeta]}$

(ii) Die Abbildung $tr\colon \Omega_{\mathcal{E}'[\zeta]|K[\zeta]} \to \Omega_{\mathcal{E}[\zeta]|K[\zeta]}$, $w \mapsto \sum_{\sigma\in G} \sigma(w)$ *schränkt sich zu einer* $\mathcal{E}$*-linearen Abbildung* $tr\colon \Omega_{\mathcal{E}'|K} \to \Omega_{\mathcal{E}|K}$ *ein.*

Beweis. Wir haben schon zuvor gesehen, dass $dt = p(1+t')^{p-1} \cdot dt'$ und damit auch

$$\frac{dt}{p(1+t)} = \frac{dt}{p(1+t')^p} = \frac{p(1+t')^{p-1} \cdot dt'}{p(1+t')^p} = \frac{dt'}{1+t'}.$$

Um (i) zu beweisen, zeigen wir die folgende Kette von Inklusionen

$$(\Omega_{\mathcal{E}'[\zeta]|K[\zeta]})^G \subset \left(\frac{1}{p}\sum_{\sigma\in G} \sigma\right) \Omega_{\mathcal{E}'[\zeta]|K[\zeta]} \subset \Omega_{\mathcal{E}[\zeta]|K[\zeta]} \subset (\Omega_{\mathcal{E}'[\zeta]|K[\zeta]})^G.$$

Die erste Inklusion ist dabei leicht zu sehen, denn für $x \in (\Omega_{\mathcal{E}'[\zeta]|K[\zeta]})^G$ ist $x = \frac{1}{p}\sum_{\sigma\in G}\sigma(x)$. Für die zweite Inklusion wenden wir $\frac{1}{p}\sum_{\sigma\in G}\sigma$ auf ein $f\cdot dt' \in \Omega_{\mathcal{E}'[\zeta]|K[\zeta]}$ an:

$$\begin{aligned}\frac{1}{p}\sum_{\sigma\in G}\sigma(f\cdot dt') &= \frac{1}{p}\sum_{\sigma\in G}\sigma(f)\cdot d\sigma(t') = \frac{1}{p}\sum_{\sigma\in G}\sigma(f)\zeta^{\chi(\sigma)}\cdot dt'\\ &= \frac{1}{p}\sum_{\sigma\in G}\sigma(f)\underbrace{\zeta^{\chi(\sigma)}(1+t')}_{=\sigma(1+t')}\cdot\frac{dt'}{1+t'}\\ &= \underbrace{\left(\frac{1}{p}\sum_{\sigma\in G}\sigma(f\cdot(1+t'))\right)}_{\in(\mathcal{E}'[\zeta])^G=\mathcal{E}[\zeta]}\underbrace{\frac{1}{p(1+t)}}_{\in\mathcal{E}[\zeta]}\cdot dt \in \Omega_{\mathcal{E}[\zeta]|K[\zeta]}.\end{aligned}$$

Damit bleibt nur noch die letzte Inklusion zu zeigen. Wenden wir dafür $\sigma\in G$ auf ein $f\cdot dt \in \Omega_{\mathcal{E}[\zeta]|K[\zeta]}$ an, so erhalten wir

$$\begin{aligned}\sigma(f\cdot dt) &= \sigma(fp(1+t')^{p-1}\cdot dt') = \sigma(f)p\zeta^{\chi(\sigma)(p-1)}(1+t')^{p-1}\underbrace{d\sigma(t')}_{=\zeta^{\chi(\sigma)}\cdot dt'}\\ &= \underbrace{\sigma(f)}_{=f}\underbrace{\zeta^{\chi(\sigma)p}}_{=1}\underbrace{p(1+t')^{p-1}\cdot dt'}_{=dt} = f\cdot dt,\end{aligned}$$

womit die Gleichheit gezeigt wäre.

Für (ii) wollen wir zunächst zeigen, dass für ein $g\in\mathcal{E}'$ die Summe $\sum_{\sigma\in G}\sigma(g)$ bereits in $\mathcal{E}$ liegt. Da $\mathcal{E}'[\zeta] = (\mathcal{E}[\zeta])[1+t']$, existieren für $f\in\mathcal{E}'[\zeta]$ eindeutig bestimmte $f_0,\dots,f_{p-1}\in\mathcal{E}[\zeta]$ mit $f=\sum_{i=0}^{p-1}f_i(1+t')^i$ und es gilt

$$\sum_{\sigma\in G}\sigma(f) = \sum_{\sigma\in G}\sum_{i=0}^{p-1}\sigma(f_i)\sigma(1+t')^i = \sum_{\sigma\in G}\sum_{i=0}^{p-1}f_i\zeta^{i\chi(\sigma)}(1+t')^i = \sum_{i=0}^{p-1}\underbrace{\left(\sum_{k=0}^{p-1}(\zeta^i)^k\right)}_{=0\text{ für }i\neq 0}f_i(1+t')^i = p\cdot f_0.$$

Ist nun $g=\sum_{i=0}^{p-1}f_i(1+t')^i\in\mathcal{E}'$, so liegen alle $f_0,\dots,f_{p-1}$ bereits in $\mathcal{E}$, da $\{1,(1+t'),\dots,(1+t')^{p-1}\}$ sowohl eine $\mathcal{E}[\zeta]$-Basis von $\mathcal{E}'[\zeta]$, als auch eine $\mathcal{E}$-Basis von $\mathcal{E}'$ ist. Also liegt für $g\in\mathcal{E}'$ die Summe $\sum_{\sigma\in G}\sigma(g) = p\cdot f_0$ in $\mathcal{E}$. Damit erhalten wir für $g\in\mathcal{E}'$ schließlich

$$\begin{aligned}tr(g\cdot dt') &= \sum_{\sigma\in G}\sigma(g)\cdot d\sigma(t') = \sum_{\sigma\in G}\sigma(g)\zeta^{\chi(\sigma)}\cdot dt' = \sum_{\sigma\in G}\sigma(g)\zeta^{\chi(\sigma)}(1+t')\frac{dt'}{(1+t')}\\ &= \left(\sum_{\sigma\in G}\sigma(g\cdot(1+t'))\right)\frac{1}{p(1+t)}\cdot dt \in \Omega_{\mathcal{E}|K}.\end{aligned}$$

□

Lemma 7.24. *(i) Schreibt man* $f = \sum_{i=0}^{p-1} f_i(1+t')^i \in \mathcal{E}' = \mathcal{E}[1+t']$ *mit* $f_0, \dots f_{p-1} \in \mathcal{E}$ *wie oben, so gilt*

$$tr(f \cdot dt') = f_{p-1} \cdot dt \in \mathcal{E} \cdot dt = \Omega_{\mathcal{E}|K}.$$

Insbesondere ist dann wegen $\mathcal{O}_{\mathcal{E}'} = \mathcal{O}_{\mathcal{E}}[1+t']$ *auch* $tr(\mathcal{O}_{\mathcal{E}'} \cdot dt') \subset \mathcal{O}_{\mathcal{E}} \cdot dt$.

(ii) $tr: \Omega_{\mathcal{E}'|K} \to \Omega_{\mathcal{E}|K}$ *ist stetig bzgl. der schwachen Topologie.*

Beweis. Zu (i): Für $f = \sum_{i=0}^{p-1} f_i(1+t')^i$ mit $f_i \in \mathcal{E}$ gilt:

$$\begin{aligned} tr(f \cdot dt') &= \sum_{\sigma \in G} \sigma(f \cdot dt') = \sum_{i=0}^{p-1} f_i \sum_{\sigma \in G} \sigma(1+t')^i \cdot d\sigma(t') \\ &= \sum_{i=0}^{p-1} f_i \underbrace{\left(\sum_{\sigma \in G} (\zeta^{i+1})^{\chi(\sigma)} \right)}_{=0 \text{ für } i \neq p-1} (1+t')^i \cdot dt' \\ &= f_{p-1} p (1+t')^{p-1} \cdot dt' = f_{p-1} \cdot dt. \end{aligned}$$

Für (ii) zeigen wir zunächst

(a) $tr(W[[t']] \cdot dt') \subset W[[t]] \cdot dt$;

(b) $\forall n, m \geq 0 \; \exists M \geq 0 : \; tr(t'^M W[[t']] \cdot dt') \subset (p^n \mathcal{O}_{\mathcal{E}} + t^m W[[t']]) \cdot dt$.

Ähnlich wie im Beweis von Lemma 5.2 zeigt man, dass sowohl $W[[t]]$ als auch $W[[t']]$ separiert und vollständig bzgl. der p-adischen Topologie ist. Betrachtet man nun die Restklassen $\mod p$ von $(1+t')^i$ mit $0 \leq i \leq p-1$, so bilden diese nach Lemma 1.26 eine Basis der Erweiterung $k[[t']]|k[[t]]$. Für ein $f \in W[[t']]$ existieren dann $f_{0i} \in W[[t]]$ mit $0 \leq i \leq p-1$ und ein $f_1' \in W[[t']]$ mit

$$f = \sum_{i=0}^{p-1} f_{0i}(1+t')^i + p f_1'.$$

Genauso existieren $f_{1i} \in W[[t]]$ mit $0 \leq i \leq p-1$ und ein $f_2' \in W[[t']]$, sodass

$$\begin{aligned} f &= \sum_{i=0}^{p-1} f_{0i}(1+t')^i + p f_1' = \sum_{i=0}^{p-1} f_{0i}(1+t')^i + p \left(\sum_{i=0}^{p-1} f_{1i}(1+t')^i + p f_2' \right) \\ &= \sum_{i=0}^{p-1} (f_{0i} + p f_{1i})(1+t')^i + p^2 f_2'. \end{aligned}$$

Induktiv erhalten wir für $n \in \mathbb{N}$ Elemente $f_{ji} \in W[[t]]$ mit $0 \leq i \leq p-1$, $0 \leq j \leq n$ und $f_n' \in W[[t']]$ mit

$$f = \sum_{i=0}^{p-1} \left(\sum_{j=0}^{n} p^j f_{ji} \right) (1+t')^i + p^n f_n'.$$

Aufgrund der p-adischen Separiertheit von $W[[t']]$ und der p-adischen Vollständigkeit von $W[[t]]$ und $W[[t']]$ gilt dann

$$f = \sum_{i=0}^{p-1} \underbrace{\left(\sum_{j=0}^{\infty} p^j f_{ij} \right)}_{=:f_i \in W[[t]]} (1+t')^i = \sum_{i=0}^{p-1} f_i (1+t')^i.$$

Da auch $W[[t]]$ p-adisch separiert ist und die Restklassen $\mod p$ von $1, (1+t'), \ldots, (1+t')^{p-1}$ eine Basis von $k[[t']]|k[[t]]$ bilden, ist die obige Summendarstellung sogar eindeutig. Also bilden $1, (1+t'), \ldots, (1+t')^{p-1}$ auch eine Basis von $W[[t']]|W[[t]]$. Wegen (i) ist damit $tr(f \cdot dt') = f_{p-1} \cdot dt \in W[[t]] \cdot dt$.

Für (b) seien $n, m \geq 0$ zwei beliebige natürliche Zahlen. Wir setzen $M := p(m+n) \geq 0$ und wählen ein $f = t'^M g \in t'^M W[[t']]$ mit $g \in W[[t']]$. Wegen $t = (1+t')^p - 1$ können wir t'^p schreiben als $t'^p = t + px$, wobei $x = -\frac{1}{p} \sum_{i=1}^{p-1} \binom{p}{i} t'^i \in W[[t']]$. Damit lässt sich f wie folgt zerlegen:

$$\begin{aligned}
f &= t'^M g = (t'^p)^{m+n} g = (t+px)^{m+n} g \\
&= \left(\sum_{i=0}^{m+n} \binom{m+n}{i} t^{m+n-i} (px)^i \right) g \\
&= t^m \underbrace{\left(\sum_{i=0}^{n} \binom{m+n}{i} t^{n-i} (px)^i \right) g}_{=:h_1 \in W[[t']]} + p^n \underbrace{\left(\sum_{i=n+1}^{m+n} \binom{m+n}{i} t^{m+n-i} p^{i-n} x^i \right) g}_{=:h_2 \in W[[t']]} \\
&= t^m h_1 + p^n h_2.
\end{aligned}$$

Aufgrund der eindeutigen Summendarstellung in $\mathcal{E}' = \mathcal{E}[1+t']$ ist tr $\mathcal{E}$-linear. Zusammen mit (a) folgt dann

$$tr(f \cdot dt') = t^m tr(h_1 \cdot dt') + p^n tr(h_2 \cdot dt') \in (t^m W[[t]] + p^n W[[t]]) \cdot dt \subset (t^m W[[t]] + p^n \mathcal{O}_{\mathcal{E}}) \cdot dt,$$

womit auch (b) gezeigt wäre.

Um die Stetigkeit von tr zu zeigen, wählen wir eine offene Menge $U \cdot dt \subset \Omega_{\mathcal{E}|K}$ und $f \cdot dt' \in tr^{-1}(U \cdot dt)$. Dann existieren für jedes $k \geq 0$ natürliche Zahlen $n, m \geq 0$ mit

$$tr(f \cdot dt') + p^{-k}(p^n \mathcal{O}_{\mathcal{E}} + t^m W[[t]]) \cdot dt \subset U \cdot dt.$$

Wählen wir $M \in \mathbb{N}$ wie in (b) und setzen $U_{nM}^{(k)} := p^{-k}(p^n \mathcal{O}_{\mathcal{E}'} + t'^M W[[t']])$, so gilt schließlich

$$\begin{aligned}
tr(f \cdot dt' + U_{nM}^{(k)} \cdot dt') &= tr(f \cdot dt') + p^{-k}(p^n tr(\mathcal{O}_{\mathcal{E}'} \cdot dt') + tr(t'^M W[[t']] \cdot dt')) \\
&\subset tr(f \cdot dt') + p^{-k}(p^n \mathcal{O}_{\mathcal{E}} \cdot dt + t^m W[[t]] \cdot dt) \\
&\subset U \cdot dt.
\end{aligned}$$

Also ist $tr^{-1}(U \cdot dt)$ offen in $\Omega_{\mathcal{E}'|K}$ und damit $tr\colon \Omega_{\mathcal{E}'|K} \to \Omega_{\mathcal{E}|K}$ stetig bzgl. der schwachen Topologie. □

Lemma 7.25. *(i) Die Abbildung $\varphi\colon \Omega_{\mathcal{E}'|K} \to \Omega_{\mathcal{E}'|K}$, $f \cdot dt' \mapsto \varphi(f) \cdot d\varphi(t')$ bildet isomorph auf $\Omega_{\mathcal{E}|K} \subset \Omega_{\mathcal{E}'|K}$ ab.*

(ii) Für $u \in E^*$ gilt:

$$(tr \circ \varphi^{-1})(d_{log}(Col(u))) = d_{log}(Col(u)),$$

wobei $d_{log}\colon \mathcal{E}^* \to \Omega_{\mathcal{E}|K}$, $f \mapsto f^{-1}\frac{df}{dt} \cdot dt$.

Beweis. Wir haben bereits zuvor gesehen, dass $\varphi\colon \mathcal{E}' \to \mathcal{E}'$ isomorph auf $\mathcal{E} \subset \mathcal{E}'$ abbildet. Außerdem ist $\varphi(t') = t$, womit schließlich die gewünschte Isomorphie folgt. Für (ii) wollen wir zunächst zeigen, dass die folgenden Aussagen gelten.

(a) $\varphi \circ \frac{d}{dt'} = \frac{d}{dt} \circ \varphi$ als Abbildungen von $\mathcal{E}'$ nach $\mathcal{E}$, denn für $a \in W, n \in \mathbb{Z}$ gilt

$$\varphi\left(\frac{d}{dt'}(at'^n)\right) = \varphi(ant'^{n-1}) = n\varphi(a)t^{n-1} = \frac{d}{dt}(\varphi(a)t^n) = \frac{d}{dt}(\varphi(at'^n)).$$

(b) Für $d'_{log}\colon \mathcal{E}'^* \to \Omega_{\mathcal{E}'|K}$, $f \mapsto f^{-1}\frac{df}{dt'} \cdot dt'$ gilt $d'_{log|_{\mathcal{E}^*}} = d_{log}$, denn für $f(t) \in \mathcal{E}^*$ ist

$$d'_{log}(f) = f^{-1}\frac{df(t)}{dt'} \cdot dt' = f^{-1}\frac{df(t)}{dt}\frac{dt}{dt'} \cdot dt' = f^{-1}\frac{df}{dt} \cdot dt = d_{log}(f).$$

Wir schreiben daher auch einfach d_{log} anstatt d'_{log}.

(c) Für $f, g \in \mathcal{E}'^*$ gilt $d_{log}(fg) = d_{log}(f) + d_{log}(g)$, denn

$$\begin{aligned} d_{log}(fg) &= (fg)^{-1}\frac{d}{dt'}(fg) \cdot dt' = (fg)^{-1}(g\frac{df}{dt'} + f\frac{dg}{dt'}) \cdot dt' = f^{-1}\frac{df}{dt'} \cdot dt' + g^{-1}\frac{dg}{dt'} \cdot dt' \\ &= d_{log}(f) + d_{log}(g). \end{aligned}$$

(d) Für $\sigma \in G$ gilt $d_{log} \circ \sigma = \sigma \circ d_{log}$ als Abbildungen von $\mathcal{E}'^*$ nach $\Omega_{\mathcal{E}'|K}$, denn für

$f = \sum_{n\in\mathbb{Z}} a_n t'^n \in \mathcal{E}'^*$ ist

$$\begin{aligned}
\sigma(d_{log}(f)) &= \sigma\left(f^{-1}\frac{df}{dt'}\cdot dt'\right) = \sigma(f^{-1})\sigma\left(\frac{d}{dt'}\sum_{n\in\mathbb{Z}} a_n t'^n\right)\cdot d\sigma(t') \\
&= \sigma(f)^{-1}\left(\sum_{n\in\mathbb{Z}} a_n n\sigma(t')^{n-1}\right)\zeta^{\chi(\sigma)}\cdot dt' \\
&= \sigma(f)^{-1}\left(\sum_{n\in\mathbb{Z}} a_n n\zeta^{\chi(\sigma)}(\zeta^{\chi(\sigma)}(1+t')-1)^{n-1}\right)\cdot dt' \\
&= \sigma(f)^{-1}\left(\frac{d}{dt'}\sum_{n\in\mathbb{Z}} a_n(\zeta^{\chi(\sigma)}(1+t')-1)^n\right)\cdot dt' \\
&= \sigma(f)^{-1}\left(\frac{d}{dt'}\sum_{n\in\mathbb{Z}} a_n\sigma(t')^n\right)\cdot dt' \\
&= \sigma(f)^{-1}\frac{d\sigma(f)}{dt'}\cdot dt' = d_{log}(\sigma(f)).
\end{aligned}$$

(e) $N_{\mathcal{E}'[\zeta]|\mathcal{E}[\zeta]|_{\mathcal{E}'}} = N_{\mathcal{E}'|\mathcal{E}}$, denn $\{1,(1+t'),\ldots,(1+t')^{p-1}\}$ ist sowohl eine $\mathcal{E}[\zeta]$-Basis von $\mathcal{E}'[\zeta]$, als auch eine $\mathcal{E}$-Basis von $\mathcal{E}'$.

Damit folgt schließlich für alle $u \in E^*$:

$$\begin{aligned}
tr(\varphi^{-1}(d_{log}(Col(u)))) &= tr\left(\varphi^{-1}\left(Col(u)^{-1}\frac{dCol(u)}{dt}\cdot dt\right)\right) \\
&= tr\left(\varphi^{-1}(Col(u)^{-1})\varphi^{-1}\left(\frac{dCol(u)}{dt}\cdot dt\right)\right) \\
&\overset{(i)}{=} tr\left(\varphi^{-1}(Col(u)^{-1})\varphi^{-1}\left(\frac{dCol(u)}{dt}\right)\cdot dt'\right) \\
&\overset{(a)}{=} tr\left(\varphi^{-1}(Col(u))^{-1}\frac{d}{dt'}\varphi^{-1}(Col(u))\cdot dt'\right) \\
&= tr(d_{log}(\varphi^{-1}(Col(u)))) = \sum_{\sigma\in G}\sigma(d_{log}(\varphi^{-1}(Col(u)))) \\
&\overset{(d)}{=} \sum_{\sigma\in G} d_{log}(\sigma(\varphi^{-1}(Col(u)))) \overset{(c)}{=} d_{log}\left(\prod_{\sigma\in G}\sigma(\varphi^{-1}(Col(u)))\right) \\
&= d_{log}(N_{\mathcal{E}'[\zeta]|\mathcal{E}[\zeta]}(\varphi^{-1}(Col(u)))) \overset{(e)}{=} d_{log}(N_{\mathcal{E}'|\mathcal{E}}\circ\varphi^{-1}(Col(u))) \\
&= d_{log}(N_\varphi(Col(u))) = d_{log}(Col(u)).
\end{aligned}$$

□

Lemma 7.26. *(i) Für $\omega' \in \Omega_{\mathcal{E}'|K}$ gilt: $res_{\mathcal{E}'}(\omega') = res_{\mathcal{E}}(tr(\omega'))$.*

(ii) Für $\omega \in \Omega_{\mathcal{E}|K}$ gilt: $res_{\mathcal{E}'}(\omega) = p\cdot res_{\mathcal{E}}(\omega)$.

Beweis. Wir zeigen zuerst (ii) und schreiben dafür $\omega = (\sum_{n\in\mathbb{Z}} c_n t^n)\cdot d_{log}t = \omega_0 + c_0\cdot d_{log}t$ mit $\omega_0 := (\sum_{n\in\mathbb{Z}\setminus\{0\}} c_n t^n)\cdot d_{log}t$. Wir haben bereits im Beweis von Satz 7.13 gesehen, dass $res_{\mathcal{E}}(\omega_0) = 0$, denn ω_0 liegt im Abschluss des Bildes von $d\colon \mathcal{E} \to \Omega_{\mathcal{E}|K}$. Aufgrund des kommutativen Würfels 7.22 liegt $\omega_0 \in \Omega_{\mathcal{E}|K} \hookrightarrow \Omega_{\mathcal{E}'|K}$ auch im Abschluss des Bildes von $d\colon \mathcal{E}' \to \Omega_{\mathcal{E}'|K}$. Wegen der Stetigkeit von $res_{\mathcal{E}'}$ ist somit auch $res_{\mathcal{E}'}(\omega_0) = 0$. Aus der K-Linearität von $res_{\mathcal{E}}$ und $res_{\mathcal{E}'}$ folgt damit $res_{\mathcal{E}'}(\omega) = c_0 res_{\mathcal{E}'}(d_{log}t) = res_{\mathcal{E}'}(d_{log}t)\cdot res_{\mathcal{E}}(\omega)$ und es genügt dementsprechend $res_{\mathcal{E}'}(d_{log}t) = p$ zu zeigen.

