[chapter] [chapter] [chapter] [chapter] [chapter]

Universität Leipzig
Fakultät für Mathematik und Informatik
Mathematisches Institut

Das explizite Reziprozitätsgesetz im Falle einer zyklotomischen Erweiterung von $\mathbb{Q}_p$

Diplomarbeit
im Studiengang Diplom-Mathematik

überarbeitete Fassung

Leipzig, Februar 2003

vorgelegt von Rainer Munck,
geboren am 10. Mai 1976

Inhaltsverzeichnis

1 Einleitung **1**

2 Grundlagen **3**

2.1 Erweiterungen lokaler Körper 3

2.2 Die Logarithmus- und Exponentialfunktion 5

3 Lokale Klassenkörpertheorie **7**

3.1 Lokale Klassenkörpertheorie 7

3.2 Lokales Normrestsymbol und Kummertheorie 13

3.3 Hilbertsymbol und explizites Reziprozitätsgesetz 16

4 Vorbereitungen **20**

4.1 Die Logarithmus- und Exponentialfunktion in K_n 20

4.2 Zur Differente von K_n 22

4.3 Über Spuren und Normen 24

4.4 Das Potenzrestsymbol 29

4.5 Spezielle Eigenschaften des Hilbertsymbols 33

5 Das explizite Reziprozitätsgesetz **37**

5.1 Die beiden Ergänzungssätze 37

5.2 Das explizite Reziprozitätsgesetz 48

5.3 Weitere Resultate 72

6 Zerlegung unter Charakteren **76**

6.1 Allgemeines 76

6.2 Der Spezialfall $n = 0$ 79

6.3 Ausblick auf den Fall $n > 0$ 96

Kapitel 1

Einleitung

In seinen Disquisitiones arithmeticae von 1801 bewies C. F. Gauß das quadratische Reziprozitätsgesetz. Mit Hilfe dieses Gesetzes lässt sich entscheiden, ob eine ungerade Primzahl p ein quadratischer Rest modulo einer anderen ungeraden Primzahl p' ist.

In einem Erweiterungskörper F von $\mathbb{Q}$, der die m-ten Einheitswurzeln enthält, ist es das m-te Potenzrestsymbol, mit dessen Hilfe festgestellt werden kann, ob ein Element $u \in \mathcal{O}_F$ ein m-ter Potenzrest modulo eines Primideals $\mathfrak{p} \subseteq \mathcal{O}_F$ ist. Bedingung an $\mathfrak{p}$ ist, dass es über keinem Primteiler von m liegt. Es war also von Interesse, ein explizites Reziprozitätsgesetz für das m-te Potenzrestsymbol zu finden.

Da für ein Ideal $\mathfrak{b} \subseteq \mathcal{O}_F$ die Eindeutigkeit der Zerlegung in Primideale gilt, kann man das Potenzrestsymbol auf multiplikative Art und Weise auf zusammengesetzte Ideale und insbesondere auch auf Hauptideale $(b) = b\mathcal{O}_F$ erweitern. In dem Fall, dass $m = p^n$ eine Primzahlpotenz ist, ist an die Hauptideale (b) die Bedingung zu stellen, dass sie prim zu dem über der Primzahl p liegenden Primideal $\mathfrak{p}$ sein müssen, dass also $\mathfrak{p}$ nicht in der Primidealzerlegung von (b) vorkommt.

Für diesen Fall, d.h. $F = \mathbb{Q}(\zeta)$ enthält die p^n-ten Einheitswurzeln und $b \in 1 + \mathfrak{p}$ ist prim zu $\mathfrak{p}$, bewiesen E. Artin und H. Hasse in ihrem Artikel [AHa] von 1928 die beiden Ergänzungssätze

$$\left(\frac{\zeta}{b}\right)_{p^n} = \zeta^{\frac{1}{p^n}\, S(\log b)} \quad \text{und} \quad \left(\frac{\pi}{b}\right)_{p^n} = \zeta^{-\frac{1}{p^n}\, S\left(\frac{\zeta}{\pi} \log b\right)}$$

zum p^n-ten Potenzrestsymbol. Dabei ist $\pi = 1 - \zeta$ ein Erzeuger von $\mathfrak{p}$ und S die Spurabbildung $F \to \mathbb{Q}$. Das Auffinden expliziter Formeln für allgemeine Potenzrestsymbole $\left(\frac{a}{b}\right)_{p^n}$ erwies sich jedoch als schwierig.

Eine Vereinfachung des Problems wurde durch die Arbeit mit lokalen Körpern erreicht. Betrachtet wird der Körper $K_n = \mathbb{Q}_p(\zeta)$, wobei ζ eine primitive p^{n+1}-te

Einheitswurzel ist. In diesem Körper definiert man das p^{n+1}-te Hilbertsymbol, welches mit dem p^{n+1}-ten Potenzrestsymbol in engem Zusammenhang steht.

Im Jahr 1968 bewies K. Iwasawa in seinem Artikel [Iwa2] eine allgemeine explizite Formel für das p^{n+1}-te Hilbertsymbol im Fall $p \neq 2$, wobei er die Resultate von Artin-Hasse verwendete. A. Kudo gab 1971 in [Kudo] ein Gesetz für das p^{n+1}-te Hilbertsymbol im Fall $p = 2$ an, welches analog zu Iwasawas explizitem Reziprozitätsgesetz ist.

Das Anliegen dieser Arbeit ist es, die bekannten expliziten Reziprozitätsgesetze für Hilbertsymbole in Erweiterungskörpern $\mathbb{Q}_p(\zeta)$ von $\mathbb{Q}_p$, wobei ζ eine primitive m-te Einheitswurzel ist, zu formulieren und zu beweisen. Dabei werden zwei Fälle unterschieden. Zum einen der Fall, dass m teilerfremd zu p ist (vgl. Abschnitt 3.3), und zum anderen der Fall, dass $m = p^{n+1}$ eine Potenz einer Primzahl $p \neq 2$ ist (vgl. Kapitel 5).

Nach dem Beweis des Zusammenhangs zwischen dem p^{n+1}-ten Potenzrestsymbol und dem p^{n+1}-ten Hilbertsymbol in Abschnitt 4.5, werden in Abschnitt 5.1 die beiden Ergänzungssätze für das p^{n+1}-te Hilbertsymbol im lokalen Körper K_n bewiesen. Die hergestellte Beziehung zwischen Potenzrest- und Hilbertsymbol ermöglicht es, den Beweis, der in [AHa] für das Potenzrestsymbol geführt wird, auf das Hilbertsymbol zu übertragen.

In Abschnitt 5.2 wird, dem Artikel [Iwa2] von Iwasawa folgend, das explizite Reziprozitätsgesetz für das p^{n+1}-te Hilbertsymbol im Körper K_n bewiesen.

Zur Vorbereitung all dieser Überlegungen wird in Kapitel 3 die lokale Klassenkörpertheorie behandelt. Sie bildet zusammen mit der Kummertheorie die Grundlage für die Definition des Hilbertsymbols.

Ein weiteres Resultat von K. Iwasawa ist die Existenz eines Homomorphismus ψ_n, welcher die explizite Formel des Reziprozitätsgesetzes vermittelt. In Kapitel 6 wird die Zerlegung dieses Homomorphismus unter Charakteren der Galoisgruppe $G(K_n/\mathbb{Q}_p)$ untersucht. Eine vollständige Behandlung dieses Themas für den Fall $n = 0$ erfolgt in Abschnitt 6.2. Ein Ausblick auf die Zerlegung von ψ_n für $n > 0$ wird in Abschnitt 6.3 gegeben.

Kapitel 2

Grundlagen

2.1 Erweiterungen lokaler Körper

Seien K ein lokaler Körper mit normierter Exponentialbewertung $\nu_K : K \twoheadrightarrow \mathbb{Z}$ und π_K ein fixiertes Primelement von K, d.h. es gilt $\nu_K(\pi_K) = 1$. Mit

$$\mathcal{O}_K = \big\{x \in K : \nu_K(x) \geq 0\big\} \quad \text{und} \quad \mathcal{O}_K^* = \big\{x \in K : \nu_K(x) = 0\big\}$$

seien der Bewertungsring bzw. seine Einheiten bezeichnet. Das maximale Ideal von $\mathcal{O}_K$ ist $\mathfrak{m}_K = \pi_K \mathcal{O}_K$.