Um das Residuum von $d_{log}t$ zu berechnen, versuchen wir zunächst $d_{log}t$ etwas umzuformen:

$$d_{log}t = t^{-1}\cdot dt = t^{-1}p(1+t')^{p-1}\cdot dt' = p((1+t')^p - 1)^{-1}(1+t')^{p-1}\cdot dt'.$$

Des Weiteren schreiben wir

$$t = (1+t')^p - 1 = \sum_{n=1}^{p}\binom{p}{n}t'^n = t'^p(1+p\alpha),$$

mit $\alpha = \frac{1}{p}\sum_{n=1}^{p-1}\binom{p}{n}t'^{n-p} \in \mathcal{O}_{\mathcal{E}'}$. Wie bereits zuvor gesehen ist dann $(1+p\alpha)^{-1} = \sum_{k\geq 0}(-1)^k(p\alpha)^k \in 1 + p\mathcal{O}_{\mathcal{E}'}$. Fassen wir nun alles zusammen, so erhalten wir

$$\begin{aligned} d_{log}t &= pt^{-1}(1+t')^{p-1}\cdot dt' = p(t')^{-p}(1+p\alpha)^{-1}(1+t')^{p-1}dt' \\ &= \underbrace{p\,(t')^{-p+1}\left(\sum_{k\geq 0}(-1)^k(p\alpha)^k\right)(1+t')^{p-1}}_{=:\sum_{r\in\mathbb{Z}} a_r t'^r}\cdot d_{log}t'. \end{aligned}$$

Wegen $\alpha = \frac{1}{p}\sum_{n=1}^{p-1}\binom{p}{n}t'^{n-p}$, $(1+t')^{p-1} = \sum_{n=0}^{p-1}\binom{p-1}{n}t'^n$ und der Definition der Multiplikation auf $\mathcal{O}_{\mathcal{E}'}$ ist dann aus Gradgründen $a_r = 0$ für alle $r \geq 1$ und $a_0 = \binom{p-1}{p-1} = 1$. Dementsprechend ist

$$res_{\mathcal{E}'}(d_{log}t) = res_{\mathcal{E}'}\left(p\left(\sum_{r\in\mathbb{Z}} a_r t'^r\right)\cdot d_{log}t'\right) = pa_0 = p.$$

Für (i) schreiben wir ebenfalls $\omega' = u' + c\cdot d_{log}t'$ mit $u' = (\sum_{n\in\mathbb{Z}\setminus\{0\}} a_n t'^n)\cdot d_{log}t'$ und $c = res_{\mathcal{E}'}(\omega')$. Wie bereits zuvor gesehen, liegt u' im Abschluss des Bildes von $d\colon \mathcal{E}' \to \Omega_{\mathcal{E}'|K}$, d.h. es existieren $u'_n \in \mathcal{E}'$ mit $\lim_{n\to\infty} d(u'_n) = u'$. Wegen der Stetigkeit von $res_{\mathcal{E}'}$ ist damit $res_{\mathcal{E}'}(u') = 0$. Außerdem ist wegen der G-Äquivarianz von $d\colon \mathcal{E}' \to \Omega_{\mathcal{E}'|K}$ auch

$$d\left(\sum_{\sigma\in G}\sigma(f)\right) = \sum_{\sigma\in G} d(\sigma(f)) = \sum_{\sigma\in G}\sigma(df) = tr(df)$$

für alle $f \in \mathcal{E}'$. Mittels der Stetigkeit von $tr\colon \Omega_{\mathcal{E}'|K} \to \Omega_{\mathcal{E}|K}$ nach Lemma 7.24 folgt dann

$$tr(u') = tr\left(\lim_{n\to\infty} d(u_n)\right) = \lim_{n\to\infty} tr(d(u_n)) = \lim_{n\to\infty} d\left(\sum_{\sigma\in G}\sigma(u_n)\right).$$

Im Beweis von Lemma 7.23 haben wir bereits gesehen, dass $\sum_{\sigma\in G}\sigma(u_n)$ ein Element von $\mathcal{E}$ ist. Also ist aufgrund des kommutativen Würfels 7.22 $tr(u')$ im Abschluss des Bildes von $d\colon\mathcal{E}\to\Omega_{\mathcal{E}|K}$. Wegen der Stetigkeit von $res_{\mathcal{E}}$ folgt damit schließlich $res_{\mathcal{E}}(tr(u'))=0$.

Als nächstes möchten wir uns kurz klar machen, dass t invariant unter N_φ ist. Werten wir nämlich das Polynom

$$X^p-1-t=\prod_{\sigma\in G}(X-\sigma(1+t'))$$

an der Stelle 1 aus, so erhalten wir

$$\begin{aligned}t&=-\prod_{\sigma\in G}(1-\sigma(1+t'))=-\prod_{\sigma\in G}-\sigma(t')=(-1)^{p+1}\prod_{\sigma\in G}\sigma(t')\\&=N_{\mathcal{E}'[\zeta]|\mathcal{E}[\zeta]}(t')=N_{\mathcal{E}'|\mathcal{E}}(\varphi^{-1}(t))=N_\varphi(t).\end{aligned}$$

Für $tr(d_{log}t')$ ergibt sich damit

$$tr(d_{log}t')=\sum_{\sigma\in G}\sigma(d_{log}t')=\sum_{\sigma\in G}d_{log}\sigma(t')=d_{log}\left(\prod_{\sigma\in G}\sigma(t')\right)=d_{log}(N_\varphi(t))=d_{log}t.$$

Also gilt aufgrund der K-Linearität von $res_{\mathcal{E}}$ schließlich

$$res_{\mathcal{E}}(tr(\omega'))=res_{\mathcal{E}}(tr(u'))+c\cdot res_{\mathcal{E}}(tr(d_{log}t'))=c\cdot res_{\mathcal{E}}(d_{log}t)=c=res_{\mathcal{E}'}(\omega').$$

□

Lemma 7.27. *Für $\omega\in\Omega_{\mathcal{E}|K}$ ist $res_{\mathcal{E}}(tr(\varphi^{-1}(\omega)))=\varphi^{-1}(res_{\mathcal{E}}(\omega))$.*

Beweis. Sei $\omega=f\cdot d_{log}t\in\Omega_{\mathcal{E}|K}$ mit $f=\sum_{n\in\mathbb{Z}}c_nt^n\in\mathcal{E}$. Aus Teil (a) im Beweis von Lemma 7.25 erhält man

$$\varphi^{-1}(\omega)=\varphi^{-1}(f)\cdot d_{log}\varphi^{-1}(t)=\varphi^{-1}(f)\cdot d_{log}t',$$

was wegen $\varphi^{-1}(f)=\sum_{n\in\mathbb{Z}}\varphi^{-1}(c_n)t'^n$ schließlich $res_{\mathcal{E}'}(\varphi^{-1}(\omega))=\varphi^{-1}(res_{\mathcal{E}}(\omega))$ liefert. Zusammen mit Lemma 7.26 folgt dann

$$res_{\mathcal{E}}(tr(\varphi^{-1}(\omega)))=res_{\mathcal{E}'}(\varphi^{-1}(\omega))=\varphi^{-1}(res_{\mathcal{E}}(\omega)).$$

□

Satz 7.28. *Für $x\in\mathcal{E}$, $u\in E^*$ und $m\geq 0$ gilt:*

$$res(\varphi^m(x)\cdot d_{log}(Col(u)))=\varphi^m(res(x\cdot d_{log}(Col(u)))),$$

wobei wir wie zuvor $res=res_{\mathcal{E}}$ schreiben, wenn der Grundkörper zweifelsfrei feststeht.

Beweis. Wir beweisen die Aussage per Induktion über $m \geq 0$, wobei der Fall $m = 0$ trivial ist. Für $m = 1$ betrachten wir zunächst die Gleichung

$$\begin{aligned}\varphi^{-1}(res(\varphi(x) \cdot d_{log}(Col(u))) &\overset{7.27}{=} res(tr(\varphi^{-1}(\varphi(x) \cdot d_{log}(Col(u))))) \\ &= res(tr(x \cdot \varphi^{-1}(d_{log}(Col(u))))) \\ &= res(x \cdot tr(\varphi^{-1}(d_{log}(Col(u))))) \\ &\overset{7.25}{=} res(x \cdot d_{log}(Col(u))).\end{aligned}$$

Wendet man nun φ auf die Gleichung an, so hat man den Fall $m = 1$ bewiesen. Wir nehmen also nun an, dass die Behauptung für ein $m \geq 0$ gilt. Dann folgt schließlich

$$\begin{aligned}\varphi^{m+1}(res(x \cdot d_{log}(Col(u)))) &= \varphi(\varphi^m(res(x \cdot d_{log}(Col(u))))) \\ &\overset{I.V.}{=} \varphi(res(\varphi^m(x) \cdot d_{log}(Col(u)))) \\ &= res(\varphi^{m+1}(x) \cdot d_{log}(Col(u))),\end{aligned}$$

wobei die letzte Gleichheit analog zum Fall $m = 1$ gezeigt wird. □

7.5 Der Gruppenisomorphismus $\bar{\delta}_{\mathcal{E}}$

Unser Ziel in diesem Abschnitt ist es, zunächst eine gewisse Abbildung $\delta_{\mathcal{E}}: \mathcal{O}_{\mathcal{E}} \to Hom^{cont.}(G_E, \mathbb{Z}_p)$ zu konstruieren. Wie wir später sehen werden, faktorisiert die von uns konstruierte Abbildung $\delta_{\mathcal{E}}$ sogar über einen Gruppenisomorphismus $\bar{\delta}_{\mathcal{E}}: \mathcal{O}_{\mathcal{E}}/(\varphi - 1)\mathcal{O}_{\mathcal{E}} \to Hom^{cont.}(G_E, \mathbb{Z}_p)$. Dabei seien die Bezeichnungen wieder wie zuvor:

- $E \cong k((t))$ ein vollständiger, diskret bewerteter Körper der Charakteristik p mit perfektem Restklassenkörper k;
- $G_E := Gal(E^{sep}|E) \cong Gal(\mathcal{E}^{nr}|\mathcal{E})$;
- $Rep^{cont.}_{\mathbb{Z}_p}(G_E)$ = Kategorie der stetigen, $\mathbb{Z}_p$-linearen G_E-Darstellungen auf endlich erzeugten $\mathbb{Z}_p$-Moduln;
- $\Phi^{\acute{e}t}_{\mathcal{O}_{\mathcal{E}}}$ = Kategorie der etalen φ-Moduln M über $\mathcal{O}_{\mathcal{E}}$;
- $Hom^{cont.}(G_E, \mathbb{Z}_p)$ = Gruppe der stetigen Charaktere, d.h. stetigen Gruppenhomomorphismen $\chi: G_E \to \mathbb{Z}_p$. Die Gruppenoperation ist dabei die punktweise Addition der Charaktere. Aufgrund der Kommutativität von $\mathbb{Z}_p$ ist dadurch auch $Hom^{cont.}(G_E, \mathbb{Z}_p)$ eine abelsche Gruppe.

Für einen stetigen Charakter $\chi \in Hom^{cont.}(G_E, \mathbb{Z}_p)$ konstruieren wir eine stetige $\mathbb{Z}_p$-Darstellung wie folgt:

- $V_\chi := {\mathbb{Z}_p}^2 = \mathbb{Z}_p e_1 \oplus \mathbb{Z}_p e_2$ als unterliegender $\mathbb{Z}_p$-Modul;
- $G_E \times V_\chi \to V_\chi$, $(\sigma, \alpha e_1 + \beta e_2) \mapsto (\alpha + \chi(\sigma)\beta)e_1 + \beta e_2$.

Diese Abbildung definiert aufgrund der Homomorphieeigenschaft von χ eine Gruppenoperation von G_E auf V_χ. Diese Gruppenoperation ist auch noch stetig, da χ stetig ist und $\mathbb{Z}_p$ ein topologischer Ring ist. Dadurch haben wir mit V_χ eine stetige, $\mathbb{Z}_p$-lineare G_E-Darstellung konstruiert, deren unterliegender $\mathbb{Z}_p$-Modul frei vom Rang 2 ist.

Für $\chi, \chi' \in Hom^{cont.}(G_E, \mathbb{Z}_p)$ schreiben wir $V_\chi \sim V_{\chi'}$, falls ein $r \in \mathbb{Z}_p$ existiert, sodass $\psi_r \colon V_\chi \to V_{\chi'}$, $\alpha e_1 + \beta e_2 \mapsto (\alpha + r\beta)e_1 + \beta e_2$ ein Isomorphismus in $Rep^{cont.}_{\mathbb{Z}_p}(G_E)$ ist. Man sieht dabei sofort, dass $\sim$ eine Äquivalenzrelation auf den durch $\chi \in Hom^{cont.}(G_E, \mathbb{Z}_p)$ definierten Darstellungen bildet. Betrachtet man nun $\mathbb{Z}_p \in Rep^{cont.}_{\mathbb{Z}_p}(G_E)$ als freien $\mathbb{Z}_p$-Modul vom Rang 1 mit der trivialen G_E-Operation, so existiert eine exakte Sequenz

$$0 \longrightarrow \mathbb{Z}_p \xrightarrow{\alpha \mapsto \alpha e_1} V_\chi \xrightarrow{\alpha e_1 + \beta e_2 \mapsto \beta} \mathbb{Z}_p \longrightarrow 0$$

in $Rep^{cont.}_{\mathbb{Z}_p}(G_E)$. Daher bezeichnet man V_χ auch als die durch χ bestimmte Erweiterung von $\mathbb{Z}_p$ und $\mathbb{Z}_p$.

Lemma 7.29. *(i) Ist $V \in Rep^{cont.}_{\mathbb{Z}_p}(G_E)$ und sitzt V in einer exakten Sequenz $0 \to \mathbb{Z}_p \xrightarrow{f} V \xrightarrow{g} \mathbb{Z}_p \to 0$ in $Rep^{cont.}_{\mathbb{Z}_p}(G_E)$, so gilt:*

(a) V ist frei vom Rang 2 über $\mathbb{Z}_p$; ist $e_2 \in V$ mit $g(e_2) = 1$ und $e_1 := f(1)$, so ist e_1, e_2 eine $\mathbb{Z}_p$-Basis von V.

(b) Für alle $\sigma \in G$ existiert genau ein $\alpha(\sigma) \in \mathbb{Z}_p$ mit $\sigma \cdot e_2 = \alpha(\sigma)e_1 + e_2$; die Abbildung $\alpha \colon G_E \to \mathbb{Z}_p$, $\sigma \mapsto \alpha(\sigma)$ ist ein dabei ein stetiger Charakter.

(c) Es gilt $V = V_\alpha$ in $Rep^{cont.}_{\mathbb{Z}_p}(G_E)$.

(ii) Sind $\chi, \chi' \in Hom^{cont.}(G_E, \mathbb{Z}_p)$, sodass $V_\chi \sim V_{\chi'}$ in $Rep^{cont.}_{\mathbb{Z}_p}(G_E)$, so gilt bereits $\chi = \chi'$.

Beweis. (a) ist klar, da 1 ein Erzeuger von $\mathbb{Z}_p$ ist und die Sequenz $0 \to \mathbb{Z}_p \xrightarrow{f} V \xrightarrow{g} \mathbb{Z}_p \to 0$ exakt ist. Für (b) wählen wir ein beliebiges $\sigma \in G$. Da G_E trivial auf $\mathbb{Z}_p$ operiert, ist $g(\sigma \cdot e_2) = \sigma \cdot g(e_2) = g(e_2)$. Also liegt $\sigma \cdot e_2 - e_2$ in $\ker(g) = \mathrm{im}(f)$. Aufgrund der Injektivität von f existiert genau ein $\alpha(\sigma) \in \mathbb{Z}_p$ mit $f(\alpha(\sigma)) = \sigma \cdot e_2 - e_2$. Damit erhalten wir

$$\sigma \cdot e_2 = f(\alpha(\sigma)) + e_2 = \alpha(\sigma) f(1) + e_2 = \alpha(\sigma)e_1 + e_2.$$

Seien nun $\sigma, \tau \in G$. Dann gilt wegen der trivialen Operation von G_E auf $\mathbb{Z}_p$:

$$\begin{aligned}(\tau \circ \sigma) \cdot e_2 &= \tau \cdot (\sigma \cdot e_2) = \tau(\alpha(\sigma)e_1 + e_2) = \alpha(\sigma)\tau \cdot e_1 + \tau e_2 \\ &= \alpha(\sigma)\tau \cdot f(1) + \alpha(\tau)e_1 + e_2 = \alpha(\sigma) f(\tau \cdot 1) + \alpha(\tau)e_1 + e_2 \\ &= (\alpha(\tau) + \alpha(\sigma))e_1 + e_2.\end{aligned}$$

Durch die Eindeutigkeit von $\alpha(\tau \circ \sigma)$ ist damit schließlich $\alpha(\tau \circ \sigma) = \alpha(\tau) + \alpha(\sigma)$, d.h. $\alpha \in Hom(G_E, \mathbb{Z}_p)$.

Wir bezeichnen mit $\rho: G_E \times V \to V$ die Gruppenoperation von G_E auf V, welche nach unseren Voraussetzungen stetig ist. Wir wollen nun zeigen, dass dann auch $\alpha: G_E \to \mathbb{Z}_p$ stetig ist. Sei dafür $U \subset \mathbb{Z}_p$ offen und $\sigma \in \alpha^{-1}(U)$. Dann ist aber auch $U_V := Ue_1 + \mathbb{Z}_p e_2 \subset V$ offen in V mit $\sigma \cdot e_2 = \alpha(\sigma)e_1 + e_2 \in U_V$. Damit ist (σ, e_2) ein Element der offenen Untermenge $\rho^{-1}(U_V)$ von $G_E \times V$. Es existieren also offene Untermengen $H_\sigma \subset G_E$ und $W_\sigma \subset V$ mit $(\sigma, e_2) \in H_\sigma \times W_\sigma \subset \rho^{-1}(U_V)$. Damit ist aber insbesondere

$$\tau \cdot e_2 = \alpha(\tau)e_1 + e_2 \in U_V = Ue_1 + \mathbb{Z}_p e_2 \text{ für alle } \tau \in H_\sigma,$$

d.h. $\alpha(\tau) \in U$ für alle $\tau \in H_\sigma$. Auf diese Weise lässt sich dann

$$\alpha^{-1}(U) = \bigcup_{\sigma \in \alpha^{-1}(U)} H_\sigma$$

als Vereinigung offener Mengen schreiben und ist somit selbst offen. Also handelt es sich bei α sogar um einen stetigen Charakter, d.h. $\alpha \in Hom^{cont.}(G_E, \mathbb{Z}_p)$.

Damit wir V als V_α auffassen können, müssen wir zeigen, dass α unabhängig von der Wahl von $e_2 \in V$ mit $g(e_2) = 1$ ist. Sei also auch $e_2' \in V$ mit der Eigenschaft $g(e_2') = 1 = g(e_2)$. Damit liegt $e_2' - e_2$ in $\ker(g) = \mathrm{im}(f)$ und es existiert ein $z \in \mathbb{Z}_p$ mit $e_2' - e_2 = f(z) = zf(1) = ze_1$. Damit gilt aber auch für e_2' ebenfalls

$$\sigma \cdot e_2' = \sigma \cdot (ze_1 + e_2) = (z + \alpha(\sigma))e_1 + e_2 = \alpha(\sigma)e_1 + (ze_1 + e_2) = \alpha(\sigma)e_1 + e_2',$$

d.h. $V = V_\alpha$.

Für (ii) seien $\chi, \chi' \in Hom^{cont.}(G_E, \mathbb{Z}_p)$ mit $V_\chi \sim V_{\chi'}$ und $\psi_r: V_\chi \to V_{\chi'}$ der zugehörige Isomorphismus. Ist nun $\sigma \in G$, so gilt einerseits

$$\psi(\sigma \cdot e_2) = \psi(\chi(\sigma)e_1 + e_2) = (\chi(\sigma) + r)e_1 + e_2$$

und andererseits

$$\psi(\sigma \cdot e_2) = \sigma \cdot \psi(e_2) = \sigma \cdot (re_1 + e_2) = (r + \chi'(\sigma))e_1 + e_2.$$

Daraus folgt schließlich $\chi(\sigma) = \chi'(\sigma)$, was aufgrund der beliebigen Wahl von $\sigma \in G$ zu $\chi = \chi'$ führt. □

Auf quasi umgekehrte Weise konstruieren wir für ein Element $a \in \mathcal{O}_\mathcal{E}$ einen etalen φ-Modul $(D_a, g_a) \in \Phi^{\acute{e}t}_{\mathcal{O}_\mathcal{E}}$ wie folgt:

- $D_a := \mathcal{O}_\mathcal{E}{}^2 = \mathcal{O}_\mathcal{E} e_1 \oplus \mathcal{O}_\mathcal{E} e_2$ als unterliegender $\mathcal{O}_\mathcal{E}$-Modul;
- $g_a : D_a \to D_a$, $\alpha e_1 + \beta e_2 \mapsto (\varphi(\alpha) + \varphi(\beta)a)e_1 + \varphi(\beta)e_2$.

Damit ist (D_a, g_a) offensichtlich ein φ-Modul und nach Lemma 6.4 auch etal, denn die darstellende Matrix von g_a bzgl. der Basis (e_1, e_2) ist $\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \in GL_2(\mathcal{O}_\mathcal{E})$.

Für $a, b \in \mathcal{O}_\mathcal{E}$ schreiben wir $D_a \sim D_b$, falls ein $r \in \mathcal{O}_\mathcal{E}$ existiert, sodass $\psi_r : D_a \to D_b$, $\alpha e_1 + \beta e_2 \mapsto (\alpha + r\beta)e_1 + \beta e_2$, ein Isomorphismus ist. Man sieht dabei wieder sofort, dass $\sim$ eine Äquivalenzrelation auf den durch $a \in \mathcal{O}_\mathcal{E}$ definierten etalen φ-Moduln bildet. Bezeichnet man mit $\mathcal{O}_\mathcal{E} := (\mathcal{O}_\mathcal{E}, \varphi) \in \Phi^{ét}_{\mathcal{O}_\mathcal{E}}$ den trivialen φ-Modul über $\mathcal{O}_\mathcal{E}$, so gibt es in $\Phi^{ét}_{\mathcal{O}_\mathcal{E}}$ die kurze exakte Sequenz

$$0 \longrightarrow \mathcal{O}_\mathcal{E} \xrightarrow{\alpha \mapsto \alpha e_1} D_a \xrightarrow{\alpha e_1 + \beta e_2 \mapsto \beta} \mathcal{O}_\mathcal{E} \longrightarrow 0.$$

Lemma 7.30. *(i) Ist $D = (D, g) \in \Phi^{ét}_{\mathcal{O}_\mathcal{E}}$ und sitzt D in einer kurzen exakten Sequenz $0 \to \mathcal{O}_\mathcal{E} \xrightarrow{F} D \xrightarrow{G} \mathcal{O}_\mathcal{E} \to 0$ in $\Phi^{ét}_{\mathcal{O}_\mathcal{E}}$, so gilt:*

(a) D ist frei vom Rang 2 über $\mathcal{O}_\mathcal{E}$; ist nämlich $e_2 \in D$ mit $G(e_2) = 1$ und $e_1 := F(1)$, so ist (e_1, e_2) eine $\mathcal{O}_\mathcal{E}$-Basis von D.

(b) Es existiert genau ein $a \in \mathcal{O}_\mathcal{E}$ mit $g(e_2) = ae_1 + e_2$.

(c) Es gilt $D = D_a$.

(ii) Sind $a, b \in \mathcal{O}_\mathcal{E}$, so gilt:

$$D_a \sim D_b \Leftrightarrow a - b \in (\varphi - 1)\mathcal{O}_\mathcal{E} = \{\varphi(\alpha) - \alpha \mid \alpha \in \mathcal{O}_\mathcal{E}\}.$$

Beweis. (a) ist wieder klar, da 1 ein Erzeuger von $\mathcal{O}_\mathcal{E}$ ist und $0 \to \mathcal{O}_\mathcal{E} \xrightarrow{F} D \xrightarrow{G} \mathcal{O}_\mathcal{E} \to 0$ eine kurze exakte Sequenz ist. Für (b) betrachten wir $G(g(e_2)) = G \circ g(e_2) = \varphi \circ G(e_2) = \varphi(1) = 1 = G(e_2)$. Daher liegt $g(e_2) - e_2$ in $\ker(G) = \mathrm{im}(F)$. Aufgrund der Injektivität von F existiert genau ein $a \in \mathcal{O}_\mathcal{E}$ mit

$$g(e_2) = F(a) + e_2 = aF(1) + e_2 = ae_1 + e_2.$$

Damit wir D als D_a auffassen können, müssen wir ähnlich wie zuvor zeigen, dass a unabhängig von der Wahl von $e_2 \in D$ mit $G(e_2) = 1$ ist. Sei also $e_2' \in D$ mit $G(e_2') = 1 = G(e_2)$, d.h. $e_2' - e_2$ liegt in $\ker(G) = \mathrm{im}(F)$. Somit existiert ein $\alpha \in \mathcal{O}_\mathcal{E}$ mit $e_2' - e_2 = F(\alpha) = \alpha F(1) = \alpha e_1$. Daher gilt auch für e_2':

$$\sigma \cdot e_2' = \sigma(\alpha e_1 + e_2) = (\alpha + a)e_1 + e_2 = ae_1 + (\alpha e_1 + e_2) = ae_1 + e_2'.$$

Also ist $a \in \mathcal{O}_\mathcal{E}$ unabhängig von der Wahl von $e_2 \in D$ mit $G(e_2) = 1$ und somit $D = D_a$.

Für (ii) zeigen wir zuerst die Hinrichtung und nehmen an, dass $D_a \sim D_b$ gilt. Bezeichnen wir mit $\psi_r: D_a \to D_b$ den zugehörigen Isomorphismus, so gilt einerseits

$$g_b \circ \psi_r(e_2) = g_b(re_1 + e_2) = (\varphi(r) + b)e_1 + e_2$$

und andererseits

$$g_b \circ \psi_r(e_2) = \psi_r \circ g_a(e_2) = \psi_r(ae_1 + e_2) = (a + r)e_1 + e_2.$$

Daraus erhält man schließlich $a - b = \varphi(r) - r = (\varphi - 1)(r) \in (\varphi - 1)\mathcal{O}_\mathcal{E}$.

Für die Rückrichtung sei $r \in \mathcal{O}_\mathcal{E}$ mit $(\varphi - 1)(r) = a - b$ und setze $\psi_r: D_a \to D_b$, $(\alpha e_1 + \beta e_2) \mapsto (\alpha + r\beta)e_1 + \beta e_2$. Damit ist ψ_r offensichtlich ein Isomorphismus von $\mathcal{O}_\mathcal{E}$-Moduln. Außerdem gilt

$$\begin{aligned}
\psi_r \circ g_a(\alpha e_1 + \beta e_2) &= \psi_r((\varphi(\alpha) + a\varphi(\beta))e_1 + \varphi(\beta)e_2) \\
&= (\varphi(\alpha) + a\varphi(\beta) + r\varphi(\beta))e_1 + \varphi(\beta)e_2 \\
&= (\varphi(\alpha) + b\varphi(\beta) + \varphi(r)\varphi(\beta))e_1 + \varphi(\beta)e_2 \\
&= (\varphi(\alpha + r\beta) + b\varphi(\beta))e_1 + \varphi(\beta)e_2 \\
&= g_b((\alpha + r\beta)e_1 + \beta e_2) \\
&= g_b \circ \psi_r(\alpha e_1 + \beta e_2).
\end{aligned}$$

Also ist ψ_r sogar ein Isomorphismus von etalen φ-Moduln und damit $D_a \sim D_b$. □

Wie bereits in Kaptitel 6, Satz 6.8, gesehen, sind $\mathbb{D}: Rep^{cont.}_{\mathbb{Z}_p}(G_E) \to \Phi^{\acute{e}t}_{\mathcal{O}_\mathcal{E}}$ und $\mathbb{V}: \Phi^{\acute{e}t}_{\mathcal{O}_\mathcal{E}} \to Rep^{cont.}_{\mathbb{Z}_p}(G_E)$ zueinander inverse, exakte Äquivalenzen von Kategorien mit

$$\begin{aligned}
\mathcal{O}_\mathcal{E} = (\mathcal{O}_{\breve{\mathcal{E}}})^{G_E} \cong (\mathcal{O}_{\breve{\mathcal{E}}} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p)^{G_E} &= \mathbb{D}(\mathbb{Z}_p) \\
\alpha &\mapsto \alpha \otimes 1 \\
\varphi &\leftrightarrow \varphi \otimes id
\end{aligned}$$

und

$$\begin{aligned}
\mathbb{Z}_p = (\mathcal{O}_{\breve{\mathcal{E}}})^{\varphi=1} \cong (\mathcal{O}_{\breve{\mathcal{E}}} \otimes_{\mathcal{O}_\mathcal{E}} \mathcal{O}_\mathcal{E})^{\varphi=1} &= \mathbb{V}(\mathcal{O}_\mathcal{E}). \\
\alpha &\mapsto \alpha \otimes 1 \\
\sigma &\leftrightarrow \sigma \otimes id
\end{aligned}$$

Für ein $a \in \mathcal{O}_\mathcal{E}$ sei (D_a, g_a) der zuvor konstruierte etale φ-Modul. Dieser sitzt in der exakten Sequenz $0 \to \mathcal{O}_\mathcal{E} \to D_a \to \mathcal{O}_\mathcal{E} \to 0$. Aufgrund der Exaktheit von $\mathbb{V}$ und der obigen Identifikation erhalten wir die kurze exakte Sequenz $0 \to \mathbb{Z}_p \to \mathbb{V}(D_a) \to \mathbb{Z}_p \to$

0. Nach Lemma 7.29 existiert genau $\chi_a \in Hom^{cont.}(G_E, \mathbb{Z}_p)$ mit $\mathbb{V}(D_a) = V_{\chi_a}$. Da χ_a eindeutig ist, können wir die wohldefinierte Abbildung

$$\delta_{\mathcal{E}}: \mathcal{O}_{\mathcal{E}} \to Hom^{cont.}(G_E, \mathbb{Z}_p),\ a \mapsto \chi_a,$$

definieren.

Ist auf der anderen Seite $\chi \in Hom^{cont.}(G_E, \mathbb{Z}_p)$ und $V_\chi \in Rep^{cont.}_{\mathbb{Z}_p}(G_E)$ die zuvor konstruierte stetige $\mathbb{Z}_p$-Darstellung über G_E, so sitzt diese in der kurzen exakten Sequenz $0 \to \mathbb{Z}_p \to V_\chi \to \mathbb{Z}_p \to 0$. Aufgrund der vorherigen Identifikation von $\mathbb{D}(\mathbb{Z}_p) = \mathcal{O}_{\mathcal{E}}$ und der Exaktheit von $\mathbb{D}$ erhalten wir die kurze exakte Sequenz $0 \to \mathcal{O}_{\mathcal{E}} \to \mathbb{D}(V_\chi) \to \mathcal{O}_{\mathcal{E}} \to \mathcal{O}_{\mathcal{E}} \to 0$. Nach Lemma 7.30 existiert auch hier genau ein $a_\chi \in \mathcal{O}_{\mathcal{E}}$ mit $\mathbb{D}(V_\chi) = D_{a_\chi}$.

Unser nächstes Ziel ist es nun herauszufinden, dass $\delta_{\mathcal{E}}$ sogar durch $(\varphi - 1)\mathcal{O}_{\mathcal{E}}$ faktorisiert. Dafür müssen wir uns aber zunächst noch etwas genauer mit $(\varphi - 1)$ und den von uns konstruierten $\mathbb{Z}_p$-Darstellungen und etalen φ-Moduln beschäftigen.

Lemma 7.31. *Die $\mathbb{Z}_p$-lineare Abbildung $(\varphi - 1): \mathcal{O}_{\breve{\mathcal{E}}} \to \mathcal{O}_{\breve{\mathcal{E}}}$ ist surjektiv. Insbesondere existiert für alle $a \in \mathcal{O}_{\mathcal{E}}$ ein $\alpha \in \mathcal{O}_{\breve{\mathcal{E}}}$ mit $(\varphi - 1)(\alpha) = -a$.*

Beweis. Da $(\varphi - 1)$ $\mathbb{Z}_p$-linear ist, können wir die Reduktion modulo p betrachten, d.h. $(\varphi - 1): E^{sep} \to E^{sep}$, $x \mapsto x^p - x$. Sei nun $a \in \mathcal{O}_{\mathcal{E}}$, $\bar{a} := a + p\mathcal{O}_{\mathcal{E}} \in E^{sep}$ und $f(X) := X^p - X - \bar{a} \in E^{sep}[X]$. Wegen $\frac{d}{dX} f(X) = -1$ ist f separabel und damit existiert eine Nullstelle $\bar{\alpha}_0 \in E^{sep}$ von f. Sei $\alpha_0 \in \mathcal{O}_{\breve{\mathcal{E}}}$ sodass $\alpha_0 \mod p\mathcal{O}_{\breve{\mathcal{E}}} = \bar{\alpha}_0$. Also ist $a \mod p = \bar{a} = (\varphi - 1)(\bar{\alpha}_0) = (\varphi - 1)(\alpha_0) \mod p$, d.h.. es existiert ein $a_1 \in \mathcal{O}_{\mathcal{E}}$ mit $a = (\varphi - 1)(\alpha_0) + pa_1$. Induktiv erhalten wir dadurch $\alpha_n, a_n \in \mathcal{O}_{\breve{\mathcal{E}}}$ mit

$$a = \sum_{i=0}^{n} p^i (\varphi - 1)(\alpha_i) + p^{n+1} a_{n+1} = (\varphi - 1)\left(\sum_{i=0}^{n} p^i \alpha_i\right) + p^{n+1} a_{n+1}.$$

Da $\mathcal{O}_{\breve{\mathcal{E}}}$ vollständig ist, konvergiert $\alpha := \sum_{i=0}^{\infty} p^i \alpha_i$ in $\mathcal{O}_{\breve{\mathcal{E}}}$ und zusammen mit der Stetigkeit von $(\varphi - 1)$ folgt schließlich $(\varphi - 1)(\alpha) = a$. □

Lemma 7.32. *Sei $a \in \mathcal{O}_{\mathcal{E}}$ und $\alpha \in \mathcal{O}_{\breve{\mathcal{E}}}$ mit $(\varphi - 1)(\alpha) = -a$ wie in Lemma 7.31. Dann ist $\chi_\alpha: G_E \to \mathbb{Z}_p$, $\sigma \mapsto (\sigma - 1)(\alpha)$ ein wohldefinierter, stetiger Gruppenhomomorphismus, welcher nur von der Restklasse $a + (\varphi - 1)\mathcal{O}_{\mathcal{E}} \in \mathcal{O}_{\mathcal{E}}/(\varphi - 1)\mathcal{O}_{\mathcal{E}}$ abhängt.*

Beweis. Zunächst einmal müssen wir die Wohldefiniertheit von χ_α zeigen, d.h. $(\sigma - 1)(\alpha) \in \mathbb{Z}_p$ für alle $\sigma \in G_E$ und die Unabhängigkeit von der Wahl eines $\alpha \in \mathcal{O}_{\breve{\mathcal{E}}}$. Man erinnere sich daran, dass φ mit jedem $\sigma \in G_E$ kommutiert und betrachte die Gleichung

$$\begin{aligned}
\varphi((\sigma - 1)(\alpha)) &= \varphi(\sigma(\alpha) - \alpha) = \varphi(\sigma(\alpha)) - \varphi(\alpha) \\
&= \sigma(\varphi(\alpha)) - \sigma(\alpha) + \sigma(\alpha) - \varphi(\alpha) \\
&= \sigma(\varphi(\alpha) - \alpha) + \sigma(\alpha) - \varphi(\alpha) = \sigma(-a) + \sigma(\alpha) - \varphi(\alpha) \\
&= -a + \sigma(\alpha) - \varphi(\alpha) = \varphi(\alpha) - \alpha + \sigma(\alpha) - \varphi(\alpha) \\
&= (\sigma - 1)(\alpha).
\end{aligned}$$

Also liegt das Bild von χ_α in $\mathbb{Z}_p$, denn für jedes $\sigma \in G_E$ ist $\chi_\alpha(\sigma) = (\sigma - 1)(\alpha) \in (\mathcal{O}_{\breve{\mathcal{E}}})^{\varphi=1} = \mathbb{Z}_p$ nach Lemma 6.5. Sei nun $\beta \in \mathcal{O}_{\breve{\mathcal{E}}}$ mit $(\varphi - 1)(\beta) = -a = (\varphi - 1)(\alpha)$, d.h. $\alpha - \beta \in (\mathcal{O}_{\breve{\mathcal{E}}})^{\varphi=1} = \mathbb{Z}_p$. Wegen $\mathbb{Z}_p \subset \mathcal{O}_\mathcal{E}$ und $\sigma_{|\mathcal{O}_\mathcal{E}} = id_{\mathcal{O}_\mathcal{E}}$ für alle $\sigma \in G_E$ ist dann aber

$$\chi_\alpha(\sigma) = (\sigma - 1)(\alpha) = \underbrace{(\sigma - 1)(\alpha - \beta)}_{=0} + (\sigma - 1)(\beta) = \chi_\beta(\sigma).$$

Also hängt χ_α nur von $a \in \mathcal{O}_\mathcal{E}$ ab und ist somit wohldefiniert. Die Homomorphieeigenschaft von χ_α ist recht leicht zu sehen, denn für $\chi, \tau \in G_E$ gilt

$$\begin{aligned}(\sigma \circ \tau - 1)(\alpha) &= \sigma \circ \tau(\alpha) - \alpha = \sigma \circ \tau(\alpha) - \sigma(\alpha) + \sigma(\alpha) - \alpha \\ &= \sigma(\underbrace{(\tau - 1)(\alpha)}_{\in \mathbb{Z}_p \subset \mathcal{O}_\mathcal{E}}) + (\sigma - 1)(\alpha) = (\tau - 1)(\alpha) + (\sigma - 1)(\alpha).\end{aligned}$$

Für die Stetigkeit von χ_α zeigen wir zunächst, dass die Abbildung $\psi_n \colon G_E \xrightarrow{\chi_\alpha} \mathbb{Z}_p \xrightarrow{can} \mathbb{Z}_p/p^n\mathbb{Z}_p$ für alle $n \geq 1$ einen offenen Kern hat. Sei dafür $\sigma \in \ker(\psi_n)$, d.h. $(\sigma - 1)(\alpha) = \sigma(\alpha) - \alpha \in p^n\mathbb{Z}_p$. Da $\mathcal{O}_{\breve{\mathcal{E}}}$ die Vervollständigung von $\mathcal{O}_{\mathcal{E}^{nr}}$ ist, existiert ein $\alpha' \in \mathcal{O}_{\mathcal{E}^{nr}}$ mit $\alpha - \alpha' = p^n\beta$ für ein $\beta \in \mathcal{O}_{\breve{\mathcal{E}}}$. Für $\tau \in H_\sigma := Gal(\mathcal{E}^{nr}|\mathcal{E}[\alpha']) \leq Gal(\mathcal{E}^{nr}|\mathcal{E}) \cong G_E$ gilt dann

$$\begin{aligned}(\sigma \circ \tau - 1)(\alpha) &= (\sigma - 1)(\alpha) + (\tau - 1)(\alpha) = (\sigma - 1)(\alpha) + (\tau - 1)(\alpha - \alpha') + \underbrace{(\tau - 1)(\alpha')}_{=0, \text{ da } \tau \in H_\sigma} \\ &= (\sigma - 1)(\alpha) + (\tau - 1)(\alpha - \alpha') = (\sigma - 1)(\alpha) + p^n(\tau - 1)(\beta) \\ &\equiv 0 \mod p^n,\end{aligned}$$

da $\sigma \in \ker(\psi_n)$. Nach dem Hauptsatz der Galoistheorie ist $H_\sigma \leq G_E$ offen und damit auch $\ker(\psi_n)$, denn $\ker(\psi_n) = \bigcup_{\sigma \in \ker(\psi_n)} \sigma H_\sigma$.

Sei nun $U \subset \mathbb{Z}_p$ offen und $\sigma \in \chi_\alpha^{-1}(U)$. Damit existiert ein $n \geq 1$ mit $\chi_\alpha(\sigma) + p^n\mathbb{Z}_p \subset U$. Da $\ker(\psi_n)$ eine offene Umgebung von 1_{G_E} ist, ist $\sigma \cdot \ker(\psi_n)$ eine offene Umgebung von σ. Des Weiteren gilt

$$\chi_\alpha(\sigma \cdot \ker(\psi_n)) = \chi_\alpha(\sigma) + \chi_\alpha(\ker(\psi_n)) \subset \chi_\alpha(\sigma) + p^n\mathbb{Z}_p \subset U.$$

Also handelt es sich bei $\chi_\alpha^{-1}(U)$ um eine offene Menge und damit bei χ_α um einen stetigen Gruppenhomomorphismus.

Damit bleibt nur noch zu zeigen, dass χ_α nur von der Restklasse $a + (\varphi - 1)\mathcal{O}_\mathcal{E}$ abhängt. Sei dafür $b \in \mathcal{O}_\mathcal{E}$ mit $a - b \in (\varphi - 1)\mathcal{O}_\mathcal{E}$, d.h. $a - b = \varphi(c)$ für ein $c \in \mathcal{O}_\mathcal{E}$. Ist zudem $\beta \in \mathcal{O}_{\breve{\mathcal{E}}}$ mit $(\varphi - 1)(\beta) = -b$, so gilt

$$(\varphi - 1)(\beta) = -b = -a + a - b = (\varphi - 1)(\alpha) + (\varphi - 1)(c) = (\varphi - 1)(\alpha + c).$$

Wie zuvor gesehen ist dann

$$\chi_\beta(\sigma) = \chi_{\alpha+c}(\sigma) = (\sigma-1)(\alpha+c) = \chi_\alpha(\sigma) + (\sigma-1)(c) \overset{c\in\mathcal{O}_\mathcal{E}}{=} \chi_\alpha(\sigma).$$

Also ist $\chi_\beta = \chi_\alpha$ und damit hängt χ_α nur von der Restklasse $a + (\varphi-1)\mathcal{O}_\mathcal{E}$ ab. □

Lemma 7.33. *(i) Sind $a, b \in \mathcal{O}_\mathcal{E}$ mit $D_a \sim D_b$, so ist auch $\mathbb{V}(D_a) = V_{\chi_a} \sim V_{\chi_b} = \mathbb{V}(D_b)$.*

(ii) Sind $\chi, \chi' \in Hom^{cont.}(G_E, \mathbb{Z}_p)$ mit $V_\chi \sim V_{\chi'}$, so ist auch $\mathbb{D}(V_\chi) = D_{a_\chi} \sim D_{a_{\chi'}} = \mathbb{D}(V_{\chi'})$.

Beweis. (ii) sieht man recht leicht, da aus $V_\chi \sim V_{\chi'}$ mittels Lemma 7.29 (ii) sofort $\chi = \chi'$ und damit $a_\chi = a_{\chi'}$ folgt. Es seien nun (e_1, e_2) eine Basis von D_{a_χ} und (e_1', e_2') eine Basis von $D_{a'_\chi}$ wie in Lemma 7.30. In dem Beweis von Lemma 7.30 haben wir jedoch auch gesehen, dass dann $e_1 = e_1'$ und $e_2 = re_1 + e_2'$ für ein $r \in \mathcal{O}_\mathcal{E}$ gelten muss. Wegen $\chi = \chi'$ ist dann

$$\psi_r : D_{a_\chi} \to D_{a_{\chi'}},\ \alpha e_1 + \beta e_2 \mapsto \alpha e_1 + \beta e_2 = (\alpha + r\beta)e_1' + \beta e_2'$$

ein Isomorphismus und es gilt damit $\mathbb{D}(V_\chi) = D_{a_\chi} \sim D_{a_{\chi'}} = \mathbb{D}(V_\chi)$.

Für (i) seien $a, b \in \mathcal{O}_\mathcal{E}$ mit $D_a \sim D_b$. Es existiert also ein $r \in \mathcal{O}_\mathcal{E}$, sodass $\psi_r : D_a \to D_b$, $(xe_1 + ye_2) \mapsto (x + ry)e_1 + ye_2$ ein Isomorphismus ist. Aus dem Beweis von Lemma 7.30 ergibt sich, dass dann $a - b = (\varphi-1)(r)$ gilt. Nach Lemma 7.31 existieren zudem $\alpha, \beta \in \mathcal{O}_{\breve{\mathcal{E}}}$ mit $(\varphi-1)(\alpha) = -a$ und $(\varphi-1)(\beta) = -b$. Insbesondere ist dann $(\varphi-1)(r) = a - b = (\varphi-1)(\beta-\alpha)$ und damit $\alpha - \beta + r \in \ker(\varphi-1) = (\mathcal{O}_{\breve{\mathcal{E}}})^{\varphi-1} = \mathbb{Z}_p$.