Sei L/K eine Erweiterung vom Grad

$$[L : K] = n.$$

Die Bewertung ν_K von K hat eine eindeutige Fortsetzung auf L, gegeben durch

$$\nu_K(\alpha) = \frac{1}{n}\, \nu_K\big(N_{L/K}(\alpha)\big), \quad \alpha \in L,$$

(vgl. [Lor2], § 23, Satz 4). Man hat somit $\nu_K : L \to \frac{1}{n}\mathbb{Z}$. Das Bild von L unter dieser Abbildung ist eine Untergruppe von $\frac{1}{n}\mathbb{Z}$, welche die Gestalt $\frac{1}{e}\mathbb{Z}$ hat. Dabei ist $e \in \mathbb{N}$ ein Teiler von n. Die Zahl e heißt Verzweigungsindex der Erweiterung L/K. Folglich gilt für die normierte Exponentialbewertung $\nu_L : L \twoheadrightarrow \mathbb{Z}$

$$\nu_L = e\, \nu_K.$$

Elemente $\pi_L \in L$ mit $\nu_L(\pi_L) = 1$ heißen Primelemente von L, für ein Primelement π_L gilt

$$\pi_L^e = u\pi_K$$

mit einer Einheit $u \in \mathcal{O}_L^*$. Seien λ und κ die Restklassenkörper von L bzw. K, d.h. $\lambda = \mathcal{O}_L/\mathfrak{m}_L$ und $\kappa = \mathcal{O}_K/\mathfrak{m}_K$. Der Grad der Körpererweiterung λ/κ,

$$f = [\lambda : \kappa],$$

heißt Trägheitsgrad der Erweiterung L/K. Schreibt man $\kappa = \mathbb{F}_q$, so ist $\lambda = \mathbb{F}_{q^f}$. Zwischen dem Grad n der Erweiterung L/K, dem Verzweigungsindex e und dem Trägheitsgrad f besteht die Beziehung

$$n = ef$$

(vgl. [Lor2], § 24, Satz 1). Im Fall $n = f,\ e = 1$ heißt die Erweiterung L/K unverzweigt, im Fall $n = e,\ f = 1$ nennt man sie sie rein verzweigt.

Zu jeder endlichen Erweiterung L/K existiert ein Zwischenkörper $\widetilde{K}$, so dass $[\widetilde{K} : K] = f$ und $[L : \widetilde{K}] = e$. Dieser Körper $\widetilde{K}$ heißt maximal unverzweigte Erweiterung von K (vgl. [Lor2], § 24, Satz 3 (iv)).

Ist L/K eine endliche unverzweigte Erweiterung, so ist L/K galoissch. Für die Galoisgruppe gilt

$$G(L/K) \cong G(\lambda/\kappa) \cong G(\mathbb{F}_{q^f}/\mathbb{F}_q).$$

Die Gruppe auf der rechten Seite ist zyklisch und wird von dem Automorphismus $\varphi : x \mapsto x^q$ erzeugt. Das φ entsprechende Element $\varphi_{L/K}$ aus $G(L/K)$ heißt Frobeniusautomorphismus von L/K (vgl. [Lor2], § 24, Satz 4 (iii) und [Neu], Kap.II, § 7, Satz (7.12) (ii)).

Da bei den Betrachtungen des Hilbertsymbols ein Körper zugrunde liegt, der die m-ten Einheitswurzeln enthält, soll nun die Frage untersucht werden, welche Einheitswurzeln bereits in $\mathbb{Q}_p$ enthalten sind. Allgemeiner wird gleich die Struktur von Einheitswurzel-Erweiterungen $\mathbb{Q}_p(\zeta)/\mathbb{Q}_p$ untersucht.

Satz 2.1 *Sei ζ_m eine primitive m-te Einheitswurzel.*

(i) *Im Fall $(m, p) = 1$ ist $\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p$ eine unverzweigte Erweiterung vom Grad f, wobei f der kleinste Exponent ist, für den $m \,\big|\, (p^f - 1)$ gilt* (vgl. [Neu], Kap.II, § 7, Satz (7.12)).

(ii) *Ist $m = p^k$ eine p-Potenz, so ist $\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p$ eine rein verzweigte Erweiterung vom Grad $e = \varphi(m) = (p-1)p^{k-1}$. Das Element $\pi = 1 - \zeta_m$ ist ein Primelement von $\mathbb{Q}_p(\zeta_m)$.*

Insbesondere enthält $\mathbb{Q}_p$ im Fall $m \,\big|\, (p-1)$ alle m-ten Einheitswurzeln.

Beweis von (ii): Sei $m = p^k$ eine p-Potenz. Das Minimalpolynom von ζ_m über $\mathbb{Q}_p$ ist das p^k-te Kreisteilungspolynom (vgl. [Lor1], § 9, Beweis von Satz 3' und nachfolgende Bemerkung)

$$f(X) = \frac{X^{p^k} - 1}{X^{p^{k-1}} - 1} = 1 + X^{p^{k-1}} + X^{2p^{k-1}} + \ldots + X^{(p-1)p^{k-1}},$$

woraus ersichtlich ist, dass

$$n := [\mathbb{Q}_p(\zeta_m) : \mathbb{Q}_p] = (p-1)p^{k-1}.$$

Sei $\pi = 1 - \zeta_m$. Dann ist π Nullstelle des Polynoms

$$g(X) = f(1-X) = \sum_{j=0}^{p-1} (1-X)^{jp^{k-1}}.$$

Wegen $\pi = 1 - \zeta_m$ und $\zeta_m = 1 - \pi$ gilt $\mathbb{Q}_p(\zeta_m) = \mathbb{Q}_p(\pi)$. Somit ist g das Minimalpolynom von π über $\mathbb{Q}_p$, denn es ist normiert und hat den richtigen Grad. Das Absolutglied von g ist

$$g(0) = f(1) = p,$$

demnach gilt $N_{\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p}(\pi) = p$. Sei mit ν die eindeutige Fortsetzung der p-adischen Bewertung v_p von $\mathbb{Q}_p$ auf $\mathbb{Q}_p(\zeta_m)$ bezeichnet. Dann ergibt sich

$$\nu(\pi) = \frac{1}{n}\, v_p\big(N_{\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p}(\pi)\big) = \frac{1}{n}\, v_p(p) = \frac{1}{n}.$$

Im allgemeinen ist ν eine Abbildung $\nu : \mathbb{Q}_p(\zeta_m) \twoheadrightarrow \frac{1}{e}\mathbb{Z}$, wobei e, der Verzweigungsindex der Erweiterung $\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p$, ein Teiler von n ist. Da mit π ein Element gefunden ist, für das $\nu(\pi) = \frac{1}{n}$ gilt, ist gezeigt, dass $e = n$ ist. Somit ist $\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p$ eine rein verzweigte Erweiterung. Außerdem ist damit bewiesen, dass π ein Primelement von $\mathbb{Q}_p(\zeta_m)$ ist, da es minimale Bewertung hat.

QED

2.2 Die Logarithmus- und Exponentialfunktion

In diesem Abschnitt werden die Logarithmus- und Exponentialfunktion auf einem lokalen Körper eingeführt und eine wichtige Eigenschaft dieser Funktionen angegeben.

Satz 2.2 *Sei $K/\mathbb{Q}_p$ eine endliche Körpererweiterung. Das maximale Ideal im Bewertungsring $\mathcal{O}_K$ sei mit $\mathfrak{m}_K$ bezeichnet. Dann gibt es einen eindeutig bestimmten, stetigen Homomorphismus*

$$\log : K^* \to K$$

mit $\log p = 0$, der für $1 - x \in (1 + \mathfrak{m}_K)$ die Reihendarstellung

$$\log(1-x) = -\sum_{k \geq 1} \frac{x^k}{k}$$

besitzt. Insbesondere gilt $\log(xy) = \log(x) + \log(y)$ für $x, y \in (1 + \mathfrak{m}_K)$ (vgl. [Neu], Kap.II, § 5, Satz (5.4) und Beweis).

Aus der Funktionalgleichung folgt für eine Einheitswurzel ζ in K, dass $\log(\zeta) = 0$.

Satz 2.3 *Sei* $\exp(x) := \sum_{k\geq 0} \frac{x^k}{k!}$. *Für eine endliche Erweiterung* $K/\mathbb{Q}_p$ *mit Verzweigungsindex* e *sind* exp *und* log *im Fall* $r > \frac{e}{p-1}$ *zueinander inverse Isomorphismen*

$$\exp : \mathfrak{m}_K^r \to (1 + \mathfrak{m}_K^r), \quad \log : (1 + \mathfrak{m}_K^r) \to \mathfrak{m}_K^r,$$

(vgl. [Neu], Kap.II, § 5, Satz (5.5)).

Kapitel 3

Lokale Klassenkörpertheorie

In dem folgenden Kapitel wird die lokale Klassenkörpertheorie (Theorem 3.7) vorgestellt. Zusammen mit der Kummertheorie (Satz 3.10) bildet sie die Grundlage für die Definition des Hilbertsymbols. Zum Abschluss des Kapitels wird das explizite Reziprozitätsgesetz im teilerfremden Fall $(m, p) = 1$ bewiesen (Theorem 3.12).

3.1 Lokale Klassenkörpertheorie

Die Hauptaussage der lokalen Klassenkörpertheorie ist die Existenz eines Isomorphismus

$$r_{L/K} : G(L/K) \to K^*/N_{L/K}L^*$$

für eine endliche abelsche Galois-Erweiterung L/K lokaler Körper. Dabei bezeichnet $N_{L/K} : L \to K$ die Normabbildung. Für eine nicht-abelsche Erweiterung hat man einen Isomorphismus

$$r_{L/K} : G(L/K)^{ab} \to K^*/N_{L/K}L^*,$$

wobei $G(L/K)^{ab} = G(L/K)/G'(L/K)$ die größte abelsche Faktorgruppe ist. Mit $G'(L/K)$ ist die Kommutatoruntergruppe von $G(L/K)$ bezeichnet. Die Faktorgruppe $G(L/K)^{ab}$ korrespondiert mit der größten abelschen Teilerweiterung L^{ab}/K von L/K.

Ausgangspunkt der folgenden Betrachtungen ist ein lokaler Körper k mit endlichem Restklassenkörper $\kappa = \mathbb{F}_q$. Sei $\bar{k}$ der separable Abschluss des Körpers k. Dann ist $\bar{k}/k$ eine unendliche Galois-Erweiterung, die alle endlichen galoisschen Erweiterungen K/k umfasst. Die Galois-Gruppe

$$G := G(\bar{k}/k)$$

ist eine pro-endliche Gruppe, und zwar als projektiver Limes der Gruppen $G(K/k)$, wobei K/k alle endlichen galoisschen Teilerweiterungen von $\bar{k}/k$ durchläuft,

$$G \cong \varprojlim_K G(K/k).$$

Der projektive Limes wird bezüglich der Einschränkungsabbildungen

$$G(K'/k) \to G(K/k), \quad \tau \mapsto \tau_{|K}$$

gebildet, wobei $K \subseteq K'$. Versieht man die endlichen Galoisgruppen $G(K/k)$ mit der diskreten Topologie, d.h. der Topologie, die durch die Potenzmenge gegeben ist, und betrachtet die Produkttopologie auf $\prod_K G(K/k)$, so wird der projektive Limes

$$G \subseteq \prod_{\substack{K/k \\ endl. \\ gal.}} G(K/k)$$

als Teilmenge des Produkts zu einer topologischen Gruppe. Diese Topologie heißt Krulltopologie. In ihr ist durch

$$\big\{\sigma G(\bar{k}/K),\ K/k \text{ endlich, galoissch}\big\}$$

eine offene Umgebungsbasis des Elementes $\sigma \in G(\bar{k}/k)$ gegeben (vgl. [Lor1], § 12, F5 und Definition davor, und [Neu], Kap. IV, § 1, Ausführungen vor Satz (1.1)). Das Einselement besitzt somit eine Umgebungsbasis, die aus lauter Normalteilern besteht.

Satz 3.1 (Hauptsatz der Galoistheorie) *Die Zuordnung*

$$F \longleftrightarrow G(\bar{k}/F) =: G_F$$

von Zwischenkörpern F von $\bar{k}/k$ zu den abgeschlossenen Untergruppen G_F von $G(\bar{k}/k)$ ist eineindeutig. Der Körper F ist der Fixkörper der Gruppe G_F (vgl. [Lor1], § 12, Satz 4).

Lemma 3.2 *Jede offene Untergruppe H von $G = G(\bar{k}/k)$ ist abgeschlossen. Eine Untergruppe von G ist genau dann offen, wenn sie endlichen Index in G hat.*

Beweis: Sei $H \subseteq G$ eine offene Untergruppe. Dann ist ihr Komplement als Vereinigung der offenen Nebenklassen $\sigma H,\ \sigma \in G,\ \sigma \neq id$, ebenfalls offen. Also ist H abgeschlossen.
Sei H offen mit Zwischenkörper F, d.h. $H = G(\bar{k}/F)$. Dann gilt

$$G/H \cong G(\bar{k}/k)/G(\bar{k}/F) \cong G(F/k). \tag{3.1}$$

Da H offen ist, enthält es eine Menge $G(\bar{k}/L)$, wobei L/k endlich und abelsch ist. Aus $G(\bar{k}/L) \subseteq G(\bar{k}/F) = H$ folgt $F \subseteq L$. Somit sind auch F/k und $G(F/k)$ endlich, d.h. H hat endlichen Index in G.
Sei jetzt H eine abgeschlossene Teilmenge mit endlichem Index in G und Fixkörper F. Durch Anwendung von Gleichung (3.1) auf diese Situation folgt die Endlichkeit von $G(F/k)$ und somit ist auch die Endlichkeit von F/k. Sei $\hat{F}$ die normale Hülle von F. Dann ist die Erweiterung $\hat{F}/k$ endlich und galoissch. Aus $F \subseteq \hat{F}$ folgt $G(\bar{k}/\hat{F}) \subseteq G(\bar{k}/F) = H$. Da $G(\bar{k}/\hat{F})$ offen ist, ist auch H als Vereinigung der offenen Nebenklassen $\sigma G(\bar{k}/\hat{F}),\ \sigma \in G(\bar{k}/F),\ \sigma \neq id$, offen.

QED

Sei $\tilde{k}/k$ die maximal unverzweigte Erweiterung von $\bar{k}/k$, d.h. $\tilde{k}$ ist das Kompositum aller unverzweigten Erweiterungen von k (vgl. [Neu], Kap.II, § 7, Definition (7.4)). Dann gilt

$$G(\tilde{k}/k) \cong G(\overline{\mathbb{F}}_q/\mathbb{F}_q) \tag{3.2}$$

(vgl. [Neu], Kap.II, § 7, Satz (7.5)). Für eine endliche Erweiterung $\mathbb{F}_{q^n}/\mathbb{F}_q$ ist $G(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$. Bei diesem Isomorphismus wird die 1 auf den Automorphismus $x \mapsto x^q$ abgebildet. Sei

$$\widehat{\mathbb{Z}} := \varprojlim_n \mathbb{Z}/n\mathbb{Z}$$

der projektive Limes der $\mathbb{Z}/n\mathbb{Z}$ bezüglich der Projektionen $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z},\ m|n$. Dann besteht die Isomorphie $G(\overline{\mathbb{F}}_q/\mathbb{F}_q) \cong \widehat{\mathbb{Z}}$, also

$$\iota : G(\tilde{k}/k) \cong \widehat{\mathbb{Z}} \tag{3.3}$$

(vgl. [Neu], Kap.IV, § 2, Beispiele 4 und 5). Mit Hilfe des Chinesischen Restsatzes $\mathbb{Z}/n\mathbb{Z} \cong \prod_p \mathbb{Z}/p^{\nu_p(n)}\mathbb{Z}$ erhält man für $\widehat{\mathbb{Z}}$ die alternative Darstellung

$$\widehat{\mathbb{Z}} \cong \prod_{p\ prim} \mathbb{Z}_p.$$

Versieht man $\widehat{\mathbb{Z}}$ in analoger Weise wie G mit einer Topologie, d.h. die endlichen Gruppen $\mathbb{Z}/n\mathbb{Z}$ werden mit der diskreten Topologie versehen und $\widehat{\mathbb{Z}}$ erhält die induzierte Topologie des direkten Produktes, so ergeben sich als die offenen Untergruppen von $\widehat{\mathbb{Z}}$ genau die Untergruppen $n\widehat{\mathbb{Z}},\ n \in \mathbb{N}$ (vgl. [Neu], Kap.IV, § 2, Beispiel 4).