Behauptung: $e_1^{(a)} := 1 \otimes e_1, e_2^{(a)} := (\alpha \otimes e_1 + 1 \otimes e_2)$ ist eine $\mathbb{Z}_p$-Basis von $\mathbb{V}(D_a) = (\mathcal{O}_{\breve{\mathcal{E}}} \otimes_{\mathcal{O}_\mathcal{E}} D_a)^{\varphi=1}$.
Zunächst einmal müssen wir zeigen, dass die angegebenen Elemente überhaupt in $\mathbb{V}(D_a)$ liegen. Dies ist aber leicht zu sehen, denn einerseits gilt

$$(\varphi \otimes g_a)(e_1^{(a)}) = \varphi(1) \otimes g_a(e_1) = 1 \otimes e_1 = e_1^{(a)}$$

und andererseits auch

$$\begin{aligned}(\varphi \otimes g_a)(e_2^{(a)}) &= \varphi(\alpha) \otimes g_a(e_1) + \varphi(1) \otimes g_a(e_2) \overset{\varphi(\alpha)=-a+\alpha}{=} -a \otimes e_1 + \alpha \otimes e_1 + 1 \otimes ae_1 + 1 \otimes e_2 \\ &= \alpha \otimes e_1 + 1 \otimes e_2 = e_2^{(a)}.\end{aligned}$$

Aus der exakten Sequenz $0 \to \mathcal{O}_\mathcal{E} \xrightarrow{F} D_a \xrightarrow{G} \mathcal{O}_\mathcal{E} \to 0$ erhalten wir die exakte Sequenz $0 \to \mathbb{Z}_p \xrightarrow{id\otimes F} \mathbb{V}(D_a) \xrightarrow{id\otimes G} \mathbb{Z}_p \to 0$, wobei wir $\mathbb{Z}_p$ über den Isomorphismus $(\alpha \mapsto \alpha \otimes 1) : \mathbb{Z}_p \to \mathbb{V}(\mathcal{O}_\mathcal{E})$ mit $\mathbb{V}(\mathcal{O}_\mathcal{E})$ identifizieren. Die beiden Vektoren $e_1^{(a)}$ und $e_2^{(a)}$ erfüllen die Eigenschaften

$$(id \otimes F)(1) = (id \otimes F)(1 \otimes 1) = id(1) \otimes F(1) = 1 \otimes e_1 = e_1^{(a)}$$

und

$$(id \otimes G)(e_2^{(a)}) = id(\alpha) \otimes G(e_1) + id(1) \otimes G(e_2) = \alpha \otimes \underbrace{G \circ F}_{=0}(1) + 1 \otimes 1 = 1.$$

Also ist $(e_1^{(a)}, e_2^{(a)})$ eine $\mathbb{Z}_p$-Basis von $\mathbb{V}(D_a)$ wie in Lemma 7.29 (i) und es existiert ein eindeutiges $\chi_a \in Hom^{cont.}(G_E, \mathbb{Z}_p)$ mit $\mathbb{V}(D_a) = \mathbb{Z}_p e_1^{(a)} \oplus \mathbb{Z}_p e_2^{(a)} = V_{\chi_a}$ und

$$\sigma \cdot e_2^{(a)} = (\sigma \otimes id)(e_2^{(a)}) = \chi_a(\sigma) e_1^{(a)} + e_2^{(a)} \text{ für alle } \sigma \in G_E.$$

Völlig analog lässt sich zeigen, dass $e_1^{(b)} := 1 \otimes e_1, e_2^{(b)} := \beta \otimes e_1 + 1 \otimes e_2$ eine $\mathbb{Z}_p$-Basis von $\mathbb{V}(D_b)$ ist und ein $\chi_b \in Hom^{cont.}(G_E, \mathbb{Z}_p)$ existiert, sodass $\mathbb{V}(D_b) = \mathbb{Z}_p e_1^{(b)} \oplus \mathbb{Z}_p e_2^{(b)} = V_{\chi_b}$ und

$$\sigma \cdot e_2^{(b)} = (\sigma \otimes id)(e_2^{(b)}) = \chi_b(\sigma) e_1^{(b)} + e_2^{(b)} \text{ für alle } \sigma \in G_E.$$

Nach unseren Voraussetzungen ist $\psi_r \colon D_a \to D_b$ ein Isomorphismus. Aufgrund der Funktorialität von $\mathbb{V}$ ist damit auch $\mathbb{V}(\psi_r) := id \otimes \psi_r \colon \mathbb{V}(D_a) \to \mathbb{V}(D_b)$ ein Isomorphismus, welcher gegeben ist durch

$$\begin{aligned}
\mathbb{V}(\psi_r)(xe_1^{(a)} + ye_2^{(a)}) &= (id \otimes \psi_r)(xe_1^{(a)} + ye_2^{(a)}) \\
&= x(id \otimes \psi_r)(1 \otimes e_1) + y(id \otimes \psi_r)(\alpha \otimes e_1 + 1 \otimes e_2) \\
&= x(1 \otimes \psi_r(e_1)) + y(\alpha \otimes \psi_r(e_1) + 1 \otimes \psi_r(e_2)) \\
&= x(1 \otimes e_1) + y(\alpha \otimes e_1 + 1 \otimes (re_1 + e_2)) \\
&= x(1 \otimes e_1) + y((\alpha + r) \otimes e_1 + 1 \otimes e_2), \text{ da } r \in \mathcal{O}_\mathcal{E} \\
&= x(1 \otimes e_1) + y((\alpha - \beta + r) \otimes e_1 + \beta \otimes e_1 + 1 \otimes e_2) \\
&= x(1 \otimes e_1) + y(\alpha - \beta + r)(1 \otimes e_1) + (\beta \otimes e_1 + 1 \otimes e_2), \text{ da } \alpha - \beta + r \in \mathbb{Z}_p \\
&= (x + (\alpha - \beta + r)y)(1 \otimes e_1) + ye_2^{(b)} \\
&= (x + (\alpha - \beta + r)y)e_1^{(b)} + ye_2^{(b)}.
\end{aligned}$$

Also ist $\mathbb{V}(D_a) = V_{\chi_a} \sim V_{\chi_b} = \mathbb{V}(D_b)$ mit $\alpha - \beta + r \in \mathbb{Z}_p$. □

Lemma 7.34. *Für alle $\chi \in Hom^{cont.}(G_E, \mathbb{Z}_p)$ existiert ein $\alpha \in \mathcal{O}_{\check{\mathcal{E}}}$ mit $(\varphi - 1)(\alpha) \in \mathcal{O}_\mathcal{E}$ und $\chi = \chi_\alpha$, d.h. $\chi(\sigma) = (\sigma - 1)(\alpha)$ für alle $\sigma \in G_E$.*

Beweis. Sei $V_\chi = \mathbb{Z}_p e_1 \oplus \mathbb{Z}_p e_2$ die zu χ gehörige stetige $\mathbb{Z}_p$-Darstellung mit $\sigma \cdot e_2 = \chi(\sigma)e_1 + e_2$. Wir haben die exakte Sequenz

$$0 \to \mathbb{Z}_p \xrightarrow{f} V_\chi \xrightarrow{g} \mathbb{Z}_p \to 0.$$

Da die Ringerweiterung der diskreten Bewertungsringe $\mathbb{Z}_p \subset \mathcal{O}_{\check{\mathcal{E}}}$ flach und $\mathbb{D}$ exakt ist, erhalten wir die exakten Sequenzen

$$0 \to \mathcal{O}_{\check{\mathcal{E}}} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p \xrightarrow{id \otimes f} \mathcal{O}_{\check{\mathcal{E}}} \otimes_{\mathbb{Z}_p} V_\chi \xrightarrow{id \otimes g} \mathcal{O}_{\check{\mathcal{E}}} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p \to 0 \qquad (1)$$

$$0 \longrightarrow \mathcal{O}_\mathcal{E} \xrightarrow{id \otimes f} \mathbb{D}(V_\chi) \xrightarrow{id \otimes g} \mathcal{O}_\mathcal{E} \longrightarrow 0. \qquad (2)$$

Nach Lemma 7.30 existiert ein $a \in \mathcal{O}_\mathcal{E}$ mit $(\mathbb{D}(V_\chi), \varphi \otimes id) = (D_a, g_a) = \mathcal{O}_\mathcal{E} e_1^{(a)} + \mathcal{O}_\mathcal{E} e_2^{(a)}$, d.h. $\varphi \otimes id = g_a$. Dabei sind nach der Konstruktion von D_a in Lemma 7.30 $e_1^{(a)} = (id \otimes f)(1) = 1 \otimes f(1) = 1 \otimes e_1$ und $(id \otimes g)(e_2^{(a)}) = 1 = 1 \otimes 1$. Wegen $(id \otimes g)(1 \otimes e_2) = 1 \otimes g(e_2) = 1 \otimes 1 = 1$ und der exakten Sequenz (1) liegt $e_2^{(a)} - 1 \otimes e_2$ in $\ker(id \otimes g) = \mathrm{im}(id \otimes f) \subset \mathcal{O}_\breve{\mathcal{E}} \otimes_{\mathbb{Z}_p} V_\chi$. Also existiert genau ein $\tilde{\alpha} \in \mathcal{O}_\breve{\mathcal{E}}$ mit

$$e_2^{(a)} = (id \otimes f)(\tilde{\alpha} \otimes 1) + 1 \otimes e_2 = \tilde{\alpha} \otimes f(1) + 1 \otimes e_2 = \tilde{\alpha} \otimes e_1 + 1 \otimes e_2.$$

Damit erhalten wir wegen $\varphi \otimes id = g_a$ schließlich

$$a e_1^{(a)} + e_2^{(a)} = (\varphi \otimes id)(e_2^{(a)}) = \varphi(\tilde{\alpha}) \otimes e_1^{(a)} + 1 \otimes e_2 = (\varphi(\tilde{\alpha}) - \tilde{\alpha}) \otimes e_1 + e_2^{(a)}.$$

Also ist $(\varphi(\tilde{\alpha}) - \tilde{\alpha} - a) \otimes e_1 = 0$ und mittels der Injektivität von

$$\rho : \mathcal{O}_\breve{\mathcal{E}} \xrightarrow{\sim} \mathcal{O}_\breve{\mathcal{E}} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p \hookrightarrow \mathcal{O}_\breve{\mathcal{E}} \otimes_{\mathbb{Z}_p} V_\chi,\ x \mapsto x \otimes e_1,$$

entsprechend $\varphi(\tilde{\alpha}) - \tilde{\alpha} = a \in \mathcal{O}_\mathcal{E}$. Da außerdem $e_2^{(a)}$ invariant unter der G_E-Operation ist, gilt für alle $\sigma \in G_E$:

$$\begin{aligned} \tilde{\alpha} \otimes e_1 + 1 \otimes e_2 = e_2^{(a)} = \sigma \cdot e_2^{(a)} &= (\sigma \otimes \sigma)(\tilde{\alpha} \otimes e_1 + 1 \otimes e_2) \\ &= \sigma(\tilde{\alpha}) \otimes e_1 + 1 \otimes (\sigma \cdot e_2) = \sigma(\tilde{\alpha}) \otimes e_1 + 1 \otimes (\chi(\sigma) e_1 + e_2) \\ &= (\sigma(\tilde{\alpha}) + \chi(\sigma)) \otimes e_1 + 1 \otimes e_2, \text{ da } \chi(\sigma) \in \mathbb{Z}_p. \end{aligned}$$

Also ist $(\chi(\sigma) + \sigma(\tilde{\alpha}) - \tilde{\alpha}) \otimes e_1 = 0$ und somit wegen der Injektivität von ρ schließlich $\chi(\sigma) = (\sigma - 1)(\alpha)$ mit $\alpha := -\tilde{\alpha} \in \mathcal{O}_\breve{\mathcal{E}}$ und $(\varphi - 1)(\alpha) = -a \in \mathcal{O}_\mathcal{E}$. □

Lemma 7.35. *(i) Für $a \in \mathcal{O}_\mathcal{E}$ gilt $\mathbb{D}(\mathbb{V}(D_a)) = D_a$.*

(ii) Für $\chi \in Hom^{cont.}(G_E, \mathbb{Z}_p)$ gilt $\mathbb{V}(\mathbb{D}(V_\chi)) = V_\chi$.

Beweis. Zu (i): Wie in Lemma 7.31 gesehen, existiert ein $\alpha \in \mathcal{O}_\breve{\mathcal{E}}$ mit $(\varphi - 1)(\alpha) = -a$. Da φ mit allen Elementen aus G_E kommutiert, ist dann auch $-a = \sigma(-a) = \sigma((\varphi - 1)(\alpha)) = (\varphi - 1)(\sigma(\alpha))$ und damit $\sigma(\alpha) - \alpha \in (\mathcal{O}_\breve{\mathcal{E}})^{\varphi=1} = \mathbb{Z}_p$ für alle $\sigma \in G_E$. Sei $D_a = \mathcal{O}_\mathcal{E} e_1 \oplus \mathcal{O}_\mathcal{E} e_2$ der zu a gehörige etale φ-Modul. Wir haben bereits im Beweis von Lemma 7.33 gesehen, dass $e_1^{(a)} := 1 \otimes e_1, e_2^{(a)} := \alpha \otimes e_1 1 \otimes e_2$ eine wie in Lemma 7.29 (i) konstruierte $\mathbb{Z}_p$-Basis von $\mathbb{V}(D_a)$ ist.

Wir setzen nun $e_1^\mathbb{D} := 1 \otimes e_1^{(a)}, e_2^\mathbb{D} := -\alpha \otimes e_1^{(a)} + 1 \otimes e_2^{(a)} \in \mathcal{O}_\breve{\mathcal{E}} \otimes_{\mathbb{Z}_p} \mathbb{V}(D_a)$ und zeigen $e_1^\mathbb{D}, e_2^\mathbb{D} \in \mathbb{D}(\mathbb{V}(D_a))$. Für $\sigma \in G_E$ ist nämlich auf der einen Seite

$$\begin{aligned} \sigma \cdot e_1^\mathbb{D} &= (\sigma \otimes \sigma)(1 \otimes e_1^{(a)}) = 1 \otimes ((\sigma \otimes id)(e_1^{(a)})) = 1 \otimes (1 \otimes e_1) \\ &= 1 \otimes e_1^{(a)} = e_1^\mathbb{D} \end{aligned}$$

und andererseits

$$\begin{aligned}\sigma \cdot e_2^{(a)} &= \sigma \otimes \sigma(-\alpha \otimes e_1^{(a)} + 1 \otimes e_2^{(a)}) = -\sigma(\alpha) \otimes \sigma \cdot e_1^{(a)} + 1 \otimes \sigma \cdot e_2^{(a)} \\ &= -\sigma(\alpha) \otimes (\sigma \otimes id(1 \otimes e_1)) + 1 \otimes (\sigma \otimes id(\alpha \otimes e_1 + 1 \otimes e_2)) \\ &= -\sigma(\alpha) \otimes e_1^{(a)} + 1 \otimes (\sigma(\alpha) \otimes e_1) + 1 \otimes (1 \otimes e_2) \\ &= -\sigma(\alpha) \otimes e_1^{(a)} + 1 \otimes ((\sigma(\alpha) - \alpha) \otimes e_1) + 1 \otimes (\alpha \otimes e_1) + 1 \otimes (1 \otimes e_2) \\ &= -\sigma(\alpha) \otimes e_1^{(a)} + (\sigma(\alpha) - \alpha) \otimes (1 \otimes e_1) + 1 \otimes (\alpha \otimes e_1 + 1 \otimes e_2), \text{ da } \sigma(\alpha) - \alpha \in \mathbb{Z}_p \\ &= -\alpha \otimes e_1^{(a)} + 1 \otimes e_2^{(a)} = e_2^{\mathbb{D}}.\end{aligned}$$

Also liegen $e_1^{\mathbb{D}}$ und $e_2^{\mathbb{D}}$ in $\mathbb{D}(\mathbb{V}(D_a))$.

Wir haben die exakte Sequenz $0 \to \mathcal{O}_\mathcal{E} \xrightarrow{F} D_a \xrightarrow{G} \mathcal{O}_\mathcal{E} \to 0$, woraus wir die exakte Sequenz $0 \to \mathbb{Z}_p \xrightarrow{id \otimes F} \mathbb{V}(D_a) \xrightarrow{is \otimes G} \mathbb{Z}_p \to 0$ erhalten. Die beiden Basiselemente $e_1^{(a)}, e_2^{(a)} \in \mathbb{V}(D_a)$ waren so konstruiert, dass $(id \otimes F)(1) = e_1^{(a)}$ und $(id \otimes G)(e_2^{(a)}) = 1$ gilt. Aus der letzten exakten Sequenz erhalten wir wiederum die kurze exakte Sequenz

$$0 \longrightarrow \mathcal{O}_\mathcal{E} \xrightarrow{id \otimes id \otimes F} \mathbb{D}(\mathbb{V}(D_a)) \xrightarrow{id \otimes id \otimes G} \mathcal{O}_\mathcal{E} \longrightarrow 0.$$

Dann gilt für $e_1^{\mathbb{D}}, e_2^{\mathbb{D}} \in \mathbb{D}(\mathbb{V}(D_a))$ einerseits

$$(id \otimes id \otimes F)(1) = (id \otimes id \otimes F)(1 \otimes 1 \otimes 1) = 1 \otimes 1 \otimes F(1) = 1 \otimes (1 \otimes e_1) = e_1^{\mathbb{D}}$$

und andererseits

$$\begin{aligned}(id \otimes id \otimes G)(e_2^{\mathbb{D}}) &= (id \otimes id \otimes G)(-\alpha \otimes 1 \otimes e_1 + 1 \otimes \alpha \otimes e_1 + 1 \otimes 1 \otimes e_2) \\ &= -\alpha \otimes 1 \otimes \underbrace{G \circ F}_{=0}(1) + 1 \otimes \alpha \otimes \underbrace{G \circ F}_{=0}(1) + 1 \otimes 1 \otimes \underbrace{G(e_2)}_{=1} = 1 \otimes 1 \otimes 1 = 1.\end{aligned}$$

Nach Lemma 7.30 ist damit $(e_1^{\mathbb{D}}, e_2^{\mathbb{D}})$ eine $\mathcal{O}_\mathcal{E}$-Basis von $\mathbb{D}(\mathbb{V}(D_a))$. Außerdem gilt für $e_2^{\mathbb{D}} \in \mathbb{D}(\mathbb{V}(D_a)) = (\mathbb{D}(\mathbb{V}(D_a)), \varphi \otimes id)$:

$$\begin{aligned}(\varphi \otimes id)(e_2^{\mathbb{D}}) &= (\varphi \otimes id)(-\alpha \otimes e_1^{(a)} + 1 \otimes e_2^{(a)}) = -\varphi(\alpha) \otimes e_1^{(a)} + 1 \otimes e_2^{(a)} \\ &= (a - \alpha) \otimes e_1^{(a)} + 1 \otimes e_2^{(a)} = a(1 \otimes e_1^{(a)}) + (-\alpha \otimes e_1^{(a)} + 1 \otimes e_2^{(a)}) \\ &= a e_1^{\mathbb{D}} + e_2^{\mathbb{D}}.\end{aligned}$$

Also ist $\mathbb{D}(\mathbb{V}(D_a)) = D_a$, wobei wir e_1 mit $e_1^{\mathbb{D}}$ und e_2 mit $e_2^{\mathbb{D}}$ identifizieren.

Zu (ii): Für $\chi \in Hom^{cont.}(G_E, \mathbb{Z}_p)$ existiert nach Lemma 7.34 ein $\alpha \in \mathcal{O}_\mathcal{E}$ mit $(\varphi - 1)(\alpha) \in \mathcal{O}_\mathcal{E}$, d.h. $(\varphi - 1)(\alpha) = -a$ für ein $a \in \mathcal{O}_\mathcal{E}$, und $\chi(\sigma) = (\sigma - 1)(\alpha)$ für alle $\sigma \in G_E$. Sei $V_\chi = \mathbb{Z}_p e_1 \oplus \mathbb{Z}_p e_2$ die zu χ gehörige $\mathbb{Z}_p$-Darstellung. Mit der gleichen Vorgehensweise wie in (i) lässt sich schließlich zeigen:

- $\mathbb{D}(V_\chi) = \mathcal{O}_\mathcal{E}\tilde{e}_1 \oplus \mathcal{O}_\mathcal{E}\tilde{e}_2 = D_a$, wobei $\tilde{e}_1 := 1 \otimes e_1$ und $\tilde{e}_2 := -\alpha \otimes e_1 + 1 \otimes e_2$ eine $\mathcal{O}_\mathcal{E}$-Basis von $\mathbb{D}(V_\chi)$ ist, wie sie in Lemma 7.30 konstruiert wird.
- $\mathbb{V}(\mathbb{D}(V_\chi)) = \mathbb{Z}_p e_1^{\mathbb{V}} \oplus \mathbb{Z}_p e_2^{\mathbb{V}}$, wobei $e_1^{\mathbb{V}} := 1 \otimes \tilde{e}_1$ und $e_2^{\mathbb{V}} := \alpha \otimes \tilde{e}_1 + 1 \otimes \tilde{e}_2$ eine $\mathbb{Z}_p$-Basis von $\mathbb{V}(\mathbb{D}(V_\chi))$ ist, wie sie in Lemma 7.29 konstruiert wird.

Aus dem letzten Punkt erhält man für $\sigma \in G_E$ wegen $\sigma(\alpha) = \chi(\sigma) + \alpha$ und $\chi(\sigma) \in \mathbb{Z}_p$ schließlich

$$\begin{aligned}\sigma \cdot e_2^{\mathbb{V}} &= (\sigma \otimes id)(\alpha \otimes \tilde{e}_1 + 1 \otimes \tilde{e}_2) = \sigma(\alpha) \otimes \tilde{e}_1 + 1 \otimes \tilde{e}_2 \\ &= (\chi(\sigma) + \alpha) \otimes \tilde{e}_1 + 1 \otimes \tilde{e}_2 = \chi(\sigma) e_1^{\mathbb{V}} + e_2^{\mathbb{V}}.\end{aligned}$$

Also gilt auch $\mathbb{V}(\mathbb{D}(V_\chi)) = V_\chi$, wobei wir e_1 mit $e_1^{\mathbb{V}}$ und e_2 mit $e_2^{\mathbb{V}}$ identifizieren. □

Satz 7.36. *Ist $a \in \mathcal{O}_\mathcal{E}$ und $\alpha \in \mathcal{O}_\mathcal{E}$ mit $(\varphi - 1)(\alpha) = -a$, so stimmt der stetige Charakter $\delta_\mathcal{E}(a)$ mit dem stetigen Charakter χ_α überein.*

Beweis. Sei $D_a = \mathcal{O}_\mathcal{E} e_1 \oplus \mathcal{O}_\mathcal{E} e_2$ der zu $a \in \mathcal{O}_\mathcal{E}$ gehörige etale φ-Modul. Im Beweis von Lemma 7.33 haben wir bereits gesehen, dass die Elemente $e_1^{(a)} := 1 \otimes e_1, e_2^{(a)} := \alpha \otimes e_1 + 1 \otimes e_2$ eine wie in Lemma 7.29 konstruierte $\mathbb{Z}_p$-Basis von $\mathbb{V}(D_a)$ bilden. Nach der Konstruktion von $\delta_\mathcal{E}$ ist $\chi := \delta_\mathcal{E}(a) \in Hom^{cont.}(G_E, \mathbb{Z}_p)$ mit $\mathbb{V}(D_a) = V_\chi$. Ist nun $\sigma \in G_E$, so erhält man einerseits

$$\sigma \cdot e_2^{(a)} = \chi(\sigma) e_1^{(a)} + e_2^{(a)} = \chi(\sigma) e_1^{(a)} + \alpha \otimes e_1 + 1 \otimes e_2$$

und andererseits

$$\sigma \cdot e_2^{(a)} = (\sigma \otimes id)(\alpha \otimes e_1 + 1 \otimes e_2) = \sigma(\alpha) \otimes e_1 + 1 \otimes e_2.$$

Daher gilt

$$\chi(\sigma) e_1^{(a)} = \sigma(\alpha) \otimes e_1 - \alpha \otimes e_1 = \underbrace{(\sigma(\alpha) - \alpha)}_{= \chi_\alpha(\sigma) \in \mathbb{Z}_p} \otimes e_1 = \chi_\alpha(\sigma) e_1^{(a)},$$

woraus schließlich $\chi_\alpha(\sigma) = \chi(\sigma) = \delta_\mathcal{E}(a)(\sigma)$ für alle $\sigma \in G_E$ folgt. □

Korollar 7.37. *Die Abbildung $\delta_\mathcal{E}: \mathcal{O}_\mathcal{E} \to Hom^{cont.}(G_E, \mathbb{Z}_p)$ ist sogar ein Gruppenhomomorphismus.*

Beweis. Um die Homomorphieeigenschaft nachzuweisen, wählen wir $a, b \in \mathcal{O}_\mathcal{E}$, sowie $\alpha, \beta \in \mathcal{O}_\mathcal{E}$ mit $(\varphi - 1)(\alpha) = -a$ und $(\varphi - 1)(\beta) = -b$. Dann ist auch $(\varphi - 1)(\alpha + \beta) = -(a + b)$ und zusammen mit Satz 7.36 folgt für alle $\sigma \in G_E$:

$$\begin{aligned}\delta_\mathcal{E}(a + b)(\sigma) &= \chi_{\alpha+\beta}(\sigma) = (\sigma - 1)(\alpha + \beta) = (\sigma - 1)(\alpha) + (\sigma - 1)(\beta) \\ &= \chi_\alpha(\sigma) + \chi_\beta(\sigma) \\ &= \delta_\mathcal{E}(a)(\sigma) + \delta_\mathcal{E}(b)(\sigma).\end{aligned}$$

□

Sind nun $a, b \in \mathcal{O}_\mathcal{E}$ mit $a - b \in (\varphi - 1)\mathcal{O}_\mathcal{E}$, so ist nach Lemma 7.30 (ii) $D_a \sim D_b$ und damit wegen Lemma 7.33 auch $V_{\delta_\mathcal{E}(a)} = \mathbb{V}(D_a) \sim \mathbb{V}(D_b) = V_{\delta_\mathcal{E}(b)}$. Mit Hilfe von Lemma 7.29 folgt daraus aber, dass bereits $\delta_\mathcal{E}(a) = \delta_\mathcal{E}(b)$ gilt. Also faktorisiert $\delta_\mathcal{E}$ über $\bar{\delta}_\mathcal{E}: \mathcal{O}_\mathcal{E}/(\varphi - 1)\mathcal{O}_\mathcal{E} \to Hom^{cont.}(G_E, \mathbb{Z}_p)$.