Als Resultat dieser Betrachtungen erhält man einen surjektiven Homomorphismus

$$d : G(\bar{k}/k) \twoheadrightarrow \widehat{\mathbb{Z}}$$

mit Kern I. Da $I \subseteq G(\bar{k}/k)$ eine abgeschlossene Untergruppe ist, hat I die Gestalt $I = G(\bar{k}/F)$ mit einem Zwischenkörper F. Es gilt

$$G(\tilde{k}/k) \cong \widehat{\mathbb{Z}} \cong G(\bar{k}/k)/I \cong G(F/k),$$

woraus $F = \tilde{k}$ folgt. Folglich ist $I = G(\bar{k}/\tilde{k})$.

Lemma 3.3 *Der Homomorphismus d ist stetig.*

BEWEIS: Der Homomorphismus d ist die Hintereinanderausführung der Einschränkungsabbildung $\rho : G(\bar{k}/k) \to G(\tilde{k}/k)$ und des Isomorphismus ι aus Gleichung (3.3),

$$d : G(\bar{k}/k) \xrightarrow{\rho} G(\tilde{k}/k) \xrightarrow{\iota} \widehat{\mathbb{Z}}.$$

Um die Stetigkeit von d zu zeigen, genügt es, die Stetigkeit der Abbildungen ι und ρ zu zeigen. Zuvor sei angemerkt, dass die von $G(\bar{k}/k)$ auf $G(\tilde{k}/k)$ induzierte Topologie die Krulltopologie von $G(\tilde{k}/k)$ ist (vgl. [Lor1], § 12, Ende der Bemerkungen nach Satz 4).
Für das Urbild $\iota^{-1}\big(n\widehat{\mathbb{Z}}\big)$ einer offenen Untergruppe $n\widehat{\mathbb{Z}}$ von $\widehat{\mathbb{Z}}$ gilt

$$G(\tilde{k}/k)/\iota^{-1}(n\widehat{\mathbb{Z}}) \cong \widehat{\mathbb{Z}}/n\widehat{\mathbb{Z}} \cong \mathbb{Z}/n\mathbb{Z}.$$

Es hat demnach endlichen Index in $G(\tilde{k}/k)$ und ist somit offen. Folglich ist ι stetig.
Sei $G(\tilde{k}/K)$ ein Element der offenen Basisumgebung der Eins in $G(\tilde{k}/k)$, d.h. K/k ist endlich und galoissch. Das Urbild dieser Menge unter der Abbildung ρ ist die Menge $G(\bar{k}/K)$, welche ein Element der offenen Basisumgebung der Eins in $G(\bar{k}/k)$ ist. Somit ist auch ρ stetig.

QED

Für einen Zwischenkörper K werde die Abbildung

$$G(\bar{k}/K) \to \widehat{\mathbb{Z}} \tag{3.4}$$

betrachtet, welche durch Einschränkung von d auf $G(\bar{k}/K)$ entsteht. Diese Abbildung hat das Bild $f_K\widehat{\mathbb{Z}}$, wobei

$$f_K = \big|\, \widehat{\mathbb{Z}}/d\big(G(\bar{k}/K)\big) \,\big| \,.$$

Somit ist die Abbildung

$$d_K := \frac{1}{f_K}\, d : G(\bar{k}/K) \twoheadrightarrow \widehat{\mathbb{Z}}$$

surjektiv und hat denselben Kern wie (3.4), nämlich

$$I_K := G(\bar{k}/K) \cap I = G(\bar{k}/K) \cap G(\bar{k}/\tilde{k}) = G(\bar{k}/K\tilde{k}) = G(\bar{k}/\widetilde{K}).$$

Dabei bezeichnet $\widetilde{K}$ die maximal unverzweigte Erweiterung von K. Mit dieser Beziehung erhält man einen Isomorphismus

$$d_K : G(\widetilde{K}/K) \simeq \widehat{\mathbb{Z}}. \tag{3.5}$$

Das Element $\varphi_K \in G(\widetilde{K}/K)$ mit $d_K(\varphi_K) = 1 \in \widehat{\mathbb{Z}}$ heißt Frobenius über K. Somit kann man $G(\widetilde{K}/K)$ mit $\{\varphi_K^n,\ n \in \widehat{\mathbb{Z}}\}$ identifizieren. Für eine galoissche Erweiterung L/K sei $\mathrm{Frob}(\widetilde{L}/K)$ die Halbgruppe

$$\begin{aligned}\mathrm{Frob}(\widetilde{L}/K) &:= \left\{\sigma \in G(\widetilde{L}/K) : d_K(\sigma) \in \mathbb{N}\backslash\{0\}\right\} \\ &= \left\{\sigma \in G(\widetilde{L}/K) : \sigma_{|_{\widetilde{K}}} = \varphi_K^n,\ n \in \mathbb{N}\backslash\{0\}\right\} \ \subseteq\ G(\widetilde{L}/K).\end{aligned}$$

Ist die Erweiterung L/K endlich, so ist die Abbildung

$$\mathrm{Frob}(\widetilde{L}/K) \twoheadrightarrow G(L/K)$$

surjektiv (vgl. [Neu], Kap.IV, § 4, Satz (4.4)). Somit kann jedes $\sigma \in G(L/K)$ zu einem $\widetilde{\sigma} \in \mathrm{Frob}(\widetilde{L}/K)$ angehoben werden. Dieses $\widetilde{\sigma}$ ist dann der Frobenius über seinem Fixkörper Σ, d.h. $\widetilde{\sigma} = \varphi_\Sigma$ (vgl. [Neu], Kap.IV, § 4, Satz (4.5)). Dabei ist der Fixkörper zu einem Element $\tau \in G(\bar{k}/k)$ als der Fixkörper des Abschlusses $\overline{\langle\tau\rangle}$ der von τ erzeugten Untergruppe $\{\tau^n,\ n \in \mathbb{Z}\} \subseteq G(\bar{k}/k)$ definiert.

Für eine endliche galoissche Erweiterung L/K lokaler Körper sei die Reziprozitätsabbildung gemäß

$$r_{\widetilde{L}/K} : \mathrm{Frob}(\widetilde{L}/K) \to K^*/N_{\widetilde{L}/K}\widetilde{L}^*, \quad \sigma \mapsto N_{\Sigma/K}(\pi_\Sigma) \mod N_{\widetilde{L}/K}\widetilde{L}^*$$

definiert. Dabei bezeichnen Σ den Fixkörper zu σ und π_Σ ein Primelement aus Σ^*. Die Reziprozitätsabbildung ist unabhängig von der speziellen Wahl des Primelements und multiplikativ (vgl. [Neu], Kap.IV, § 5, Definition (5.2) und Satz (5.5)). Damit ist gemeint, dass für $\sigma_1\sigma_2 = \sigma_3$ in $\mathrm{Frob}(\widetilde{L}/K)$ mit Fixkörpern Σ_i und Primelementen π_i die Beziehung

$$N_{\Sigma_1/K}(\pi_1)N_{\Sigma_2/K}(\pi_2) \equiv N_{\Sigma_3/K}(\pi_3) \mod N_{\widetilde{L}/K}\widetilde{L}^*$$

gilt. Wegen $N_{\widetilde{L}/K} = N_{L/K} \circ N_{\widetilde{L}/L}$ besteht die Beziehung $N_{\widetilde{L}/K}\widetilde{L}^* \subseteq N_{L/K}L^*$. Zusammen mit der Surjektivität der Abbildung $\mathrm{Frob}(\widetilde{L}/K) \twoheadrightarrow G(L/K)$ ergibt sich für jede endliche Galois-Erweiterung L/K der Reziprozitätshomomorphismus.

Definition 3.4 *Der Reziprozitätshomomorphismus*

$$r_{L/K} : G(L/K) \to K^*/N_{L/K}L^*$$

wird über das folgende Diagramm vermittelt.

$$\begin{array}{ccccc}
\sigma & G(L/K) & \xrightarrow{r_{L/K}} & K^*/N_{L/K}L^* & x \bmod N_{L/K}L^* \\
\vdots & \uparrow & & \uparrow & \uparrow \\
\widetilde{\sigma} & \mathrm{Frob}(\widetilde{L}/K) & \xrightarrow[r_{\widetilde{L}/K}]{} & K^*/N_{\widetilde{L}/K}\widetilde{L}^* & x \bmod N_{\widetilde{L}/K}\widetilde{L}^* \\
\sigma & & \longmapsto & N_{\Sigma/K(\pi_\Sigma)} \bmod N_{\widetilde{L}/K}\widetilde{L}^* &
\end{array}$$

Er ist unabhängig von der speziellen Wahl des Urbildes $\widetilde{\sigma}$ von σ (vgl. [Neu], Kap.IV, § 5, Satz (5.6)).