Lemma 7.38. *$\bar{\delta}_\mathcal{E}: \mathcal{O}_\mathcal{E}/(\varphi - 1)\mathcal{O}_\mathcal{E} \to Hom^{cont.}(G_E, \mathbb{Z}_p)$ ist eine Bijektion.*

Beweis. Für die Injektivität seien $a + (\varphi - 1)\mathcal{O}_\mathcal{E}, b + (\varphi - 1)\mathcal{O}_\mathcal{E} \in \mathcal{O}_\mathcal{E}/(\varphi - 1)\mathcal{O}_\mathcal{E}$ mit $\bar{\delta}_\mathcal{E}(a + (\varphi - 1)\mathcal{O}_\mathcal{E}) = \chi_a = \chi_b = \bar{\delta}_\mathcal{E}(b + (\varphi - 1)\mathcal{O}_\mathcal{E})$. Nach Definition von $\bar{\delta}_\mathcal{E}$ ist dann $\mathbb{V}(D_a) = V_{\chi_a} = V_{\chi_b} = \mathbb{V}(D_b)$, also insbesondere $V_{\chi_a} \sim V_{\chi_b}$. Aus Lemma 7.35 folgt daraus

$$D_a = \mathbb{D}(\mathbb{V}(D_a)) = \mathbb{D}(V_{\chi_a}) \sim \mathbb{D}(V_{\chi_b}) = \mathbb{D}(\mathbb{V}(D_b)) = D_b.$$

Mittels 7.30 (ii) erhält man schließlich $a - b \in (\varphi - 1)\mathcal{O}_\mathcal{E}$.

Für die Surjektivität sei $\chi \in Hom^{cont.}(G_E, \mathbb{Z}_p)$. Wie bereits zuvor gesehen existiert dann ein $a \in \mathcal{O}_\mathcal{E}$ mit $\mathbb{D}(V_\chi) = D_a$. Aus Lemma 7.35 folgt damit, dass $V_\chi = \mathbb{V}(\mathbb{D}(V_\chi)) = \mathbb{V}(D_a)$. Nach Definition von $\bar{\delta}_\mathcal{E}$ ist dann $\bar{\delta}_\mathcal{E}(a + (\varphi - 1)\mathcal{O}_\mathcal{E}) = \chi$. □

Da $\mathbb{Z}_p$ eine abelsche Gruppe ist, gilt sogar $Hom^{cont.}(G_E, \mathbb{Z}_p) = Hom^{cont.}({G_E}^{ab}, \mathbb{Z}_p)$ und somit $\bar{\delta}_\mathcal{E}: \mathcal{O}_\mathcal{E}/(\varphi - 1)\mathcal{O}_\mathcal{E} \to Hom^{cont.}({G_E}^{ab}, \mathbb{Z}_p)$.

7.6 Berechnung der Invarianten einer Algebra nach Witt

Für einen lokalen Körper L bezeichnen wir wie gewohnt mit $inv_L: H^2(L^{sep}|L) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$ die zugehörige Invariantenabbildung. In diesem Abschnitt wollen wir die Invariante einer Azumaya-Algebra unter der Identifikation

$$Br(L) = \bigcup_{\substack{L'|L \text{ endl.} \\ \text{Galois}}} Br(L'|L) \overset{3.8}{\cong} \bigcup_{\substack{L'|L \text{ endl.} \\ \text{Galois}}} H^2(L'|L) = H^2(L^{sep}|L) \overset{inv_L}{\cong} \mathbb{Q}/\mathbb{Z}$$

nach der Vorgehensweise von Ernst Witt explizit berechnen, wenn $L = E \cong k((t))$ ein lokaler Körper der Charakteristik p ist. Zunächst setzen wir allerdings nur voraus, dass $E \cong k((t))$ ein vollständiger, diskret bewerteter Körper der Charakteristik p mit vollkommenem Restklassenkörper k ist.

Lemma 7.39. *Es existiert ein G_E-äquivarianter, injektiver Ringhomomorphismus $\iota: \mathcal{O}_\mathcal{E} \to W(E)$, für den das Diagramm*

$$\begin{array}{ccc} \mathcal{O}_\mathcal{E} & \xhookrightarrow{\iota} & W(E) \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle F} \\ \mathcal{O}_\mathcal{E} & \xhookrightarrow{\iota} & W(E) \end{array}$$

kommutiert. Des Weiteren existiert analog ein Ringhomomorphismus $\check{\iota}\colon \mathcal{O}_{\check{\mathcal{E}}} \to W(E^{sep})$*, sodass das Diagramm*

$$\begin{array}{ccc} \mathcal{O}_{\mathcal{E}} & \xhookrightarrow{\iota} & W(E) \\ \downarrow & & \downarrow \\ \mathcal{O}_{\check{\mathcal{E}}} & \xhookrightarrow{\check{\iota}} & W(E^{sep}) \end{array}$$

kommutiert und sodass $\check{\iota} \circ \varphi = F \circ \check{\iota}$ *gilt.*

Beweis. Die Multiplikation mit p ist offensichtlich injektiv in $\mathcal{O}_{\mathcal{E}}$, d.h. nach Lemma 5.6 ist auch $\Phi_{\mathcal{O}_{\mathcal{E}}}\colon W(\mathcal{O}_{\mathcal{E}}) \to \mathcal{O}_{\mathcal{E}}^{\mathbb{N}_0}$ injektiv. Da außerdem $\varphi\colon \mathcal{O}_{\mathcal{E}} \to \mathcal{O}_{\mathcal{E}}$ ein Frobenius-Lift ist, ist $\Phi_{\mathcal{O}_{\mathcal{E}}}\colon W(\mathcal{O}_{\mathcal{E}}) \to \mathcal{O}_{\mathcal{E}}^{\mathbb{N}_0}$ nach Satz 5.10 ein Ringhomomorphismus mit

$$\mathrm{im}(\Phi_{\mathcal{O}_{\mathcal{E}}}) = \left\{ (u_n)_{n\geq 0} \mid \forall n \geq 0 : \varphi(u_n) \equiv u_{n+1} \mod p^{n+1}\mathcal{O}_{\mathcal{E}} \right\},$$

wie in Lemma 5.7 gesehen. Man beachte, dass auch $\varphi\colon \mathcal{O}_{\mathcal{E}} \to \mathcal{O}_{\mathcal{E}}$ injektiv ist, denn $\mathcal{O}_{\mathcal{E}}$ ist ein diskreter Bewertungsring mit maximalem Ideal $p\mathcal{O}_{\mathcal{E}}$, d.h. insbesondere ein lokaler Hauptidealring. Somit ist das Primideal $\ker(\varphi)$ entweder 0 oder $p\mathcal{O}_{\mathcal{E}}$. Da aber $\varphi(p) = p$, muss $\ker(\varphi) = 0$ gelten und schließlich φ injektiv sein. Damit erhalten wir einen injektiven Ringhomomorphismus

$$\psi\colon \mathcal{O}_{\mathcal{E}} \to \mathcal{O}_{\mathcal{E}}^{\mathbb{N}_0}, a \mapsto (\varphi^n(a))_{n\geq 0}$$

mit $\mathrm{im}(\psi) \subset \mathrm{im}(\Phi_{\mathcal{O}_{\mathcal{E}}})$. Wir setzen $\tilde{\iota} := \Phi_{\mathcal{O}_{\mathcal{E}}}^{-1} \circ \psi\colon \mathcal{O}_{\mathcal{E}} \hookrightarrow W(\mathcal{O}_{\mathcal{E}})$ und erhalten dadurch einen wohldefinierten, injektiven Ringhomomorphismus, welcher eindeutig durch die Eigenschaft $(\Phi_{\mathcal{O}_{\mathcal{E}}} \circ \tilde{\iota})(a) = (\varphi^n(a))_{n\geq 0}$ für $a \in \mathcal{O}_{\mathcal{E}}$ definiert ist.

Aus dem Ringhomomorphismus $can\colon \mathcal{O}_{\mathcal{E}} \to E, a \mapsto a + p\mathcal{O}_{\mathcal{E}}$ erhalten wir nach Satz 5.10 den Ringhomomorphismus

$$W(can)\colon W(\mathcal{O}_{\mathcal{E}}) \to W(E), (a_n)_{n\geq 0} \mapsto (a_n + p\mathcal{O}_{\mathcal{E}})_{n\geq 0}$$

und setzen schließlich $\iota := W(can) \circ \tilde{\iota}\colon \mathcal{O}_{\mathcal{E}} \to W(E)$. Angenommen, es existiert ein $a \in \ker(\iota)$ mit $a \neq 0$. Dann existieren $u \in \mathcal{O}_{\mathcal{E}}^*, n \in \mathbb{N}_0$ mit $a = up^n$. Da ι ein Ringhomomorphismus ist, muss auch $\iota(u)$ eine Einheit in $W(E)$ sein und somit insbesondere $\iota(u) \neq 0$. Wegen $0 = \iota(a) = \iota(u)\iota(p)^n$ ist dann $\iota(p) = 0$, da $W(E)$ nach Satz 5.18 (i) ein Integritätsbereich ist. Daraus würde aber folgen, dass $0 = \iota(p) = p\iota(1) = p \cdot 1_{W(E)}$, d.h. $char(W(E)) = p$, was ein Widerspruch zu Lemma 5.19 ist. Also handelt es sich bei ι um einen injektiven Ringhomomorphismus. Da G_E trivial auf $W(E)$ und $\mathcal{O}_{\mathcal{E}}$ operiert, ist auch trivialerweise $\iota\colon \mathcal{O}_{\mathcal{E}} \hookrightarrow W(E)$ G_E-äquivariant.

Sei nun $a \in \mathcal{O}_{\mathcal{E}}$ und $(a_m)_{m\geq 0} \in W(\mathcal{O}_{\mathcal{E}})$ mit $\tilde{\iota}(a) = (a_m)_{m\geq 0}$, d.h. $(\varphi^n(a))_{n\geq 0} = \Phi_{\mathcal{O}_{\mathcal{E}}} \circ \tilde{\iota}(a) =$

$\Phi_{\mathcal{O}_\mathcal{E}}((a_m)_{m\geq 0}) = (\Phi_n((a_m)_{m\geq 0}))_{n\geq 0}$. Da $\varphi\colon \mathcal{O}_\mathcal{E} \to \mathcal{O}_\mathcal{E}$ ein Ringhomomorphismus ist, gilt:

$$\begin{aligned}\Phi_{\mathcal{O}_\mathcal{E}}((\varphi(a_m))_{m\geq 0}) &= (\Phi_n((\varphi(a_m))_{m\geq 0}))_{n\geq 0} = (\varphi(\Phi_n((a_m)_{m\geq 0})))_{n\geq 0}\\ &= (\varphi(\varphi^n(a)))_{n\geq 0} = (\varphi^n(\varphi(a)))_{n\geq 0}\\ &= \Phi_{\mathcal{O}_\mathcal{E}} \circ \tilde{\iota}(\varphi(a)).\end{aligned}$$

Aufgrund der Injektivität von $\Phi_{\mathcal{O}_\mathcal{E}}$ ist dann $\tilde{\iota}(\varphi(a)) = (\varphi(a_m))_{m\geq 0}$. Da $char(E) = p$, folgt zusammen mit Satz 5.16 (i):

$$\begin{aligned}F(\iota(a)) &= F((a_m + p\mathcal{O}_\mathcal{E})_{m\geq 0}) = (a_m^p + p\mathcal{O}_\mathcal{E})_{m\geq 0} = (\varphi(a_m) + p\mathcal{O}_\mathcal{E})_{m\geq 0}\\ &= W(can)((\varphi(a_m))_{m\geq 0}) = W(can) \circ \tilde{\iota}(\varphi(a))\\ &= \iota \circ \varphi(a).\end{aligned}$$

Also gilt $F \circ \iota = \varphi \circ \iota$.

Auf analoge Weise können wir einen injektiven Ringhomomorphismus $\check{\iota}\colon \mathcal{O}_{\check{\mathcal{E}}} \hookrightarrow W(E^{sep})$ konstruieren. Da $\Phi_{\mathcal{O}_{\check{\mathcal{E}}}}\colon W(\mathcal{O}_{\check{\mathcal{E}}}) \to \mathcal{O}_{\check{\mathcal{E}}}^{\mathbb{N}_0}$, $\varphi\colon \mathcal{O}_{\check{\mathcal{E}}} \to \mathcal{O}_{\check{\mathcal{E}}}$ und $can\colon \mathcal{O}_{\check{\mathcal{E}}} \to E^{sep}$ jeweils Fortsetzungen von $\Phi_{\mathcal{O}_\mathcal{E}}\colon W(\mathcal{O}_\mathcal{E}) \to \mathcal{O}_\mathcal{E}^{\mathbb{N}_0}$, $\varphi\colon \mathcal{O}_\mathcal{E} \to \mathcal{O}_\mathcal{E}$ und $can\colon \mathcal{O}_\mathcal{E} \to E$ sind, kommutiert das Diagramm

$$\begin{array}{ccc}\mathcal{O}_\mathcal{E} & \xhookrightarrow{\iota} & W(E)\\ \downarrow & & \downarrow\\ \mathcal{O}_{\check{\mathcal{E}}} & \xhookrightarrow{\check{\iota}} & W(E^{sep}).\end{array}$$

Damit bleibt nur noch die G_E-Äquivarianz zu zeigen, welche bei ι trivial war. Sei dafür $\sigma \in G_E$ und $a \in \mathcal{O}_{\check{\mathcal{E}}}$. Dann gilt wegen der Kommutativität von φ und σ:

$$\begin{aligned}\Phi_{\mathcal{O}_{\check{\mathcal{E}}}}(\tilde{\check{\iota}}(\sigma(a))) &= (\varphi^n(\sigma(a)))_{n\geq 0} = (\sigma(\varphi^n(a)))_{n\geq 0} = \sigma \cdot (\varphi^n(a))_{n\geq 0}\\ &= \sigma \cdot \Phi_{\mathcal{O}_{\check{\mathcal{E}}}}(\tilde{\check{\iota}}(a)) = \sigma \cdot (\Phi_n(\tilde{\check{\iota}}(a)))_{n\geq 0}\\ &= (\sigma(\Phi_n(\tilde{\check{\iota}}(a))))_{n\geq 0} = (\Phi_n(\sigma(\tilde{\check{\iota}}(a))))_{n\geq 0}\\ &= \Phi_{\mathcal{O}_{\check{\mathcal{E}}}}(\sigma(\tilde{\check{\iota}}(a)).\end{aligned}$$

Aufgrund der Injektivität von $\Phi_{\mathcal{O}_{\check{\mathcal{E}}}}$ ist $\tilde{\check{\iota}}$ G_E-äquivariant. Nach der Definition der G_E-Operation auf $\mathcal{O}_{\check{\mathcal{E}}}$ ist $can\colon \mathcal{O}_{\check{\mathcal{E}}} \to E^{sep}$ trivialerweise G_E-äquivariant und damit auch $W(can)\colon W(\mathcal{O}_{\check{\mathcal{E}}}) \to W(E^{sep})$, da G_E diagonal auf $W(\mathcal{O}_{\check{\mathcal{E}}})$ und $W(E^{sep})$ operiert. Insgesamt ist damit dann auch $\check{\iota} = W(can) \circ \tilde{\check{\iota}}\colon \mathcal{O}_{\check{\mathcal{E}}} \hookrightarrow W(E^{sep})$ G_E-äquivariant. □

Aufgrund der injektiven Einbettungen $\mathcal{O}_\mathcal{E} \hookrightarrow W(E)$ und $\mathcal{O}_{\check{\mathcal{E}}} \hookrightarrow W(E^{sep})$ schreiben wir von nun an einfach $\mathcal{O}_\mathcal{E} \subset W(E)$ und $\mathcal{O}_{\check{\mathcal{E}}} \subset W(E^{sep})$.

Lemma 7.40. *Die Sequenz additiver Gruppen*

$$0 \longrightarrow W(\mathbb{F}_p) \longrightarrow W(E^{sep}) \xrightarrow{F-id} W(E^{sep}) \longrightarrow 0$$

ist exakt.

Beweis. Da $char(E^{sep}) = p$, lässt sich $\mathbb{F}_p$ einbetten in E^{sep} und damit auch $W(\mathbb{F}_p)$ in $W(E^{sep})$. Ist nun $a = (a_n)_{n\geq 0} \in W(\mathbb{F}_p)$, so gilt nach Lemma 5.16

$$(F - id)(a) = (a_n^p)_{n\geq 0} - (a_n)_{n\geq 0} = (a_n)_{n\geq 0} - (a_n)_{n\geq 0} = 0,$$

da $a_n \in \mathbb{F}_p$ für alle $n \geq 0$. Auf der anderen Seite gilt für $a \in \ker(F - id)$:

$$a = (a_n)_{n\geq 0} = F(a) = (a_n^p)_{n\geq 0},$$

d.h. $a_n = a_n^p$ für alle $n \geq 0$. Also ist $a_n \in \mathbb{F}_p$ für alle $n \geq 0$ und damit $a \in W(\mathbb{F}_p)$.

Schließlich bleibt noch die Surjektivität von $F - id$ zu zeigen. Nach Satz 5.14 (iv) ist $W(E^{sep})$ vollständig und separiert bzgl. der durch $(V_m(E^{sep}))_{m\geq 0}$ definierten Topologie. Außerdem ist nach Lemma 5.15

$$\bar{\tau}: E^{sep} \xrightarrow{\sim} W(E^{sep})/V_1(E^{sep}),\ a_0 \mapsto (a_0, 0, 0, \ldots) + V_1(E^{sep})$$

ein Isomorphismus. Wir schreiben daher der Einfachheit halber $a_0 = (a_0, 0, 0, \ldots) + V_1(E^{sep}) = a + V_1(E^{sep})$ für ein $a = (a_n)_{n\geq 0} \in W(E^{sep})$. Da die Witt-Ringoperation in der ersten Komponente mit der üblichen komponentenweisen Ringoperation übereinstimmt, ist $F - id \mod V_1(E^{sep})$ gegeben durch

$$W(E^{sep}) \to W(E^{sep})/V_1(E^{sep}) \cong E^{sep},\ (a_n)_{n\geq 0} \mapsto (a_n^p)_{n\geq 0} - (a_n)_{n\geq 0} \mapsto a_0^p - a_0.$$

Aufgrund von Lemma 5.16 gilt

$$(F - id)(V(a)) = F \circ V(a) - V(a) = V \circ F(a) - V(a) = V((F - id)(a))$$

für alle $a \in W(E^{sep})$. Daher induziert $F - id$ die Abbildung

$$\overline{F - id}: E^{sep} \cong W(E^{sep})/V_1(E^{sep}) \to E^{sep},\ a_0 \mapsto a_0^p - a_0.$$

Sei nun $a = (a_n)_{n\geq 0} \in W(E^{sep})$ und $a_0 = a + V_1(E^{sep}) \in E^{sep}$. Das Polynom $f(X) := X^p - X - a_0 \in E^{sep}$ ist separabel und somit existiert ein $\alpha_0 \in E^{sep}$ mit $f(\alpha_0) = 0$. Sei $\alpha^{(0)} \in W(E^{sep})$ mit $\alpha^{(0)} + V_1(E^{sep}) = \alpha_0$. Damit ist

$$a + V_1(E^{sep}) = a_0 = \alpha_0^p - \alpha_0 = (\overline{F - id})(\alpha_0) = (F - id)(\alpha^{(0)}) + V_1(E^{sep}),$$

d.h. es existiert ein $a^{(1)} \in W(E^{sep})$ mit $a = (F - id)(\alpha^{(0)}) + V(a^{(1)})$. Analog erhält man $\alpha^{(1)}, a^{(2)} \in W(E^{sep})$ mit $a^{(1)} = (F - id)(\alpha^{(1)}) + V(a^{(2)})$, woraus

$$\begin{aligned} a &= (F - id)(\alpha^{(0)}) + V(a^{(1)}) = (F - id)(\alpha^{(0)}) + V((F - id)(\alpha^{(1)}) + V(a^{(2)})) \\ &= (F - id)(\alpha^{(0)} + V(\alpha^{(1)})) + V^2(a^{(2)}) \end{aligned}$$

folgt. Induktiv erhält man schließlich $\alpha^{(n)}, a^{(n)} \in W(E^{sep})$ mit

$$a = (F - id)\left(\sum_{i=0}^{n} V^i(\alpha^{(i)})\right) + V^{n+1}(a^{(n+1)}) \text{ für alle } n \geq 0.$$

Da $W(E^{sep})$ vollständig und separiert ist bzgl. der durch $(V_m(E^{sep}))_{m\geq 0}$ definierten Topologie und $(V^i(\alpha^{(i)}))_{i\geq 0}$ eine Nullfolge ist, konvergiert die Reihe $\alpha := \sum_{i=0}^{\infty} V^i(\alpha^{(i)})$ in $W(E^{sep})$. Wegen $F \circ V = V \circ F$ ist zudem $F - id$ stetig und deshalb $(F - id)(\alpha) = a$, da auch $(V^{n+1}(a^{(n+1)}))_{n\geq 0}$ eine Nullfolge ist. □

Wir bezeichnen wieder mit $W_n(E) = W(E)/V_n(E)$ bzw. $W_n(E^{sep}) = W(E^{sep})/V_n(E^{sep})$ die Wittvektoren der Länge n. Aufgrund der mengentheoretischen Bijektion zwischen E^n und $W_n(E)$ bzw. $(E^{sep})^n$ und $W_n(E^{sep})$ aus Lemma 5.14 schreiben wir der Einfachheit halber lediglich $b = (b_0, \ldots, b_{n-1})$ für ein Element aus $W_n(E)$ bzw. $W_n(E^{sep})$.