Für unverzweigte Erweiterungen L/K hat der Reziprozitätshomomorphismus $r_{L/K}$ folgende Eigenschaft.

Satz 3.5 *Sei L/K eine endliche unverzweigte Erweiterung lokaler Körper. Dann wird der Frobeniushomomorphismus $\varphi_{L/K} \in G(L/K)$ auf ein Primelement von K abgebildet,*

$$r_{L/K}(\varphi_{L/K}) = \pi_K \mod N_{L/K}L^*.$$

Dabei ist der Frobeniushomomorphismus $\varphi_{L/K}$ als das Bild von φ_K unter der Surjektion

$$G(\widetilde{K}/K) \twoheadrightarrow G(L/K)$$

definiert. Seien $n = [L : K]$ der Grad der Körpererweiterung L/K sowie $\kappa \cong \mathbb{F}_q$ und λ die Restklassenkörper von K bzw. L. In der Sequenz

$$\widehat{\mathbb{Z}} \;\cong\; G(\widetilde{K}/K) \;\twoheadrightarrow\; G(L/K) \;\cong\; G(\lambda/\kappa) \;\cong\; \mathbb{Z}/n\mathbb{Z} \tag{3.6}$$

entsprechen sich die Elemente $1 \mapsto \varphi_K \mapsto \varphi_{L/K} \mapsto (x \mapsto x^q) \mapsto 1$ gegenseitig (vgl. Gleichung (3.2) und die Bemerkungen nach Gleichung (3.5)). Der Frobeniushomomorphismus $\varphi_{L/K}$ induziert somit auf dem Restklassenkörper den Homomorphismus $x \mapsto x^q$.

Beweis von Satz 3.5: Da L/K unverzweigt ist, gilt $\widetilde{L} = \widetilde{K}$. Nach Definition von $\varphi_{L/K}$ ist $\varphi_K \in G(\widetilde{K}/K) = G(\widetilde{L}/K)$ ein Urbild von $\varphi_{L/K}$. Der Fixkörper von φ_K ist K, so dass

$$r_{\widetilde{L}/K}(\varphi_K) \;=\; \pi_K \mod N_{\widetilde{L}/K}\widetilde{L}^* \;\mapsto\; \pi_K \mod N_{L/K}L^*,$$

also $r_{L/K}(\varphi_{L/K}) = \pi_K \mod N_{L/K}L^*$.

QED

Um zu zeigen, dass $r_{L/K}$ ein Isomorphismus ist, wie eingangs erwähnt, reicht es nach [Neu] (vgl. Kap.IV, § 6, Klassenkörperaxiom (6.1), Theorem (6.3) und Kap.IV, § 3, Bemerkung vor Axiom (3.1)) aus, das folgende Theorem zu überprüfen. Obwohl es nur Aussagen über zyklische Körpererweiterungen enthält, impliziert es die Behauptung von Theorem 3.7 über den Reziprozitätshomomorphismus für alle endlichen galoisschen Erweiterungen.

Theorem 3.6 (Klassenkörperaxiom) *Für jede zyklische Erweiterung L/K lokaler Körper gilt*

(i) $\mid K^*/N_{L/K}L^* \mid = [L:K]$,

(ii) *Satz 90 von Hilbert:* $\mid {}_{N_{L/K}}L^*/I_{G(L/K)}L^* \mid = 1$.

Dabei bezeichnen ${}_{N_{L/K}}L^* = \{x \in L : N_{L/K}(x) = 1\}$ die Norm-Eins-Gruppe und $I_{G(L/K)}L^*$ die Untergruppe der Norm-Eins-Gruppe, die von Elementen der Form $\frac{\sigma x}{x}$, $x \in L^*$, $\sigma \in G(L/K)$, erzeugt wird. Damit ergibt sich eine andere Formulierung von Hilberts Satz 90.

> Für eine zyklische Erweiterung L/K mit Erzeuger $\sigma \in G(L/K)$ hat ein Element $y \in L^*$ genau dann die Norm $N_{L/K}(y) = 1$, wenn es in der Form $y = \frac{\sigma x}{x}$ mit $x \in L^*$ geschrieben werden kann.

Da das Klassenkörperaxiom im Falle lokaler Körper erfüllt ist (vgl. [Neu], Kap.V, § 1, Theorem (1.1)), ist der oben betrachtete Reziprozitätshomomorphismus $r_{L/K}$ surjektiv und hat den Kommutator $G'(L/K)$ als Kern (vgl. [Neu], Kap.V, § 1, Theorem (1.3)).

Theorem 3.7 (Lokales Reziprozitätsgesetz) *Für jede endliche galoissche Erweiterung L/K lokaler Körper hat man einen Isomorphismus*

$$r_{L/K} : G(L/K)^{ab} \to K^*/N_{L/K}L^*.$$

3.2 Lokales Normrestsymbol und Kummertheorie

Als Umkehrabbildung des Reziprozitätshomomorphismus ergibt sich für jede endliche Galois-Erweiterung L/K lokaler Körper eine surjektive Abbildung

$$(\ .\ , L/K) : K^* \to G(L/K)^{ab}, \quad a \mapsto (a, L/K) \tag{3.7}$$

mit dem Kern $N_{L/K}L^*$, das lokale Normrestsymbol.

Sei $L = \mathbb{Q}_p(\zeta)$ mit einer primitiven m-ten Einheitswurzel ζ. Dann ist $L/\mathbb{Q}_p$ eine endliche abelsche Galois-Erweiterung. Das Bild $(a, L/\mathbb{Q}_p)$ eines Elementes $a \in \mathbb{Q}_p^*$ unter dem lokalen Normrestsymbol ist ein Automorphismus σ_a der Galoisgruppe $G(L/\mathbb{Q}_p)$, der durch seine Wirkung auf ζ festgelegt ist. Da die Elemente der Galoisgruppe primitive m-te Einheitswurzeln wieder auf primitive m-te Einheitswurzeln abbilden, gilt

$$(a, L/\mathbb{Q}_p)\zeta = \zeta^{u_a}$$

mit einem von a abhängigen Exponenten u_a. Zur Bestimmung dieses Exponenten ist eine Fallunterscheidung notwendig.

Satz 3.8 *Sei $L = \mathbb{Q}_p(\zeta)$ mit einer primitiven m-ten Einheitswurzel ζ. Dann gelten für das lokale Normrestsymbol $(\, . \, , L/\mathbb{Q}_p)$ folgende Aussagen.*

(i) *Im Fall $(m,p) = 1$ gilt*

$$(a, L/\mathbb{Q}_p)\zeta = \zeta^{p^{v_p(a)}}.$$

Dabei ist v_p die eindeutige Fortsetzung der p-adischen Bewertung von $\mathbb{Q}_p$ nach L.

(ii) *Falls $m = p^n$ eine p-Potenz ist, gilt*

$$(a, L/\mathbb{Q}_p)\zeta = \zeta^{u^{-1}},$$

wobei $a = up^{v_p(a)}$. Hier bezeichnet $\zeta^{u^{-1}}$ eine Potenz ζ^r mit einem $r \in \mathbb{Q}_p$, für welches $ru \equiv 1 \mod p^n$ gilt (vgl. [Neu], Kap.V, § 2, Theorem (2.4)).

BEWEIS von (i): Da $L/\mathbb{Q}_p$ nach Satz 2.1unverzweigt ist, ergibt sich die Behauptung als direkte Folgerung aus Satz 3.5.

QED

Als Verallgemeinerung von Satz 3.5 ergibt sich, dass das lokale Normrestsymbol für unverzweigte Erweiterungen L/K durch

$$(a, L/K) = \varphi_{L/K}^{\nu_K(a)}$$

gegeben ist. Dabei ist $\varphi_{L/K}$ der Frobeniushomomorphismus und ν_K die Fortsetzung der Bewertung von K.