Lemma 7.41. *Sei $n \in \mathbb{N}$ und $(F - id)\colon W_n(E^{sep}) \to W_n(E^{sep})$ die Reduktion von $(F - id)\colon W(E^{sep}) \to W(E^{sep})$ modulo $V_n(E^{sep})$. Dann ist $W_n(\mathbb{F}_p) = \ker(F - id) \cong \mathbb{Z}/p^n\mathbb{Z}$.*

Beweis. $W_n(\mathbb{F}_p) = \ker(F - id)$ folgt analog zum Beweis von Lemma 7.40. Wir wollen nun zeigen, dass $\ker(F - id)$ sogar zyklisch ist mit Erzeuger $\mathbf{1} = (1, 0, \ldots, 0) \in W_n(\mathbb{F}_p) = \ker(F - id)$. Bezeichnen wir mit δ_{ij} das Kronecker-Delta, so ist wegen $p^i \cdot \mathbf{1} = (\delta_{ij})_{0\leq j\leq n-1} \neq 0$ für $i < n$, aber $p^n \cdot \mathbf{1} = 0$ die Ordnung von $\mathbf{1}$ gleich p^n. Da aber $|W_n(\mathbb{F}_p)| = |\mathbb{F}_p^n| = p^n$, ist $\mathbf{1}$ bereits ein Erzeuger von $W_n(\mathbb{F}_p)$. Also ist $W_n(\mathbb{F}_p) = \ker(F - id) \cong \mathbb{Z}/p^n\mathbb{Z}$. □

Satz 7.42. *Sei $L|K$ eine endliche Galoiserweiterung mit Galoisgruppe G. Dann gibt es ein $\beta \in L$, sodass $(\tau(\beta))_{\tau\in G}$ eine K-Basis von L ist. Eine solche Basis heißt Normalbasis von $L|K$.*

Beweis. Einen Beweis der Aussage findet man in [Lo1], *§12, Satz 3* auf Seite 149. □

Lemma 7.43. *Sei $L|K$ eine endliche Galoiserweiterung mit zyklischer Galoisgruppe $G = Gal(L|K) = \langle\sigma\rangle$. Ist $Tr_{L|K}\colon L \to K$ die Spur und $\gamma \in L$, so sind äquivalent:*

(i) $Tr_{L|K}(\gamma) = 0$;

(ii) Es gibt ein $\alpha \in L$ mit $\gamma = \sigma(\alpha) - \alpha$.

Beweis. $(i) \Rightarrow (ii)$: Nach Satz 7.42 existiert ein $\beta \in L$, sodass $(\sigma^k(\beta))_{0\leq k\leq n-1}$ eine K-Basis von L ist, wobei $n := [L : K]$. Damit ist insbesondere $Tr_{L|K}(\beta) = \sum_{k=0}^{n-1} \sigma^k(\beta) \neq 0$. Schreiben wir nun $\gamma = \sum_{k=0}^{n-1} a_k\sigma^k(\beta)$ mit $a_k \in K$, so ist wegen

$$0 = Tr_{L|K}(\gamma) = \sum_{k=0}^{n-1} a_k \underbrace{Tr_{L|K}(\sigma^k(\beta))}_{=Tr_{L|K}(\beta)} = \left(\sum_{k=0}^{n-1} a_k\right) Tr_{L|K}(\beta)$$

und $Tr_{L|K}(\beta) \neq 0$ schließlich $\sum_{k=0}^{n-1} a_k = 0$. Wir setzen $\alpha := \sum_{k=0}^{n-1} a_k \sum_{j=0}^{k-1} \sigma^j(\beta) \in L$. Dann gilt:

$$\begin{aligned}
\sigma(\alpha) &= \sum_{k=0}^{n-1} a_k \sum_{j=0}^{k-1} \sigma^{j+1}(\beta) = \sum_{k=0}^{n-1} a_k \sum_{j=1}^{k} \sigma^j(\beta) + \underbrace{\left(\sum_{k=0}^{n-1} a_k\right)}_{=0} \beta \\
&= \sum_{k=0}^{n-1} a_k \sum_{j=1}^{k-1} \sigma^j(\beta) + \sum_{k=0}^{n-1} a_k \sigma^0(\beta) + \sum_{k=0}^{n-1} a_k \sigma^k(\beta) \\
&= \underbrace{\sum_{k=0}^{n-1} a_k \sum_{j=0}^{k-1} \sigma^j(\beta)}_{=\alpha} + \underbrace{\sum_{k=0}^{n-1} a_k \sigma^k(\beta)}_{=\gamma} \\
&= \alpha + \gamma.
\end{aligned}$$

$(ii) \Rightarrow (i)$: Sei $\alpha \in L$ mit $\gamma = \sigma(\alpha) - \alpha$. Dann gilt:

$$Tr_{L|K}(\gamma) = Tr_{L|K}(\sigma(\alpha)) - Tr_{L|K}(\alpha) = Tr_{L|K}(\alpha) - Tr_{L|K}(\alpha) = 0.$$

□

Aufgrund der Surjektivität von $F - id \colon W(E^{sep}) \to W(E^{sep})$ ist natürlich auch die Reduktion modulo $V_n(E^{sep})$, d.h. $F - id \colon W_n(E^{sep}) \to W_n(E^{sep})$ surjektiv. Ist also $a \in W_n(E) \subset W_n(E^{sep})$, so existiert ein $\alpha = (\alpha_0, \ldots, \alpha_{n-1}) \in W_n(E^{sep})$ mit $(F - id)(\alpha) = a$. Da die Elemente $\alpha_0, \ldots, \alpha_{n-1}$ in E^{sep} liegen, ist die Körpererweiterung $E(\alpha) := E(\alpha_0, \ldots, \alpha_{n-1})|E$ separabel. Bezeichnet man mit S eine beliebige Teilmenge von $W_n(E)$, so ist $(F - id)^{-1}(S) \subset W_n(E^{sep})$ und daher auch die Körpererweiterung $E((F - id)^{-1}(S))|E$ algebraisch und separabel. Wählen wir wie zuvor $a \in W_n(E)$ und $\alpha \in W_n(E^{sep})$ mit $(F - id)(\alpha) = a$, so gilt für alle $\sigma \in G_E = Gal(E^{sep}|E)$:

$$(F - id)(\sigma \cdot \alpha) = \sigma \cdot (F - id)(\alpha) = \sigma \cdot a = a,$$

da σ ein Körperautomorphismus ist mit $\sigma_{|_E} = id$. Also ist

$$\sigma(E((F - id)^{-1}(S))) \subset E((F - id)^{-1}(S)) \text{ für alle } \sigma \in G_E$$

und damit $E((F - id)^{-1}(S))|E$ sogar Galois.

Sei nun $a \in (F - id)(W_n(E))$, d.h. es existiert ein $\alpha \in W_n(E)$ mit $(F - id)(\alpha) = a$. Angenommen es gibt ein $\beta \in W_n(E^{sep})$ mit $(F - id)(\beta) = a$. Dann liegt β wegen $\alpha - \beta \in \ker(F - id) = W_n(\mathbb{F}_p) \subset W_n(E)$ und $\beta = \alpha - (\alpha - \beta)$ bereits in $W_n(E)$. Daraus erhalten wir $(F - id)^{-1}((F - id)(W_n(E))) \subset W_n(E)$ und schließlich $E((F - id)^{-1}((F - id)(W_n(E)))) = E$. Ersetzen wir also S durch die von S und $(F - id)^{-1}(W_n(E))$ erzeugte Untergruppe von $W_n(E)$, so ändert sich die Galoiserweiterung $E((F - id)^{-1}(S))|E$ nicht. Daher nehmen

wir von nun an S stets als Untergruppe von $W_n(E)$ mit $(F-id)(W_n(E)) \subset S$ an.

Im Folgenden bezeichnen wir mit G_S die Galoisgruppe der Körpererweiterung $E((F-id)^{-1}(S))|E$ und definieren die Abbildung

$$G_S \times S/\mathrm{im}(F-id) \to W_n(\mathbb{F}_p),\ (\sigma, a+(F-id)(W_n(E))) \mapsto (\sigma-1)(\alpha),$$

wobei $\alpha \in W_n(E^{sep})$ mit $(F-id)(\alpha) = a$. Diese Abbildung ist wohldefiniert, denn

1. für $b = (F-id)(\beta)$ mit $\beta \in W_n(E)$ ist nämlich $(\sigma-1)(\beta) = \sigma(\beta) - \beta = \beta - \beta = 0$;
2. sind $\alpha, \beta \in W_n(E^{sep})$ mit $(F-id)(\alpha) = (F-id)(\beta) = a$, so ist $\alpha - \beta \in \ker(F-id) = W_n(\mathbb{F}_p) \subset W_n(E)$ und damit $(\sigma-1)(\alpha) = (\sigma-1)(\beta) + \underbrace{(\sigma-1)(\alpha-\beta)}_{=0} = (\sigma-1)(\beta)$;
3. für $\alpha \in W_n(E^{sep})$ mit $(F-id)(\alpha) = a$ ist auch $(F-id)(\sigma\cdot\alpha) = \sigma\cdot(F-id)(\alpha) = \sigma\cdot a = a$ und deshalb $(\sigma-1)(\alpha) \in \ker(F-id) = W_n(\mathbb{F}_p) \cong \mathbb{Z}/p^n\mathbb{Z}_p$ für alle $\sigma \in G_S$.

Fixieren wir nun ein $\sigma \in G_S$, so ist aufgrund der Additivität von $(F-id)$ und $(\sigma-1)$ auch

$$\chi_\sigma : S/\mathrm{im}(F-id) \to W_n(\mathbb{F}_p),\ a+\mathrm{im}(F-id) \mapsto (\sigma-1)(\alpha)$$

additiv, das heißt $\chi_\sigma \in Hom(S/\mathrm{im}(F-id), W_n(\mathbb{F}_p))$. Ist auf der anderen Seite $a \in S$ fest, so ist

$$\psi^{(a)} : G_S \to W_n(\mathbb{F}_p),\ \sigma \mapsto \chi_\sigma(a+\mathrm{im}(F-id)) = (\sigma-1)(\alpha)$$

ein Gruppenhomomorphismus, denn für $\sigma, \tau \in G_S$ gilt:

$$\psi^{(a)}(\sigma\tau) = \sigma\tau(\alpha) - \alpha = \sigma\tau(\alpha) - \sigma(\alpha) + \sigma(\alpha) - \alpha = \sigma(\underbrace{\tau(\alpha)-\alpha}_{\in W_n(\mathbb{F}_p)}) + (\sigma-1)(\alpha)$$

$$= (\tau-1)(\alpha) + (\sigma-1)(\alpha) = \psi^{(a)}(\sigma) + \psi^{(a)}(\tau)$$

Damit erhalten wir zwei Gruppenhomomorphismen

$$G_S \to Hom(S/\mathrm{im}(F-id), W_n(\mathbb{F}_p)),\ \sigma \mapsto \chi_\sigma,$$

und

$$S/\mathrm{im}(F-id) \to Hom(G_S, W_n(\mathbb{F}_p)),\ a+\mathrm{im}(F-id) \mapsto \psi^{(a)}.$$

Wir können sogar zeigen, dass diese beide injektiv sind. Ist nämlich einerseits $\sigma \in G_S$ mit $\chi_\sigma = 0$, so ist $\chi_\sigma(a+\mathrm{im}(F-id)) = 0$ für alle $a \in S$, d.h.

$$0 = \chi_\sigma(a+\mathrm{im}(F-id)) = \sigma(\alpha) - \alpha$$

für alle $\alpha \in (F-id)^{-1}(S)$. Also ist $\sigma_{|_{E((F-id)^{-1}(S))}} = id$ und somit $\sigma = 1_{G_S}$. Andererseits folgt aus $\psi^{(a)} = 0$, dass $\sigma(\alpha) - \alpha = \psi^{(a)}(\sigma) = 0$ für alle $\sigma \in G_S$. Damit ist bereits $\alpha \in W_n(E)$ und

schließlich $a = (F - id)(\alpha) \in (F - id)(W_n(E)) = \mathrm{im}(F - id)$.

Ist nun $\sigma \in G_S$, so gilt:

$$\chi_{\sigma^{p^n}}(a + \mathrm{im}(F - id)) = p^n \underbrace{\chi_\sigma(a + \mathrm{im}(F - id))}_{\in W_n(\mathbb{F}_p) \cong \mathbb{Z}/p^n\mathbb{Z}} = 0.$$

Aus der Injektivität von $G_S \hookrightarrow Hom(S/\mathrm{im}(F - id), W_n(\mathbb{F}_p))$ folgt, dass bereits $\sigma^{p^n} = 1$ gelten muss, d.h. G_S vom Exponenten p^n ist. Analog folgt aus der Injektivität von $S/\mathrm{im}(F - id) \hookrightarrow Hom(G_S, W_n(\mathbb{F}_p))$, dass auch $S/\mathrm{im}(F - id)$ vom Exponenten p^n ist.

Sind G_S und $S/\mathrm{im}(F - id)$ sogar zyklisch, so folgt hieraus, dass die Ordnung jeweils p-Potenzen sein müssen, welche kleiner oder gleich p^n sind. In diesem Fall können wir das folgende leicht zu zeigende Resultat anwenden.

Ist $H = \langle h \rangle$ eine zyklische Gruppe der Ordnung N und $U = \langle u \rangle$ eine zyklische Gruppe der Ordnung M mit $M \mid N$, so ist $Hom(U, H)$ ebenfalls zyklisch mit Ordnung M und Erzeuger $(u \mapsto \frac{N}{M} \cdot h) \colon U \to H$.

Wegen $G_S \hookrightarrow Hom(S/\mathrm{im}(F - id), W_n(\mathbb{F}_p))$, $S/\mathrm{im}(F - id) \hookrightarrow Hom(G_S, W_n(\mathbb{F}_p))$ und $W_n(\mathbb{F}_p) \cong \mathbb{Z}/p^n\mathbb{Z}$ ist G zyklisch genau dann, wenn $S/\mathrm{im}(F - id)$ zyklisch ist. In diesem Fall haben wegen

$$|G_S| \leq |Hom(S/\mathrm{im}(F - id), W_n(\mathbb{F}_p))| = |S/\mathrm{im}(F - id)| \leq |Hom(G_S, W_n(\mathbb{F}_p))| = |G_S|$$

sowohl G_S als auch $S/\mathrm{im}(F - id)$ die Ordnung p^m für ein $m \leq n$. Insbesondere erhält man daraus zusammen mit der Injektivität der beiden Gruppenhomomorphismen, dass diese bereits Gruppenisomorphismen sind.

Satz 7.44. *(i) Sei $a = (a_0, \ldots, a_{n-1}) \in W_n(E)$ und $\alpha = (\alpha_0, \ldots, \alpha_{n-1}) \in W_n(E^{sep})$ mit $(F - id)(\alpha) = a$. Dann ist die Galoiserweiterung $E[\alpha_0, \ldots, \alpha_{n-1}]|E$ zyklisch vom Exponenten p^n.*

(ii) Ist umgekehrt $E'|E$ eine zyklische Galoiserweiterung vom Exponenten p^n, so ist E' von der Form wie in (i).

(iii) $[E[\alpha_0, \ldots, \alpha_{n-1}] : E] = p^n \Leftrightarrow a_0 \notin (\varphi - 1)(E)$.

(iv) Ist $a_0 \notin (\varphi - 1)(E)$, so gilt: Es gibt einen Erzeuger $\sigma \in Gal(E[\alpha_0, \ldots, \alpha_{n-1}]|E)$ mit $\sigma \cdot \alpha = (\sigma(\alpha_0), \ldots \sigma(\alpha_{n-1})) = (\alpha_0, \ldots, \alpha_{n-1}) + (1, 0, \ldots, 0) = \alpha + 1_{W_n(E^{sep})}$ in $W_n(E^{sep})$.

Beweis. (i) folgt sofort aus den vorherigen Ausführungen mit $S/\mathrm{im}(F - id) = \langle a + \mathrm{im}(F - id) \rangle$. Für (ii) setzen wir $G := Gal(E'|E) = \langle \sigma \rangle$, $T_n \colon W_n(E') \to W_n(E')$, $\gamma \mapsto \sum_{\rho \in G} \rho(\gamma)$, und

$Tr_{E'|E}\colon E' \to E$ als die Spur von $E'|E$. Da $E'|E$ vom Exponenten p^n ist, ist $[E' : E] = p^m$ für ein $m \leq n$. Wir setzen $c := p^{n-m} \cdot 1 = p^{n-m}(1, 0, \ldots, 0) \in W_n(\mathbb{F}_p) \subset W_n(E)$ und haben damit

$$T_n(c) = p^{n-m} T_n(1) = p^{n-m} \sum_{k=0}^{p^m-1} \sigma^k(1) = p^n \cdot 1 = 0 \text{ in } W_n(E).$$

Behauptung: Es existiert ein $\alpha \in W_n(E')$ mit $c = (\sigma - 1)(\alpha)$.

Sei dafür etwas allgemeiner $c = (c_0, \ldots, c_{n-1}) \in W_n(E')$ mit $T_n(c) = 0$. Da die Witt-Addition in der ersten Komponente der komponentenweisen Addition entspricht, ist

$$0 = T_n(c) = (Tr_{E'|E}(c_0), *, \ldots, *),$$

also insbesondere $Tr_{E'|E}(c_0) = 0$. Nach Lemma 7.43 existiert ein $\alpha_0 \in E'$ mit $c_0 = \sigma(\alpha_0) - \alpha_0$ und es gilt

$$c - (\sigma - 1)(\tau(\alpha_0)) = (c_0, \ldots, c_{n-1}) - (\sigma(\alpha_0) - \alpha_0, *, \ldots, *) = (0, c_1^{(1)}, c_2^{(1)}, \ldots, c_{n-1}^{(1)})$$

für geeignete $c_1^{(1)}, c_2^{(1)}, \ldots, c_{n-1}^{(1)} \in E'$, wobei hierbei τ den Teichmüller-Lift bezeichnet. Damit ist

$$T_n((0, c_1^{(1)}, c_2^{(1)}, \ldots, c_{n-1}^{(1)})) = T_n(c) + \underbrace{T_n(\sigma \cdot \tau(\alpha_0))}_{=T_n(\tau(\alpha_0))} - T_n(\tau(\alpha_0)) = 0.$$

Aufgrund der Additivität von $V\colon W_{n-1}(E') \to W_n(E')$, $(b_0, \ldots, b_{n-2}) \mapsto (0, b_0, \ldots, b_{n-2})$, aus Lemma 5.14 gilt

$$V \circ T_{n-1}((c_1^{(1)}, c_2^{(1)}, \ldots, c_{n-1}^{(1)})) = T_n \circ V((c_1^{(1)}, c_2^{(1)}, \ldots, c_{n-1}^{(1)})) = T_n((0, c_1^{(1)}, c_2^{(1)}, \ldots, c_{n-1}^{(1)})) = 0.$$

Nach Definition von V muss dann aber bereits $T_{n-1}((c_1^{(1)}, c_2^{(1)}, \ldots, c_{n-1}^{(1)})) = 0$ gelten. Analog zur vorherigen Vorgehensweise erhält man $\alpha_1, c_2^{(2)}, c_3^{(2)}, \ldots c_{n-1}^{(2)} \in E'$ mit

$$(c_1^{(1)}, \ldots, c_{n-1}^{(1)}) = (\sigma - 1)(\tau(\alpha_1)) + (0, c_2^{(2)}, \ldots, c_{n-1}^{(2)}).$$

Dann gilt:

$$\begin{aligned} c &= (\sigma - 1)(\tau(\alpha_0)) + (0, c_1^{(1)}, \ldots, c_{n-1}^{(1)}) = (\sigma - 1)(\tau(\alpha_0)) + V((c_1^{(1)}, \ldots, c_{n-1}^{(1)})) \\ &= (\sigma - 1)(\tau(\alpha_0)) + V((\sigma - 1)(\tau(\alpha_1)) + (0, c_2^{(2)}, \ldots, c_{n-1}^{(2)})) \\ &= (\sigma - 1)(\tau(\alpha_0) + V(\tau(\alpha_1))) + V^2((c_2^{(2)}, \ldots, c_{n-1}^{(2)})). \end{aligned}$$

Induktiv erhalten wir dadurch nach n Schritten schließlich $\alpha_0, \ldots, \alpha_{n-1} \in E'$ mit

$$c = (\sigma - 1)\left(\sum_{i=0}^{n-1} V^i(\tau(\alpha_i))\right) \overset{5.14(i)}{=} (\sigma - 1)(\underbrace{(\alpha_0, \ldots, \alpha_{n-1})}_{=:\alpha \in W_n(E')}) = (\sigma - 1)(\alpha).$$

Bezogen auf unser $c = p^{n-m} \cdot 1 \in W_n(\mathbb{F}_p) = \ker(F - id) \subset W_n(E')$ existiert also ein $\alpha \in W_n(E')$ mit $(\sigma - 1)(\alpha) = c$. Setzen wir $a := (F - id)(\alpha) \in W_n(E')$, so ist wegen

$$\begin{aligned}\sigma(a) - a &= \sigma((F - id)(\alpha)) - (F - id)(\alpha) = (F - id)(\sigma(\alpha)) - (F - id)(\alpha) \\ &= (F - id)(\sigma(\alpha) - \alpha) = (F - id)(c) = 0\end{aligned}$$

bereits $a \in W_n(E)$. Für eine natürliche Zahl $k \in \mathbb{N}_0$ gilt außerdem

$$\begin{aligned}\sigma^k(\alpha) - \alpha &= \sigma^k(\alpha) - \sigma^{k-1}(\alpha) + \sigma^{k-1}(\alpha) - \sigma^{k-2}(\alpha) + \ldots + \sigma(\alpha) - \alpha \\ &= \sigma^{k-1}(\sigma(\alpha) - \alpha) + \sigma^{k-2}(\sigma(\alpha) - \alpha) + \ldots + \sigma(\alpha) - \alpha \\ &= \sum_{r=0}^{k-1} \sigma^r(\sigma(\alpha) - \alpha) = \sum_{r=0}^{k-1} \sigma^r(c) = \sum_{r=0}^{k-1} c \\ &= k \cdot c.\end{aligned}$$

Das bedeutet aber, dass $\sigma^k(\alpha) = \alpha$ nur dann auftritt, falls k von $ord(c) = p^m$ geteilt wird. In diesem Fall ist aber wegen $[E' : E] = p^m$ bereits $\sigma^k = id$. Also muss $E' = E(\alpha) = E[\alpha_0, \alpha_1, \ldots, \alpha_{n-1}]$ gelten.

Zu (*iii*): Wir haben bereist zuvor gesehen, dass $S/\mathrm{im}(F - id) = \langle a + \mathrm{im}(F - id)\rangle$ und $G = Gal(E[\alpha_0, \ldots, \alpha_{n-1}]|E) = \langle\sigma\rangle$ zyklisch von gleicher Ordnung sind, d.h.

$$[E[\alpha_0, \ldots, \alpha_{n-1}] : E] = |G| = ord(\sigma) < p^n \Leftrightarrow ord(a + \mathrm{im}(F - id)) < p^n \Leftrightarrow p^{n-1} \cdot a \in \mathrm{im}(F - id).$$

Ist also $p^{n-1} \cdot a \in \mathrm{im}(F - id)$, so existiert ein $\beta \in W_n(E)$ mit $(F - id)(\beta) = p^{n-1}a = p^{n-1}(F - id)(\alpha) = (F - id)(p^{n-1} \cdot \alpha)$, d.h. $p^{n-1} \cdot \alpha - \beta \in \ker(F - id) = W_n(\mathbb{F}_p) \subset W_n(E)$. Also liegt auch $p^{n-1} \cdot \alpha = \beta + (p^{n-1} \cdot \alpha - \beta)$ in $W_n(E)$ und wir erhalten die folgende Kette von Äquivalenzen:

$$\begin{aligned}[E[\alpha_0, \ldots, \alpha_{n-1}] : E] < p^n &\Leftrightarrow p^{n-1} \cdot a \in (F - id)(W_n(E)) \\ &\Leftrightarrow p^{n-1} \cdot \alpha = (0, \ldots, 0, \alpha_0^{p^{n-1}}) \in W_n(E) \\ &\Leftrightarrow \alpha_0^{p^{n-1}} \in E \\ &\Leftrightarrow \alpha_0 = \alpha_0^p - a_0 = \alpha_0^{p^2} + (-a_0)^p - a_0 = \ldots = \alpha_0^{p^{n-1}} + \sum_{i=0}^{n-2} (-a_0)^{p^i} \in E \\ &\Leftrightarrow a_0 = \alpha_0^p - \alpha_0 = \varphi(\alpha_0) - \alpha_0 = (\varphi - 1)(\alpha_0) \in (\varphi - 1)(E).\end{aligned}$$

Für die letzte Äquivalenz sei angemerkt, dass aus $(\varphi - 1)(\beta) = a_0 = (\varphi - 1)(\alpha_0)$ mit $\beta \in E$ sofort $\alpha_0 - \beta \in \ker(\varphi - 1) = \mathbb{F}_p \subset E$ und deshalb $\alpha_0 = \beta + (\alpha_0 - \beta) \in E$ folgt. Aufgrund dieser Kette von Äquivalenzen gilt dann die Behauptung in (*iii*).