Das lokale Reziprozitätsgesetz gibt die Möglichkeit einer Klassifizierung der endlichen abelschen Erweiterungen L/K lokaler Körper, wie auch bei [Neu], Kap.V, § 1, Theorem (1.4), nachgelesen werden kann. Die Zuordnung

$$L \longleftrightarrow \mathcal{N}_L := N_{L/K}L^*$$

ist eine eineindeutige Abbildung zwischen den endlichen abelschen Erweiterungen von K und den offenen Untergruppen $\mathcal{N}$ von K^* mit endlichem Index in K^*. Die Topologie von K^* ist durch die Bewertung ν_K von K gegeben. Gehören L und $\mathcal{N}$ zusammen, so heißt $\mathcal{N}$ Normengruppe der Erweiterung L/K und L heißt Klassenkörper von $\mathcal{N}$.

Für spezielle Erweiterungen L/K seien die Normengruppen angegeben.

Satz 3.9

(i) *Seien K ein Körper, der die n-ten Einheitswurzeln enthält, und $L = K(\sqrt[n]{K^*})$. Dann ist die Erweiterung L/K abelsch und es gilt*

$$N_{L/K}L^* = K^{*n}$$

(vgl. [Neu], Kap.V, § 1, Satz (1.5)).

(ii) *Seien $p \neq 2$ eine Primzahl, $K = \mathbb{Q}_p$ und $K_n = \mathbb{Q}_p(\zeta_n)$ mit einer primitiven p^{n+1}-ten Einheitswurzel ζ_n. Dann ist*

$$N_{K_n/\mathbb{Q}_p}K_n^* = \langle p\rangle \times (1 + p^{n+1}\mathbb{Z}_p),$$

wobei $\langle p\rangle = \{p^j,\ j \in \mathbb{Z}\}$.

Beweis von (ii): Zuerst soll $(1+p^{n+1}\mathbb{Z}_p) \subseteq N_{K_n/\mathbb{Q}_p}K_n^*$ gezeigt werden. Dazu wird die Abbildung

$$\varphi : p^k\mathbb{Z}_p \to p^{k+s}\mathbb{Z}_p, \quad a \mapsto (p-1)p^s a$$

betrachtet. Wegen $v_p\big((p-1)p^s a\big) = s + v_p(a) \geq s + k$ für $v_p(a) \geq k$ ist φ wohldefiniert. Außerdem ist φ ein Gruppenhomomorphismus. Um zu zeigen, dass φ ein Isomorphismus ist, wird die Umkehrabbildung

$$\varphi' : p^{k+s}\mathbb{Z}_p \to p^k\mathbb{Z}_p, \quad b = p^s b' \mapsto \frac{b'}{p-1}$$

angegeben. Diese Abbildung ist wohldefiniert, da sich jedes $b \in p^{k+s}\mathbb{Z}_p$ eindeutig als $p^s b'$ mit $b' \in p^k\mathbb{Z}_p$ schreiben läßt, und da $p-1$ eine Einheit in $\mathbb{Z}_p$ ist. Es ist leicht zu sehen, dass φ und φ' invers zueinander sind.

Nach Satz 2.3 ist die Exponentialabbildung

$$\exp : p^k\mathbb{Z}_p \to (1 + p^k\mathbb{Z}_p)$$

wegen $p > 2$ für $k \geq 1$ ein Isomorphismus. Durch diesen wird der Isomorphismus φ in den Isomorphismus

$$\psi : (1 + p^k\mathbb{Z}_p) \to (1 + p^{k+s}\mathbb{Z}_p), \quad x \mapsto x^{(p-1)p^s},$$

überführt. Für $k = 1$ und $s = n$ erhält man $(1 + p^{n+1}\mathbb{Z}_p) \cong (1 + p\,\mathbb{Z}_p)^{(p-1)p^n}$, woraus $(1+p^{n+1}\mathbb{Z}_p) \subseteq N_{K_n/\mathbb{Q}_p}K_n^*$ folgt, da die Erweiterung $K_n/\mathbb{Q}_p$ nach Satz 2.1 den Grad $(p-1)p^n$ hat.

Ebenfalls nach Satz 2.1 ist $\pi_n = 1-\zeta_n$ ein Primelement von K_n. Aus dem Beweis zu Satz 2.1, Teil (ii), erkennt man, dass π_n die Norm

$$N_{K_n/\mathbb{Q}_p}(\pi_n) = p$$

hat. Es folgt $\langle p\rangle \times (1+p^{n+1}\mathbb{Z}_p) \subseteq N_{K_n/\mathbb{Q}_p}K_n^*$. Nach dem lokalen Reziprozitätsgesetz (Theorem 3.7) hat die Gruppe $N_{K_n/\mathbb{Q}_p}K_n^*$ den Index $(p-1)p^n$ in $\mathbb{Q}_p^*$. Somit genügt es zu zeigen, dass $\langle p\rangle \times (1+p^{n+1}\mathbb{Z}_p)$ in $\mathbb{Q}_p^*$ ebenfalls den Index $(p-1)p^n$ hat. Nach [Lor2], § 25, F6, hat $\mathbb{Q}_p^*$ die Darstellung $\mathbb{Q}_p^* = \langle p\rangle \times \mu_{p-1} \times (1+p\,\mathbb{Z}_p)$. Hier bezeichnet μ_{p-1} die Gruppe der $(p-1)$-ten Einheitswurzeln. Folglich gilt

$$\mathbb{Q}_p^*/\big(\langle p\rangle \times (1+p^{n+1}\mathbb{Z}_p)\big) \cong \mu_{p-1} \times (1+p\,\mathbb{Z}_p)/(1+p^{n+1}\mathbb{Z}_p).$$

Unter Verwendung der Logarithmus-Abbildung, die für $k \geq 1$ ein Isomorphismus $(1+p^k\mathbb{Z}_p) \to p^k\mathbb{Z}_p$ ist (vgl. Satz 2.3), erhält man

$$(1+p\,\mathbb{Z}_p)/(1+p^{n+1}\mathbb{Z}_p) \;\cong\; p\,\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p \;\cong\; \mathbb{Z}/p^n\mathbb{Z},$$

woraus $\big|\mu_{p-1} \times (1+p\,\mathbb{Z}_p)/(1+p^{n+1}\mathbb{Z}_p)\big| = (p-1)p^n$ folgt.

QED

Im folgenden soll die Kummertheorie kurz vorgestellt werden, die Resultate sind auch bei [Lor1] (vgl. § 14, Satz 4 und Definition davor) zu finden.

Satz 3.10 (Kummertheorie) *Betrachtet wird ein Körper K, der die m-ten Einheitswurzeln enthält. Dann ist die Zuordnung*

$$A \longleftrightarrow L_A := K(\sqrt[m]{A})$$

eine eineindeutige Abbildung zwischen den Untergruppen $A \subseteq K^*$ mit $K^{*m} \subseteq A$ und den abelschen Erweiterungen L/K vom Exponent m, d.h. für alle $\sigma \in G(L/K)$ gilt $\sigma^m = id$. Dabei ist die Erweiterung L_A/K genau dann endlich, wenn es die Faktorgruppe A/K^{*m} ist. In diesem Fall gelten die Isomorphien

$$G(L_A/K) \cong (A/K^{*m})^\times \quad \textit{und} \quad G(L_A/K)^\times \cong A/K^{*m}.$$

Mit $H^\times$ ist die Charaktergruppe zu H bezeichnet, d.h. die Menge aller Homomorphismen $H \to K^*$. Da die hier betrachteten Gruppen den Exponenten m haben, bilden die Homomorphismen in die Gruppe $\mu_m(K)$ der m-ten Einheitswurzeln von K ab. Somit ist

$$H^\times = \mathrm{Hom}\big(H, \mu_m(K)\big).$$

3.3 Hilbertsymbol und explizites Reziprozitätsgesetz

Aus der Verbindung des lokalen Reziprozitätsgesetzes (Theorem 3.7) mit der Kummertheorie (Satz 3.10) ergibt sich das Hilbertsymbol. Betrachtet werden ein

lokaler Körper K, der die m-ten Einheitswurzeln enthält, und die Erweiterung $L = K(\sqrt[m]{K^*})$. Diese Erweiterung ist galoissch und abelsch. Nach dem lokalen Reziprozitätsgesetz und Satz 3.9, Teil (i), besteht der Isomorphismus

$$K^*/N_{L/K}L^* \cong K^*/K^{*m} \cong G(L/K), \quad a \mapsto \sigma_a := (a, L/K).$$

Mit der Kummertheorie ergibt sich der Isomorphismus

$$K^*/K^{*m} \cong G(L/K)^\times, \quad b \mapsto \chi_b.$$

Aus der Paarung

$$G(L/K) \times G(L/K)^\times \to \mu_m(K), \quad (\sigma, \chi) \mapsto \chi(\sigma)$$

erhält man somit das m-te Hilbertsymbol als nicht ausgeartete, bi-multiplikative Abbildung

$$(\,.\,,\,.\,)_m : K^*/K^{*m} \times K^*/K^{*m} \to \mu_m(K), \quad (a, b) \mapsto (a, b)_m. \tag{3.8}$$

Das Hilbertsymbol hat folgende grundlegende Eigenschaften.

Satz 3.11 *Für alle $a, a', a'', b, b', b'' \in K^*$ gilt*

(i) $(a'a'', b)_m = (a', b)_m(a'', b)_m$,
$(a, b'b'')_m = (a, b')_m(a, b'')_m$.

(ii) *Ist $(a, b)_m = 1$ für alle $b \in K^*$, so ist $a \in K^{*m}$.*

(iii) *Es gilt $(a, b)_m = 1$ genau dann, wenn a eine Norm der Erweiterung $K\big(\sqrt[m]{b}\big)/K$ ist.*

(iv) *Es gilt $(a, b)_m = (b, a)_m^{-1}$.*

(v) *Es gilt $(a, 1-a)_m = 1$ und $(a, -a)_m = 1$.*

Insbesondere folgt aus Eigenschaft (i), dass $(a^{-1}, b)_m = (a, b)_m^{-1}$ gilt.

Beweis: Die Punkte (i) und (ii) ergeben sich direkt aus der Paarung, Punkt (iv) folgt aus Punkt (v) (vgl. [Neu], Kap.V, § 3, Satz (3.2)). Der dritte Punkt ergibt sich, wenn man das Hilbertsymbol zum lokalen Normrestsymbol in Beziehung setzt. Diese Beziehung ist für $a, b \in K^*$ durch die Formel

$$(a, K(\sqrt[m]{b})/K)\ \sqrt[m]{b} = (a, L/K)\ \sqrt[m]{b} = (a, b)_m\ \sqrt[m]{b}$$

gegeben (vgl. [Neu], Kap.V, § 3, Satz (3.1)). Dies bedeutet, dass der durch das lokale Normrestsymbol gegebene Automorphismus $(a, L/K)$ auf $\sqrt[m]{b}$ durch Multiplikation mit der m-ten Einheitswurzel $(a, b)_m$ wirkt.

QED

Nach dieser allgemeinen Definition ist es nun von Interesse, explizite Formeln für das Hilbertsymbol im Fall einer Einheitswurzelerweiterung von $\mathbb{Q}_p$ zu bestimmen. Dazu ist eine Fallunterscheidung bezüglich m nötig.

Seien $K = \mathbb{Q}_p(\zeta)$ mit einer primitiven m-ten Einheitswurzel ζ und $L = K(\sqrt[m]{K^*})$. Es werde der Fall $(m,p) = 1$ betrachtet. Seien ν_K die normierte Exponentialbewertung und q die Elementezahl des Restklassenkörpers von K. Nach Satz 2.1 enthält K die Gruppe μ_{q-1} der $(q-1)$-ten Einheitswurzeln. Nach [Lor2], § 25, F6, hat die Einheitengruppe $\mathcal{O}_K^*$ des Bewertungsringes von K die Darstellung

$$\mathcal{O}_K^* = \mu_{q-1} \times (1 + \mathfrak{m}_K),$$

wobei $\mathfrak{m}_K$ das maximale Ideal von $\mathcal{O}_K$ bezeichnet. Folglich gilt nach Wahl eines Primelementes π_K

$$K^* = \langle \pi_K \rangle \times \mu_{q-1} \times (1 + \mathfrak{m}_K).$$

Für jedes $u \in K^*$ existiert also eine eindeutige Zerlegung $u = \pi_K^r \, \omega(u) \, \langle u \rangle$ mit $r \in \mathbb{Z},\ \omega(u) \in \mu_{q-1}$ und $\langle u \rangle \in (1 + \mathfrak{m}_K)$. Für $u \in \mathcal{O}_K^*$ gilt $u \equiv \omega(u) \mod \mathfrak{m}_K$.

Theorem 3.12 (Explizites Reziprozitätsgesetz) *Seien $K = \mathbb{Q}_p(\zeta)$ mit einer primitiven m-ten Einheitswurzel ζ und $L = K(\sqrt[m]{K^*})$. Im Fall $(m,p) = 1$ ist das m-te Hilbertsymbol für $a, b \in K^*$ durch die Formel*

$$(a,b)_m = \omega\left((-1)^{\nu_K(a)\nu_K(b)} \frac{b^{\nu_K(a)}}{a^{\nu_K(b)}} \right)^{\frac{q-1}{m}}$$

explizit gegeben.

Beweis: Für $a, b \in K^*$ werde das Produkt

$$\langle a,b \rangle := \omega\left((-1)^{\nu_K(a)\nu_K(b)} \frac{b^{\nu_K(a)}}{a^{\nu_K(b)}} \right)^{\frac{q-1}{m}}$$

definiert. Dieses ist in beiden Einträgen multiplikativ, da die Abbildung $x \mapsto \omega(x)$ für $x \in K^*$ multiplikativ ist. Insbesondere gilt $\langle a,b \rangle = \langle b,a \rangle^{-1}$. Somit genügt es, die Fälle $a = \pi_K,\ b = -\pi_K$ und $a = \pi_K,\ b \in \mathcal{O}_K^*$ sowie $a, b \in \mathcal{O}_K^*$ zu betrachten.

Für $a = \pi_K,\ b = -\pi_K$ gilt nach Satz 3.11, Teil (v), dass $(\pi_K, -\pi_K)_m = 1$. Andererseits ist $\langle \pi_K, -\pi_K \rangle = \omega(1)^{\frac{q-1}{m}} = 1$. Damit ist die Gleichheit $(a,b)_m = \langle a,b \rangle$ für diesen Fall gezeigt.

Seien nun $a = \pi_K$ und $b = u \in \mathcal{O}_K^*$. Dann gilt $\langle \pi_K, u \rangle = \omega(u)^{\frac{q-1}{m}}$. Sei $y = \sqrt[m]{u}$. Es soll gezeigt werden, dass $K(y)/K$ unverzweigt ist. Seien κ der Restklassenkörper von K und κ' der Zerfällungskörper von

$$X^m - u \mod \mathfrak{m}_K.$$

Nach [Lor2], § 24, Satz 3, (iii), gehört zu der Körpererweiterung κ'/κ eine eindeutige unverzweigte Erweiterung K'/K, so dass κ' der Restklassenkörper von K' ist. Da $X^m - u$ nach dem Henselschen Lemma (vgl. [Neu], Kap.II, § 4, Lemma (4.6)) über K' in Linearfaktoren zerfällt, gilt $K(y) \subseteq K'$. Nach [Neu], Kap.II, § 7, Satz (7.2), ist jede Teilerweiterung einer unverzweigten Erweiterung unverzweigt, somit ist $K(y)/K$ unverzweigt.

Aus der Unverzweigtheit von $K(y)/K$ folgt mit Satz 3.5, dass das Normrestsymbol $(\pi_K, K(y)/K)$ gerade der Frobeniushomomorphismus $\varphi_{K(y)/K}$ der Erweiterung $K(y)/K$ ist. Mit dem im Beweis zu Satz 3.11 formulierten Zusammenhang zwischen Normrest- und Hilbertsymbol folgt

$$(\pi_K, u)_m = \frac{\varphi_{K(y)/K}(y)}{y}.$$

Da der Frobeniushomomorphismus auf dem Restklassenkörper die Potenzierung mit q induziert, folgt

$$(\pi_K, u)_m \equiv y^{q-1} \equiv u^{\frac{q-1}{m}} \equiv \omega(u)^{\frac{q-1}{m}} \equiv \langle \pi_K, u \rangle \mod \mathfrak{m}_K.$$

Somit gilt $(\pi_K, u)_m = \langle \pi_K, u \rangle$, da sowohl $(\pi_K, u)_m$ als auch $\langle \pi_K, u \rangle$ $(q-1)$-te Einheitswurzeln sind, und die $(q-1)$-ten Einheitswurzeln unter der Abbildung $\mathcal{O}_K^* \to \left(\mathcal{O}_K/\mathfrak{m}_K\right)^*$ isomorph auf $\left(\mathcal{O}_K/\mathfrak{m}_K\right)^* = \kappa^*$ abgebildet werden.