Zu (*iv*): Wie wir gerade gezeigt haben, folgt aus $\alpha_0 \notin (\varphi - 1)(E)$, dass $|G| = [E[\alpha_0, \ldots, \alpha_{n-1}] :$

$E] = p^n$ gilt, wobei $G := Gal(E[\alpha_0, \dots, \alpha_{n-1}]|E)$. Außerdem haben wir bereits zuvor gesehen, dass dann auch $a + \mathrm{im}(F - id) \in S/\mathrm{im}(F - id) = \langle a + \mathrm{im}(F - id) \rangle$ die Ordnung p^n hat. Betrachte nun die Isomorphie

$$\begin{aligned} G &\xrightarrow{\sim} Hom(S/\mathrm{im}(F - id), W_n(\mathbb{F}_p)) = Hom(\langle a + \mathrm{im}(F - id) \rangle, \langle (1, 0, \dots, 0) \rangle). \\ \tau &\mapsto \chi_\tau = (a + \mathrm{im}(F - id) \mapsto \tau(\alpha) - \alpha) \end{aligned}$$

Wie bereits zuvor gesehen, ist auch $Hom(S/\mathrm{im}(F - id), W_n(\mathbb{F}_p))$ zyklisch und wird wegen $ord(a + \mathrm{im}(F - id)) = ord((1, 0, \dots, 0)) = p^n$ durch $1_{Hom} := (a + \mathrm{im}(F - id) \mapsto (1, 0, \dots, 0))$ erzeugt. Aufgrund der obigen Isomorphie existiert ein Erzeuger $\sigma \in G$ mit $\chi_\sigma = 1_{Hom}$. Das bedeutet aber schließlich

$$\sigma(\alpha) - \alpha = \chi_\sigma(a + \mathrm{im}(F - id)) = 1_{Hom}(a + \mathrm{im}(F - id)) = (1, 0, \dots, 0)$$

bzw.

$$\sigma(\alpha) = (\sigma(\alpha_0), \dots \sigma(\alpha_{n-1})) = (\alpha_0, \dots, \alpha_{n-1}) + (1, 0, \dots, 0) = \alpha + 1_{W_n(E^{sep})}.$$

□

Betrachte nun das kommutative Diagramm

$$\begin{array}{ccccc} \mathcal{O}_{\breve{\mathcal{E}}} & \hookrightarrow & W(E^{sep}) & \longrightarrow & W_n(E^{sep}) \\ \uparrow & & \uparrow & & \uparrow \\ \mathcal{O}_{\mathcal{E}} & \hookrightarrow & W(E) & \longrightarrow & W_n(E) \end{array}$$

Für $a \in \mathcal{O}_{\mathcal{E}}$ sei wie zuvor $\alpha \in \mathcal{O}_{\breve{\mathcal{E}}}$ mit $(\varphi - 1)(\alpha) = a$. Wir bezeichnen mit $(a_0, a_1, \dots, a_{n-1})$ bzw. $(\alpha_0, \alpha_1, \dots, \alpha_{n-1})$ das Bild von a bzw. α in $W_n(E)$ bzw. $W_n(E^{sep})$. Man beachte dabei, dass wegen des kommutativen Diagramms aus Lemma 7.39 $(F - id)(\alpha_0, \dots, \alpha_{n-1}) = (a_0, \dots, a_{n-1})$ gilt. Wir betrachten nun den Gruppenhomomorphismus

$$\delta_{\mathcal{E}}(a)_n \colon G_E \xrightarrow{\delta_{\mathcal{E}}(a)} \mathbb{Z}_p \xrightarrow{can} \mathbb{Z}_p/p^n\mathbb{Z}_p \cong \frac{1}{p^n}\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$$

und setzen $E_n := (E^{sep})^{\ker(\delta_{\mathcal{E}}(a)_n)}$.

Satz 7.45. *$E_n = (E^{sep})^{\ker(\delta_{\mathcal{E}}(a)_n)} = E[\alpha_0, \dots, \alpha_{n-1}]$, d.h. insbesondere ist E_n eine zyklische endliche Erweiterung von E.*

Beweis. Nach Satz 7.36 ist $\delta_{\mathcal{E}}(a)(\sigma) = -(\sigma(\alpha) - \alpha)$ für alle $\sigma \in G_E$. Außerdem ist nach Korollar 5.21 $\mathbb{Z}_p = W(\mathbb{F}_p) \subset W(E^{sep})$ und damit

$$V_n(E^{sep}) \cap \mathbb{Z}_p = V_n(E^{sep}) \cap W(\mathbb{F}_p) = V_n(\mathbb{F}_p) = p^n W(\mathbb{F}_p) = p^n\mathbb{Z}_p.$$

Wir bezeichnen mit $\check{\iota}\colon \mathcal{O}_{\check{\mathcal{E}}} \hookrightarrow W(E^{sep})$ die G_E-äquivariante Einbettung von $\mathcal{O}_{\check{\mathcal{E}}}$ in $W(E^{sep})$.

Sei nun $\rho \in \ker(\delta_{\mathcal{E}}(a)_n)$, d.h. $-(\rho(\alpha) - \alpha) \in p^n\mathbb{Z}_p = V_n(E^{sep}) \cap \mathbb{Z}_p$. Also ist $\check{\iota}(\rho(\alpha) - \alpha) \in V_n(E^{sep})$ und damit aufgrund der G_E-Äquivarianz von $\check{\iota}$ auch $\rho(\check{\iota}(\alpha)) = \alpha$ in $W_n(E^{sep})$. Nach unseren Voraussetzungen ist $\check{\iota}(\alpha) = (\alpha_0, \dots, \alpha_{n-1})$ in $W_n(E^{sep})$ und somit $(\alpha_0, \dots, \alpha_{n-1}) = (\rho(\alpha_0), \dots, \rho(\alpha_{n-1}))$. Also ist $\rho(\alpha_k) = \alpha_k$ für alle $k \in \{0, \dots, n-1\}$ und deshalb bereits $E[\alpha_0, \dots, \alpha_{n-1}] \subset (E^{sep})^{\ker(\delta_{\mathcal{E}}(a)_n} = E_n$.

Sei nun $\sigma \in Gal(E^{sep}|E[\alpha_0, \dots, \alpha_{n-1}])$. Dann ist

$$\check{\iota}(\sigma(\alpha)) = \sigma(\check{\iota}(\alpha)) = \sigma((\alpha_0, \dots, \alpha_{n-1})) = (\alpha_0, \dots, \alpha_{n-1}) = \check{\iota}(\alpha)$$

in $W_n(E^{sep})$, da $\sigma_{|_{E[\alpha_0,\dots,\alpha_{n-1}]}} = id$. Also ist $\check{\iota}(\sigma(\alpha) - \alpha) \in V_n(E^{sep})$ und wegen $\sigma(\alpha) - \alpha = \delta_{\mathcal{E}}(a)(\sigma) \in \mathbb{Z}_p$ auch $\sigma(\alpha) - \alpha \in V_n(E^{sep}) \cap \mathbb{Z}_p = p^n\mathbb{Z}_p$. Hieraus folgt aber, dass σ ein Element von $\ker(\delta_{\mathcal{E}}(a)_n)$ ist und somit $Gal(E^{sep}|E[\alpha_0, \dots, \alpha_{n-1}]) \subset \ker(\delta_{\mathcal{E}}(a)_n)$. Nach dem Hauptsatz der Galoistheorie ist dann

$$E_n = (E^{sep})^{\ker(\delta_{\mathcal{E}}(a)_n} \subset (E^{sep})^{Gal(E^{sep}|E[\alpha_0,\dots,\alpha_{n-1}])} = E[\alpha_0, \dots, \alpha_{n-1}],$$

woraus schließlich die Gleichheit folgt. Aus Satz 7.44 (i) folgt außerdem, dass $E_n = (E^{sep})^{\ker(\delta_{\mathcal{E}}(a)_n} = E[\alpha_0, \dots, \alpha_{n-1}]$ eine endliche zyklische Galoiserweiterung vom Exponenten p^n ist. □

Sei nun $\chi_n\colon G_E/\ker(\delta_{\mathcal{E}}(a)_n) \hookrightarrow \mathbb{Q}/\mathbb{Z}$ der von $\delta_{\mathcal{E}}(a)_n$ induzierte injektive Gruppenhomomorphismus. Aus Satz 7.45 erhalten wir

$$G_E/\ker(\delta_{\mathcal{E}}(a)_n) = G_E/Gal(E^{sep}|E_n) \cong Gal(E_n|E) = G_{E_n|E}$$

und somit $\chi_n\colon G_{E_n|E} \hookrightarrow \mathbb{Q}/\mathbb{Z}$ als den von $\delta_{\mathcal{E}}(a)_n$ induzierten injektiven Gruppenhomomorphismus.

Satz 7.46. *Sei $u \in E^*$ und $\tilde{a}_0, \dots \tilde{a}_{n-1} \in E$. Dann wird durch*

$$(u \mid \tilde{a}_0, \dots, \tilde{a}_{n-1}] := E \cdot T \oplus E \cdot \vartheta_0 \oplus \dots \oplus E \cdot \vartheta_{n-1}$$

zusammen mit den Relationen

- $T^{p^n} = u$;
- $\vartheta_i \cdot \vartheta_j = \vartheta_j \cdot \vartheta_i$ *für alle* $0 \le i, j \le n-1$;
- $(T \cdot \vartheta_0 \cdot T^{-1}, \dots, T \cdot \vartheta_{n-1} \cdot T^{-1}) = (\vartheta_0, \dots, \vartheta_{n-1}) + (1, 0, \dots, 0)$ *(Witt-Addition);*
- $(F - id)(\vartheta_0, \dots, \vartheta_{n-1}) = (\tilde{a}_0, \dots, \tilde{a}_{n-1})$;

eine Azumaya-Algebra der E-Dimension p^{2n} definiert.

Beweis. Einen Beweis des Satzes findet man in [Wi] in §6. □

Proposition 7.47. *Gilt $a_0 \notin (\varphi - 1)E$, so ist $(u \mid a_0, \dots, a_{n-1}]$ isomorph zu der Azumaya-Algebra, welche durch $\bar{u} \cup \delta_1(\chi_n) \in H^2(E_n|E)$ definiert wird.*

Beweis. Wie wir zuvor gesehen haben, ist $E_n = E[\alpha_0, \dots, \alpha_{n-1}]$ eine zyklische Galoiserweiterung von E. Da außerdem $a_0 \notin (\varphi - 1)E$, ist nach Satz 7.44 $[E_n : E] = p^n$ und es existiert ein Erzeuger $\sigma \in G_{E_n|E}$ mit $G_{E_n|E} = \langle \sigma \rangle$ und

$$(\sigma(\alpha_0), \dots \sigma(\alpha_{n-1})) = (\alpha_0, \dots, \alpha_{n-1}) + (1, 0, \dots, 0) = \alpha + 1_{W_n(E^{sep})}$$

in $W_n(E_n)$. Trivialerweise gilt natürlich $\alpha_i \cdot \alpha_j = \alpha_j \cdot \alpha_i$ für alle $i, j \in \{0, \dots, n-1\}$ im Körper $E_n = E[\alpha_0, \dots, \alpha_{n-1}]$ und nach Wahl der $\alpha_0, \dots, \alpha_{n-1} \in E^{sep}$ auch $(F - id)(\alpha_0, \dots, \alpha_{n-1}) = (a_0, \dots, a_{n-1})$ in $W_n(E_n)$. Durch die explizite Beschreibung der Azumaya-Algebra $A(\bar{u} \cup \delta_1(\chi_n))$ in Beispiel 3.9 wissen wir, dass diese gegeben ist durch

$$A(\bar{u} \cup \delta_1(\chi_n)) = \bigoplus_{i=0}^{p^n} E_n \cdot t^i,$$

mit den Eigenschaften $t^{p^n} = u$ und $t \cdot \beta \cdot t^{-1} = \sigma(\beta)$ für alle $\beta \in E_n$. Nach der universellen Eigenschaft von $(u \mid a_0, \dots, a_{n-1}]$ existiert dann ein Homomorphismus $\psi\colon (u \mid a_0, \dots, a_{n-1}] \to A(\bar{u} \cup \delta_1(\chi_n))$ von E-Algebren mit $\psi(T) = t$ und $\psi(\vartheta_i) = \alpha_i$ für alle $i \in \{0, \dots, n-1\}$. Damit ist natürlich $E_n = E[\alpha_0, \dots, \alpha_{n-1}]$ und t im Bild von ψ enthalten und somit nach der expliziten Beschreibung von $A(\bar{u} \cup \delta_1(\chi_n))$ der Homomorphismus ψ surjektiv.

Nach Satz 3.6 hat die Azumaya-Algebra $A(\bar{u} \cup \delta_1(\chi_n))$ die E-Dimension $[E_n : E]^2 = p^{2n}$, genauso wie $(u \mid a_0, \dots, a_{n-1}]$. Also ist $\psi\colon (u \mid a_0, \dots, a_{n-1}] \to A(\bar{u} \cup \delta_1(\chi_n))$ sogar bijektiv. □

Falls es sich bei E sogar um einen lokalen Körper handelt, d.h. der Restklassenkörper k ist endlich, so betrachten wir, wie zu Beginn des Abschnitts beschrieben, die Invariante einer Azumaya-Algebra über die Identifikation

$$Br(E) = \bigcup_{\substack{E'|E \text{ endl.} \\ \text{Galois}}} Br(E'|E) \overset{3.8}{\cong} \bigcup_{\substack{E'|E \text{ endl.} \\ \text{Galois}}} H^2(E'|E) = H^2(E^{sep}|E) \overset{inv_E}{\cong} \mathbb{Q}/\mathbb{Z}.$$

Die Invariante der Azumaya-Algebra $(u \mid a_0, \dots, a_{n-1}]$ lässt sich in diesem Fall nach dem folgenden Satz von Ernst Witt sogar explizit berechnen.

Satz 7.48. *Sind $u, a_0, \dots, a_{n-1} \in E$ mit $u \neq 0$ und sind $U, A_0, \dots A_{n-1} \in \mathcal{O}_\mathcal{E}$ mit $U + p\mathcal{O}_\mathcal{E} = u$, $A_j + p\mathcal{O}_\mathcal{E} = a_j$ für alle $j \in \{0, \dots, n-1\}$, so gilt:*

$$inv_E((u \mid a_0, \dots, a_{n-1}]) = \underbrace{Tr_{K|\mathbb{Q}_p}\left(res\left(\left(\sum_{j=0}^{n-1} p^{j-n} A_j^{p^{n-1-j}}\right) \cdot d_{log} U\right)\right)}_{\in \mathbb{Q}_p/\mathbb{Z}_p = \bigcup_{m \geq 1} \frac{1}{p^m}\mathbb{Z}_p/\mathbb{Z}_p \cong \bigcup_{m \geq 1} \frac{1}{p^m}\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}} + \mathbb{Z}_p,$$

wobei $K = Quot(W(k)), E \cong k((t))$ *und* $k \cong \mathbb{F}_{p^r}$ *für ein* $r \in \mathbb{N}$.

Beweis. Einen Beweis des Satzes findet man in [Wi] in §8. □

7.7 Explizites Reziprozitätsgesetz von Fontaine-Witt

Von nun an sei k ein endlicher Körper der Charakteristik $p > 0$, d.h. $k = \mathbb{F}_{p^r}$ für ein $r \in \mathbb{N}$. Des Weiteren sei wieder E ein vollständiger diskret bewerteter Körper der Charakteristik p mit Restklassenkörper k. Damit ist E lokal und $E \cong k((t))$ nach Satz 1.22, da k aufgrund der Endlichkeit und $char(k) = p$ perfekt ist.

Wir bezeichnen weiterhin mit G_E die Galoisgruppe von $E^{sep}|E$ und mit $\delta_{\mathcal{E}}: \mathcal{O}_{\mathcal{E}} \to Hom^{cont.}({G_E}^{ab}, \mathbb{Z}_p)$ den in Abschnitt 7.5 konstruierten Gruppenhomomorphismus. Ist $a \in \mathcal{O}_{\mathcal{E}}$ und $\alpha \in \mathcal{O}_{\mathcal{E}}$ mit $(\varphi - 1)(\alpha) = -a$, so haben wir in Lemma 7.36 gesehen, dass $(\delta_{\mathcal{E}}(a))(\sigma) = (\sigma - 1)(\alpha)$ für alle $\sigma \in {G_E}^{ab}$.

Setzen wir $W := W(k)$ und $K := Quot(W)$, so ist nach Korollar 5.21 wegen $\mathbb{F}_p \subset k$ schließlich auch $\mathbb{Z}_p = W(\mathbb{F}_p) \subset W(k) = W$ und damit $\mathbb{Q}_p = Quot(\mathbb{Z}_p) \subset Quot(W) = K$. Nach Korollar 5.21 ist zudem K die eindeutige unverzweigte Erweiterung von $\mathbb{Q}_p$ vom Grad $[k : \mathbb{F}_p] = [\mathbb{F}_{p^r} : \mathbb{F}_p] = r$. Außerdem ist wegen Lemma 1.26 der Bewertungsring $W = \mathcal{O}_K$ ein freier $\mathbb{Z}_p$-Modul vom Rang $[K : \mathbb{Q}_p] = [k : \mathbb{F}_p] = r$.

Ist $E'|E$ eine endliche abelsche Erweiterung, so bezeichnen wir mit $(\cdot, E'|E): E^* \to Gal(E'|E) =: G_{E'|E}$ das Normrestsymbol der abelschen Erweiterung $E'|E$. Beim Übergang zum projektiven Limes über alle endlichen, abelschen Erweiterungen E' von E erhält man das universelle Normrestsymbol

$$(\cdot, E): E^* \hookrightarrow {G_E}^{ab} = \varprojlim_{\substack{E'|E \text{ endl.} \\ \text{abelsch}}} Gal(E'|E),$$

wobei (u, E) eindeutig durch $((u, E'|E))_{\substack{E'|E \text{ endl.} \\ \text{abelsch}}}$ bestimmt ist. Für eine etwas genauere Beschreibung und die Injektivität des universellen Normrestsymbols sei auf [Ne2], *Satz 5.13* verwiesen.

Definition 7.49. Mittels der zuvor angegebenen Notationen definieren wir die Abbildung

$$[*, *): \mathcal{O}_{\mathcal{E}} \times E^* \to \mathbb{Z}_p,\ (x, u) \mapsto [x, u) := (\delta_{\mathcal{E}}(x))((u, E)).$$

Unser Ziel ist es nun, diese Abbildung in expliziter Weise angeben zu können. Dazu zeigen wir zunächst das folgende Lemma:

Lemma 7.50. *Ist* $\varphi: \mathcal{O}_{\mathcal{E}} \to \mathcal{O}_{\mathcal{E}}$ *ein Frobenius-Lift, so ist* $(\varphi - 1)\mathcal{O}_{\mathcal{E}} \subset \mathcal{O}_{\mathcal{E}}$ *abgeschlossen bzgl. der p-adischen Topologie.*

Beweis. Da φ $\mathbb{Z}_p$-linear ist und $(\mathcal{O}_\mathcal{E})^{\varphi=1} = \mathbb{Z}_p$, ist φ stetig bzgl. der p-adischen Topologie und $\ker(\varphi - 1) = \mathbb{Z}_p \subset \mathcal{O}_\mathcal{E}$ abgeschlossen. Sei $1, x_1, \ldots, x_r \in W$ eine $\mathbb{Z}_p$-Basis des freien $\mathbb{Z}_p$-Moduls W vom Rang $r := [k : \mathbb{F}_p] = [K : \mathbb{Q}_p]$ und betrachte den $\mathbb{Z}_p$-Modul-Homomorphismus

$$\rho: \mathcal{O}_\mathcal{E} \to W = \mathbb{Z}_p \oplus \mathbb{Z}_p x_1 \oplus \ldots \oplus \mathbb{Z}_p x_r \to \mathbb{Z}_p, \sum_{n\in\mathbb{Z}} a_n t^n \mapsto a_0 = \alpha_0 + \alpha_1 x_1 + \ldots + \alpha_r x_r \mapsto \alpha_0,$$

welcher offensichtlich $\mathbb{Z}_p$-linear und damit stetig ist. Also ist auch

$$\ker(\rho) = \left\{ \sum_{n\in\mathbb{Z}} a_n t^n \mid a_0 \in \bigoplus_{i=1}^{r} \mathbb{Z}_p x_i \right\} \subset \mathcal{O}_\mathcal{E}$$

abgeschlossen. Man beachte, dass wegen $W = \mathbb{Z}_p \oplus \left(\bigoplus_{i=1}^r \mathbb{Z}_p x_i\right)$ schließlich

$$\mathcal{O}_\mathcal{E} = \mathbb{Z}_p \oplus \ker(\rho) = \ker(\varphi - 1) \oplus \ker(\rho)$$

gilt. Daher genügt es zu zeigen, dass die Einschränkung $(\varphi-1)_{|_{\ker(\rho)}}: \ker(\rho) \to (\varphi-1)\mathcal{O}_\mathcal{E}$ ein Homöomorphismus ist. Die Bijektivität und Stetigkeit folgt hierbei direkt aus $\mathcal{O}_\mathcal{E} = \mathbb{Z}_p \oplus \ker(\rho) = \ker(\varphi - 1) \oplus \ker(\rho)$ und der $\mathbb{Z}_p$-Linearität von $(\varphi - 1)_{|_{\ker(\rho)}}$. Für die Stetigkeit von $(\varphi - 1)^{-1}_{|_{\ker(\rho)}}$ genügt es zu zeigen, dass für alle $f \in \ker(\rho)$ die p-adische Bewertung von $(\varphi - 1)(f)$ mit der von f übereinstimmt. Sei dafür $f = p^m u \in \ker(\rho)$ mit $m \geq 0$ und $u \in \mathcal{O}_\mathcal{E}^* \cap \ker(\rho)$. Angenommen $(\varphi - 1)(u) \in p\mathcal{O}_\mathcal{E}$, d.h.

$$u + p\mathcal{O}_\mathcal{E} \in \ker(E \xrightarrow{\varphi-1} E) = \mathbb{F}_p = \mathbb{Z}_p/p\mathbb{Z}_p.$$

Dann existiert ein $a \in \mathbb{Z}_p$ mit $u - a \in p\mathcal{O}_\mathcal{E}$. Da aber $u = \sum_{n\in\mathbb{Z}} a_n t^n$ und $u - a = (a_0 - a) + \sum_{n\in\mathbb{Z}\setminus\{0\}} a_n t^n \in p\mathcal{O}_\mathcal{E}$, muss $a_n \in pW$ für alle $n \neq 0$ und $a_0 - a \in pW = p\mathbb{Z}_p \oplus \left(\bigoplus_{i=1}^r p\mathbb{Z}_p x_i\right)$ gelten. Daraus erhält man wegen $u \in \ker(\rho)$, also $a_0 \in \bigoplus_{i=1}^r \mathbb{Z}_p x_i$, und $a \in \mathbb{Z}_p$, dass bereits $a \in p\mathbb{Z}_p$ und $a_0 \in \bigoplus_{i=1}^r p\mathbb{Z}_p x_i$ gelten muss. Insbesondere ist damit $a_0 \in pW$ und deshalb

$$u = \sum_{n\in\mathbb{Z}} a_n t^n \in p\mathcal{O}_\mathcal{E},$$

was ein Widerspruch zu $u \in \mathcal{O}_\mathcal{E}^* = \mathcal{O}_\mathcal{E} \setminus p\mathcal{O}_\mathcal{E}$ ist. Also ändert $(\varphi - 1)_{|_{\ker(\rho)}}$ die p-adische Bewertung nicht, was bedeutet, dass $(\varphi - 1)_{|_{\ker(\rho)}}: \ker(\rho) \to (\varphi - 1)\mathcal{O}_\mathcal{E}$ ein Homöomorphismus ist. Aufgrund der Abgeschlossenheit von $\ker(\rho) \subset \mathcal{O}_\mathcal{E}$ ist somit auch $(\varphi - 1)\mathcal{O}_\mathcal{E} \subset \mathcal{O}_\mathcal{E}$ abgeschlossen bzgl. der p-adischen Topologie. □

Nun haben wir all unser Werkzeug zusammen, um das explizite Reziprozitätsgesetz von Fontaine-Witt zu beweisen.

Satz 7.51 (Explizites Reziprozitätsgesetz von Fontaine-Witt)**.**
Sei $u \in E^*$ und $x \in \mathcal{O}_\mathcal{E}$, dann gilt:

$$[x, u) = Tr_{K|\mathbb{Q}_p}(res(x \cdot d_{log}(Col(u)))) \text{ in } \mathbb{Z}_p.$$

Beweis. Behauptung 1: Die Gleichung gilt für alle $x \in (\varphi - 1)\mathcal{O}_\mathcal{E}$.
Sei dafür $x \in (\varphi - 1)\mathcal{O}_\mathcal{E}$, d.h. $x = (\varphi - 1)(\tilde{x})$ für ein $\tilde{x} \in \mathcal{O}_\mathcal{E}$. Dann ist nach der Bemerkung vor Lemma 7.38 entsprechend $\delta_\mathcal{E}(x) = 0$ und somit $[x, u) = \delta_\mathcal{E}(x)((u, E)) = 0$.

Man beachte, dass nach Satz 1.33 (ii) die Galoisgruppe $Gal(K|\mathbb{Q}_p) \cong Gal(k|\mathbb{F}_p)$ zyklisch ist. Des Weiteren erhalten wir aus Satz 1.33 (iii), dass die Einschränkung $(\varphi : \mathcal{E} \to \mathcal{E})_{|_K}$ ein Erzeuger der Galoisgruppe $Gal(K|\mathbb{Q}_p)$ ist. Der Einfachheit halber schreiben wir deshalb $Gal(K|\mathbb{Q}_p) = \langle\varphi\rangle$. Damit ist aufgrund der Additivität von $Tr_{K|\mathbb{Q}_p}$ und *res* auch die rechte Seite der Gleichung 0, denn

$$
\begin{aligned}
&Tr_{K|\mathbb{Q}_p}(res(x \cdot d_{log}(Col(u)))) = Tr_{K|\mathbb{Q}_p}(res((\varphi - 1)(\tilde{x}) \cdot d_{log}(Col(u))))\\
&= Tr_{K|\mathbb{Q}_p}(res(\varphi(\tilde{x}) \cdot d_{log}(Col(u)))) - Tr_{K|\mathbb{Q}_p}(res(\tilde{x} \cdot d_{log}(Col(u))))\\
&= Tr_{K|\mathbb{Q}_p}(\varphi(res(\tilde{x} \cdot d_{log}(Col(u))))) - Tr_{K|\mathbb{Q}_p}(res(\tilde{x} \cdot d_{log}(Col(u)))), \text{ nach 7.28,}\\
&= \sum_{i=0}^{[K:\mathbb{Q}_p]-1} \varphi^{i+1}(res(\tilde{x} \cdot d_{log}(Col(u)))) - Tr_{K|\mathbb{Q}_p}(res(\tilde{x} \cdot d_{log}(Col(u)))), \text{ da } Gal(K|\mathbb{Q}_p) = \langle\varphi\rangle,\\
&= \sum_{i=0}^{[K:\mathbb{Q}_p]-1} \varphi^{i}(res(\tilde{x} \cdot d_{log}(Col(u)))) - Tr_{K|\mathbb{Q}_p}(res(\tilde{x} \cdot d_{log}(Col(u)))), \text{ da } \varphi^{[K:\mathbb{Q}_p]} = id = \varphi^0,\\
&= Tr_{K|\mathbb{Q}_p}(res(\tilde{x} \cdot d_{log}(Col(u)))) - Tr_{K|\mathbb{Q}_p}(res(\tilde{x} \cdot d_{log}(Col(u))))\\
&= 0
\end{aligned}
$$

Behauptung 2: Wir dürfen ohne Einschränkung annehmen, dass $x + p\mathcal{O}_\mathcal{E} \notin (\varphi - 1)E$.
Wir zeigen dafür zunächst, dass beide Seiten der Gleichung für ein festes $u \in E^*$ $\mathbb{Z}_p$-linear sind. Die $\mathbb{Z}_p$-Linearität der rechten Seite sieht man recht einfach, da $Tr_{K|\mathbb{Q}_p}$ $\mathbb{Q}_p$-linear, *res* K-linear und $\mathbb{Z}_p \subset \mathbb{Q}_p \subset K$ ist. Für die linke Seite schauen wir nochmal, wie $\delta_\mathcal{E}(x)$ genau definiert ist. In Lemma 7.31 haben wir gesehen, dass für $x \in \mathcal{O}_\mathcal{E}$ ein $y \in \mathcal{O}_\breve{\mathcal{E}}$ mit $(\varphi - 1)(y) = -x$ existiert. Für ein $\alpha \in \mathbb{Z}_p$ ist wegen der $\mathbb{Z}_p$-Linearität von $\varphi - 1$ somit auch $(\varphi - 1)(\alpha y) = -(\alpha y)$. Da $\mathbb{Z}_p \subset \mathcal{O}_\mathcal{E} = (\mathcal{O}_\breve{\mathcal{E}})^{G_E}$ und $(u, E) \in G_E$ gilt nach Lemma 7.36 schließlich

$$
\begin{aligned}
[\alpha x, u) = \delta_\mathcal{E}(\alpha x)((u, E)) = (u, E)(\alpha y) - \alpha y = \alpha(u, E)(y) - \alpha y\\
= \alpha((u, E)(y) - y) = \alpha\delta_\mathcal{E}(x)((u, E)) = \alpha[x, u).
\end{aligned}
$$

Damit ist auch die linke Seite der Gleichung $\mathbb{Z}_p$-linear für festes $u \in E^*$. Nach Behauptung 1 dürfen wir $x \notin (\varphi - 1)\mathcal{O}_\mathcal{E}$ annehmen. Außerdem existiert wegen Lemma 7.50 ein $m \geq 0$ mit $(x + p^m\mathcal{O}_\mathcal{E}) \cap (\varphi - 1)\mathcal{O}_\mathcal{E} = \varnothing$. Lässt sich x schreiben als $x = (\varphi - 1)(y_1) + px_1$ mit $y_1, x_1 \in \mathcal{O}_\mathcal{E}$, so genügt es wegen Behauptung 1 und der $\mathbb{Z}_p$-Linearität der beiden Seiten die Gleichung nur für x_1 zu beweisen. Können wir wiederum auch x_1 in der Form $x_1 = (\varphi - 1)(y_2) + px_2$ mit $y_2, x_2 \in \mathcal{O}_\mathcal{E}$ schreiben, so ist $x = (\varphi - 1)(y_1 + py_2) + p^2x_2$ und es genügt aus den gleichen Gründen wie zuvor, die Gleichung für x_2 zu zeigen. Man beachte hierbei, dass spätestens nach $m - 1$ Schritten $(x_{m-1} + p^m\mathcal{O}_\mathcal{E}) \cap (\varphi - 1)\mathcal{O}_\mathcal{E} = \varnothing$

gilt, da sonst $(x + p^m\mathcal{O}_\mathcal{E}) \cap (\varphi - 1)\mathcal{O}_\mathcal{E} \neq \varnothing$, was ein Widerspruch zur Wahl von m wäre. Also können wir ohne Einschränkung annehmen, dass die Restklasse $x + p\mathcal{O}_\mathcal{E}$ nicht in $(\varphi - 1)E$ liegt.

Behauptung 3: Wegen der Separiertheit von $\mathbb{Z}_p$ genügt es

$$[x, u) \equiv Tr_{K|\mathbb{Q}_p}(res(x \cdot d_{log}(Col(u)))) \mod p^n\mathbb{Z}_p$$

für beliebiges $n \geq 1$ zu zeigen.
Sei also ohne Einschränkung $x \in \mathcal{O}_\mathcal{E}$ mit $x + p\mathcal{O}_\mathcal{E} \notin (\varphi - 1)E$ und wähle $y \in \mathcal{O}_\mathcal{E}$ mit $(\varphi - 1)(y) = x$ (vgl. Lemma 7.31), sowie $n \geq 1$ beliebig. Wie zuvor seien

- $(x_0, \ldots, x_{n-1})$ bzw. $(y_0, \ldots, y_{n-1})$ die Bilder von x bzw. y in $W_n(E)$ bzw. $W_n(E^{sep})$;
- $\delta_\mathcal{E}(x)_n : G_E \xrightarrow{\delta_\mathcal{E}(x)} \mathbb{Z}_p \to \mathbb{Z}_p/p^n\mathbb{Z}_p \cong \frac{1}{p^n}\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$;
- $E_n := (E^{sep})^{\ker(\delta_\mathcal{E}(x)_n)} = E[y_0, \ldots, y_{n-1}]$ (vgl. Satz 7.45);
- $\chi_n : G_{E_n|E} \hookrightarrow \mathbb{Q}/\mathbb{Z}$ der durch $\delta_\mathcal{E}(x)_n$ induzierte Charakter.

Per Definition von $(\cdot, E) : E^* \hookrightarrow {G_E}^{ab}$ und $(\cdot, E_n|E) : E^* \to {G_{E_n|E}}^{ab} = G_{E_n|E}$ haben wir das kommutative Diagramm

$$\begin{array}{ccc} E^* & \xrightarrow{(\cdot,E)} & {G_E}^{ab} = \varprojlim_{\substack{E'|E \text{ endl.} \\ \text{abelsch}}} G_{E'|E} \\ \Big\downarrow{\scriptstyle can} & \searrow^{(\cdot,E_n|E)} & \Big\downarrow{\scriptstyle proj_{E_n}} \\ E^*/N_{E_n|E}(E_n^*) & \xrightarrow[rec_{E_n|E}]{} & G_{E_n|E}, \end{array}$$

wobei $rec_{E_n|E} : E^*/N_{E_n|E}(E_n^*) \xrightarrow{\sim} {G_{E_n|E}}^{ab} = G_{E_n|E}$ den Reziprozitätsisomorphismus der zyklischen Erweiterung $E_n|E$ aus Definition 4.7 bezeichnet. Wir wählen nun $U := Col(u) \in (\mathcal{O}_\mathcal{E})^{N_\varphi} \subset \mathcal{O}_\mathcal{E}^* \subset \mathcal{O}_\mathcal{E}$ als Lift von u und $A_j \in \mathcal{O}_\mathcal{E}$ mit $A_j + p\mathcal{O}_\mathcal{E} = x_j \in E$ für alle $j \in \{0, \ldots, n-1\}$.

Dann gilt:

$$\begin{aligned}
&\frac{1}{p^n}[x,u)+\mathbb{Z}_p = \delta_{\mathcal{E}}(x)_n((u,E))\\
&\quad = \chi_n((u,E_n|E)), \text{ wegen des kommutativen Diagramms,}\\
&\quad = inv_{E_n|E}(\bar{u}\cup\delta_1(\chi_n)), \text{ nach 4.8 mit } \bar{u} := u\cdot N_{E_n|E}(E_n^*)\in E^*/N_{E_n|E}(E_n^*),\\
&\quad = inv_{E_n|E}((u\mid x_0,\dots x_{n-1}]), \text{ nach 7.47 und da } x_0 = x \mod p\mathcal{O}_{\mathcal{E}}\notin(\varphi-1)E \ (*),\\
&\quad = Tr_{K|\mathbb{Q}_p}\left(res\left(\left(\sum_{j=0}^{n-1}p^{j-n}A_j^{p^{n-1-j}}\right)\cdot d_{log}(Col(u))\right)\right)+\mathbb{Z}_p, \text{ nach Satz 7.48,}\\
&\quad = \frac{1}{p^n}Tr_{K|\mathbb{Q}_p}\left(res\left(\left(\sum_{j=0}^{n-1}p^{j}A_j^{p^{n-1-j}}\right)\cdot d_{log}(Col(u))\right)\right)+\mathbb{Z}_p,
\end{aligned}$$

da $Tr_{K|\mathbb{Q}_p}$ und res beide $\mathbb{Q}_p$-linear sind.

Zu $(*)$: Die Einbettung $\mathcal{O}_{\mathcal{E}}\hookrightarrow W(E)$ ist gegeben durch

$$\mathcal{O}_{\mathcal{E}}\xrightarrow{(a\mapsto(\varphi^m(a))_{m\geq 0})}\mathrm{im}(\Phi_{\mathcal{O}_{\mathcal{E}}})\xrightarrow{\Phi_{\mathcal{O}_{\mathcal{E}}}^{-1}}W(\mathcal{O}_{\mathcal{E}})\xrightarrow{W(can)}W(\mathcal{O}_{\mathcal{E}}/p\mathcal{O}_{\mathcal{E}})=W(E).$$

Seien $X_i\in\mathcal{O}_{\mathcal{E}}$ mit $\Phi_{\mathcal{O}_{\mathcal{E}}}^{-1}((\varphi^m(x))_{m\geq 0})=(X_i)_{i\geq 0}\in W(\mathcal{O}_{\mathcal{E}})$, d.h. $X_i \mod p\mathcal{O}_{\mathcal{E}} = x_i$ für alle $i\geq 0$. Durch Anwenden von $\Phi_{\mathcal{O}_{\mathcal{E}}}$ erhält man

$$(\varphi^m(x))_{m\geq 0}=\Phi_{\mathcal{O}_{\mathcal{E}}}((X_i)_{i\geq 0})=(\Phi_m(X_0,\dots,X_m))_{m\geq 0}$$

und somit insbesondere $x=\varphi^0(x)=\Phi_0(X_0)=X_0$. Also ist $x \mod p\mathcal{O}_{\mathcal{E}} = X_0 \mod p\mathcal{O}_{\mathcal{E}} = x_0$.

Betrachte nun den Ringhomomorphismus $\iota_n\colon\mathcal{O}_{\mathcal{E}}\hookrightarrow W(E)\twoheadrightarrow W_n(E)$. Dann ist $\ker(\iota_n)\subset\mathcal{O}_{\mathcal{E}}$ ein Ideal in $\mathcal{O}_{\mathcal{E}}$ und damit $\ker(\iota_n)=p^m\mathcal{O}_{\mathcal{E}}$ für ein $m\in\mathbb{N}\cup\{\infty\}$. Auf der einen Seite ist wegen $p^nW(E)\subset V_n(E)$ auch $p^n\mathcal{O}_{\mathcal{E}}\subset\ker(\iota_n)$ und deshalb $m\leq n$. Auf der anderen Seite ist aber auch $n\geq m$, denn

$$\iota_n(p^{n-1}\cdot 1)=p^{n-1}\iota_n(1)=p^{n-1}(1,0,\dots,0)+V_n(E)=(0,\dots,0,1)+V_n(E)\neq 0$$

in $W_n(E)$. Also ist $\ker(\iota_n)=p^n\mathcal{O}_{\mathcal{E}}$ und wir können $\mathcal{O}_{\mathcal{E}}/p^n\mathcal{O}_{\mathcal{E}}$ in $W_n(E)$ einbetten. Wegen Lemma 7.39 gilt dann in $W_n(E)$:

$$\varphi^{n-1}(x)+p^n\mathcal{O}_{\mathcal{E}}=F^{n-1}(x_0,\dots,x_{n-1})=(x_0^{p^{n-1}},\dots,x_{n-1}^{p^{n-1}})=\sum_{j=0}^{n-1}p^j\tau(x_j)^{p^{n-1-j}}$$

nach Lemma 5.14 (i), Lemma 5.15 (ii) und Satz 5.16 (i), wobei $\tau\colon E\to W(E)\twoheadrightarrow W_n(E)$ den Teichmüller-Lift bezeichnet. Es gilt allerdings wegen $A_j \mod p = x_j = \tau(x_j) \mod p$ und Lemma 1.21 auch

$$A_j^{p^{n-1-j}}\equiv\tau(x_j)^{p^{n-1-j}} \mod p^{n-j} \quad\text{bzw.}\quad p^jA_j^{p^{n-1-j}}\equiv p^j\tau(x_j)^{p^{n-1-j}} \mod p^n.$$

Mittels dem zuvor gezeigten erhält man damit

$$\sum_{j=0}^{n-1} p^j A_j^{p^{n-1-j}} \equiv \sum_{j=0}^{n-1} p^j \tau(x_j)^{p^{n-1-j}} \equiv \varphi^{n-1}(x) \mod p^n \mathcal{O}_{\mathcal{E}}.$$

Also gilt für unsere Gleichung:

$$\begin{aligned}
\frac{1}{p^n}[x,u) + \mathbb{Z}_p &= \frac{1}{p^n} Tr_{K|\mathbb{Q}_p}\left(res\left(\left(\sum_{j=0}^{n-1} p^j A_j^{p^{n-1-j}}\right) \cdot d_{log}\left(Col\left(u\right)\right)\right)\right) + \mathbb{Z}_p \\
&= \frac{1}{p^n} Tr_{K|\mathbb{Q}_p}\left(res\left(\varphi^{n-1}(x) \cdot d_{log}\left(Col\left(u\right)\right)\right)\right) + \mathbb{Z}_p \\
&= \frac{1}{p^n} Tr_{K|\mathbb{Q}_p}\left(\varphi^{n-1}\left(res\left(x \cdot d_{log}\left(Col\left(u\right)\right)\right)\right)\right) + \mathbb{Z}_p, \text{ nach 7.28,} \\
&= \frac{1}{p^n} Tr_{K|\mathbb{Q}_p}\left(res\left(x \cdot d_{log}\left(Col\left(u\right)\right)\right)\right) + \mathbb{Z}_p.
\end{aligned}$$

Dabei gilt die letzte Gleichheit aus den selben Gründen wie in Behauptung 1, denn $Gal(K|\mathbb{Q}_p) = \langle\varphi\rangle$. Die damit erhaltene Gleichung ist äquivalent zu

$$[x,u) \equiv Tr_{K|\mathbb{Q}_p}(res(x \cdot d_{log}(Col(u)))) \mod p^n\mathbb{Z}_p.$$

Da $\mathbb{Z}_p$ bzgl. der p-adischen Topologie separiert ist und $n \geq 1$ beliebig gewählt war, ist schließlich

$$[x,u) = Tr_{K|\mathbb{Q}_p}(res(x \cdot d_{log}(Col(u)))).$$

□

Literaturverzeichnis

[Ar] Artin, E.: *Algebraic Numbers and Algebraic Functions*, Gordon and Breach Science Publishers New York · London · Paris, 1967.
http://www.plouffe.fr/simon/math/Algebraic%20Numbers%20and%20Algebraic%20Functions%20-%20Artin.pdf

[Bo] Bosch, S.: *Algebra*, Springer-Verlag Berlin Heidelberg New York, 5. Auflage

[Fo1] Fontaine, J.-M.; Ouyang, Y.: *Theory of p-adic Galois Representations*
http://www.math.u-psud.fr/~fontaine/galoisrep.pdf

[Fo2] Fontaine, J.-M.: *Représentations p-adiques des corps locaux*
http://math.arizona.edu/~cais/847Page/References/Fontaine-Representations_p-adique_des_corpx_locaux.pdf

[Ke] Kersten, I.: *Brauergruppen*, Universitätsverlag Göttingen, 2007.
http://www.univerlag.uni-goettingen.de/bitstream/handle/3/isbn-978-3-938616-89-5/brauergruppen.pdf?sequence=3

[Lo1] Lorenz, F.: *Einführung in die Algebra I*, Spektrum Akademischer Verlag GmbH Heidelberg · Berlin, 3. Auflage, 1999.

[Lo2] Lorenz, F.: *Einführung in die Algebra II*, Spektrum Akademischer Verlag GmbH Heidelberg · Berlin · Oxford, 2. Auflage, 1997.

[Ne1] Neukirch, J.: *Algebraische Zahlentheorie*, Springer-Verlag Berlin Heidelberg New York, 1992.

[Ne2] Neukirch, J.; Schmidt, A.: *Klassenkörpertheorie*, Springer-Verlag Berlin Heidelberg New York, 4. Ausgabe, Mai 2015.
https://www.mathi.uni-heidelberg.de/~schmidt/Neukirch/

[Sch] Schneider, P.: *Theorie des Anstiegs*, Vorlesung an der Westfälischen Wilhelms-Universität Münster im Wintersemester 2006/2007.
http://wwwmath.uni-muenster.de/u/pschnei/publ/lectnotes/Theorie-des-Anstiegs.pdf

[Ser] Serre, J.-P.: *Local Fields*, Springer-Verlag New York Heidelberg Berlin, 1979.

[Wa] Warner, S.: *Topological Rings*, North-Holland - Amsterdam · London · New York · Tokyo, 1993.

[Wi] Witt, E.: *Zyklische Körper und Algebren der Charakteristik p vom Grad p^n. Struktur diskret bewerteter perfekter Körper mit vollkommenem Restklassenkörper der Charakteristik p.*, Journal für die reine und angewandte Mathematik, Band 176 (Seiten 126 - 140), 1937.
http://gdz.sub.uni-goettingen.de/en/dms/loader/img/?PPN=PPN243919689_0176&DMDID=DMDLOG_0016

Versicherung an Eides Statt

Ich, Julian Wilmer; Franziskastraße 44, 45131 Essen; Matrikelnummer: 2247977, versichere an Eides Statt durch meine Unterschrift, dass ich die vorstehende Arbeit selbstständig und ohne fremde Hilfe angefertigt und alle Stellen, die ich wörtlich oder annähernd wörtlich aus Veröffentlichungen entnommen habe, als solche kenntlich gemacht habe, mich auch keiner anderen als der angegebenen Literatur oder sonstiger Hilfsmittel bedient habe.
Ich versichere an Eides Statt, dass ich die vorgenannten Angaben nach bestem Wissen und Gewissen gemacht habe und dass die Angaben der Wahrheit entsprechen und ich nichts verschwiegen habe.
Die Strafbarkeit einer falschen eidesstattlichen Versicherung ist mir bekannt, namentlich die Strafandrohung gemäß §156 StGB bis zu drei Jahren Freiheitsstrafe oder Geldstrafe bei vorsätzlicher Begehung der Tat bzw. gemäß §163 Abs. 1 StGB bis zu einem Jahr Freiheitsstrafe oder Geldstrafe bei fahrlässiger Begehung.

_____	_____
Ort, Datum	Unterschrift (Julian Wilmer)