Seien nun schließlich a und b Einheiten des Bewertungsringes $\mathcal{O}_K$. Dann ist $\langle a, b \rangle = 1$. Sei $y = \sqrt[m]{b}$. Dann ist $K(y)/K$ nach obiger Argumentation unverzweigt und mit der Bemerkung nach Satz 3.8 folgt mit $v_p(a) = 0$ für das Normrestsymbol $(a, K(y)/K) = id$. Damit kann man

$$(a, b)_m = \frac{(a, K(y)/K)y}{y} = 1$$

schlussfolgern. Somit ist auch in diesem Falle $(a, b)_m = \langle a, b \rangle$ gezeigt.

QED

Im Fall $p \,|\, m$ gestaltet sich die Angabe expliziter Formeln für das Hilbertsymbol schwieriger. Die vorliegende Arbeit widmet sich der Angabe solcher Formeln im Spezialfall $K_n := \mathbb{Q}_p(\zeta_n)$ mit einer primitiven p^{n+1}-ten Einheitswurzel ζ_n, also $m = p^{n+1}$.

Kapitel 4

Vorbereitungen

In diesem Kapitel werden vorbereitende Aussagen formuliert, welche für die Beweise im Kapitel 5 benötigt werden. Zu Beginn werden zunächst die Bezeichnungen eingeführt, die für die weitere Arbeit bestimmend sind.

Sei $p \neq 2$ eine Primzahl. Für $n \geq 0$ sei $K_n = \mathbb{Q}_p(\zeta_n)$ mit einer primitiven p^{n+1}-ten Einheitswurzel ζ_n. Es sei darauf hingewiesen, dass K_0 nicht $\mathbb{Q}_p$, sondern $\mathbb{Q}_p(\zeta_0)$ mit einer primitiven p-ten Einheitswurzel ζ_0 ist. Die Einheitswurzeln $\zeta_n,\ n = 0, 1, 2, \ldots$, seien so gewählt, dass für $m \geq n$ die Beziehung $\zeta_m^{p^{m-n}} = \zeta_n$ gilt. Nach Satz 2.1 ist $K_n/\mathbb{Q}_p$ eine rein verzweigte Erweiterung vom Grad

$$[K_n : \mathbb{Q}_p] = (p-1)p^n.$$

Somit sind die Erweiterungen K_m/K_n für $m \geq n$ ebenfalls rein verzweigt und haben den Grad $[K_m : K_n] = p^{m-n}$. Für die normierte Exponentialbewertung ν_n von K_n gelten die Beziehungen

$$\nu_n = (p-1)p^n v_p \quad \text{und} \quad \nu_m = p^{m-n}\nu_n \quad \text{für} \quad m \geq n,$$

wobei v_p die eindeutige Fortsetzung der p-adischen Bewertung von $\mathbb{Q}_p$ auf K_n bezeichnet. Sei $\mathcal{O}_n$ der Bewertungsring in K_n. Das Element $\pi_n = 1 - \zeta_n$ ist nach Satz 2.1 ein Primelement in $\mathcal{O}_n$, das davon erzeugte Ideal $\mathfrak{m}_n = \pi_n\mathcal{O}_n$ ist das maximale Ideal des Ringes $\mathcal{O}_n$. Die Potenzen $\mathfrak{m}_n^r,\ r \in \mathbb{Z}$, des maximalen Ideals lassen sich durch

$$\mathfrak{m}_n^r = \{x \in \mathcal{O}_n : \nu_n(x) \geq r\}$$

charakterisieren. Somit ergibt sich für $r > s$ die Enthaltenseinsrelation $\mathfrak{m}_n^r \subseteq \mathfrak{m}_n^s$. Für den Restklassenkörper κ_n von K_n gilt $\mathcal{O}_n/\mathfrak{m}_n \cong \mathbb{Z}_p/p\,\mathbb{Z}_p \cong \mathbb{F}_p$.

4.1 Die Logarithmus- und Exponentialfunktion in K_n

Lemma 4.1 *In K_n sind*

$$\exp : \mathfrak{m}_n^r \to (1 + \mathfrak{m}_n^r) \quad \textit{und} \quad \log : (1 + \mathfrak{m}_n^r) \to \mathfrak{m}_n^r$$

für $r > p^n$ zueinander inverse Isomorphismen.

BEWEIS: Da die Erweiterung $K_n/\mathbb{Q}_p$ den Verzweigungsindex $e = (p-1)p^n$ hat, ergibt sich das Lemma als eine Folgerung aus Satz 2.3.

QED

Für $r,\ s \in \mathbb{N}$ bezeichne $(1+\mathfrak{m}_n^r)^s$ die multiplikative Gruppe $\big\{(1+\pi_n^r y)^s,\ y \in \mathcal{O}_n\big\}$. Für diese Gruppen gilt das folgende Lemma.

Lemma 4.2 *Für $a,\ b \in \mathbb{N}$ mit $b \geq p^n$ gilt*

$$\big(1+\mathfrak{m}_n^b\big)^{p^a} \subseteq 1+p^a\mathfrak{m}_n^b.$$

Für $b > p^n$ gilt sogar $\big(1+\mathfrak{m}_n^b\big)^{p^a} = 1+p^a\mathfrak{m}_n^b$.

BEWEIS: Zunächst wird die Beziehung

$$1+p^a\mathfrak{m}_n^b = (1+\mathfrak{m}_n^b)^{p^a} \qquad \text{für} \qquad a,b \in \mathbb{N},\ b > p^n$$

bewiesen. Nach Lemma 4.1 und aufgrund der Voraussetzung an b ist die Abbildung

$$\log : \big(1+\mathfrak{m}_n^b\big)^{p^a} \longrightarrow p^a \log(1+\mathfrak{m}_n^b) \cong p^a\mathfrak{m}_n^b$$

ein Isomorphismus. Wegen $\nu_n(p^a) = a(p-1)p^n$ gilt $p^a\mathfrak{m}_n^b = \mathfrak{m}_n^{a(p-1)p^n+b}$. Wiederum nach Lemma 4.1 und aufgrund der Voraussetzung an b erkennt man, dass

$$\exp : \mathfrak{m}_n^{a(p-1)p^n+b} \longrightarrow \big(1+\mathfrak{m}_n^{a(p-1)p^n+b}\big) \cong \big(1+p^a\mathfrak{m}_n^b\big)$$

ein Isomorphismus ist. Insgesamt ergibt sich somit die behauptete Beziehung.

Nun ist für $b \geq p^n$ die Enthaltenseinsrelation

$$\big(1+\mathfrak{m}_n^b\big)^{p^a} \subseteq \big(1+p^a\mathfrak{m}_n^b\big) = 1+\mathfrak{m}_n^{a(p-1)p^n+b}$$

zu zeigen. Sei dazu $x = \big(1+\pi_n^b y\big)^{p^a},\ y \in \mathcal{O}_n$, ein beliebiges Element aus $(1+\mathfrak{m}_n^b)^{p^a}$. Dann gilt

$$x-1 = \sum_{j=1}^{p^a} \binom{p^a}{j} \pi_n^{bj}\, y^j.$$

Es ist nachzuweisen, dass $\nu_n(x-1) \geq a(p-1)p^n+b$ gilt. Dies ist bewiesen, wenn für alle $j = 1 \ldots p^a$ die Ungleichung

$$\nu_n\Big(\binom{p^a}{j}\pi_n^{bj}\Big) = (p-1)p^n\, v_p\Big(\binom{p^a}{j}\Big) + bj \geq a(p-1)p^n+b$$

gezeigt ist. Zunächst muss die Bewertung des Binomialkoeffizienten bestimmt werden. In der Darstellung

$$\binom{p^a}{j} = p^a \frac{p^a-1}{1} \cdot \frac{p^a-2}{2} \cdots \frac{p^a-(j-1)}{j-1} \cdot \frac{1}{j}$$

erkennt man, dass die mittleren Faktoren nicht zur p-Bewertung beitragen, denn sollte einer der Zähler durch eine Potenz p^e teilbar sein, so ist es auch der dazugehörige Nenner und umgekehrt. Insgesamt erhält man

$$v_p\Big(\binom{p^a}{j}\Big) = a - v_p(j)$$

und somit $\nu_n\big(\binom{p^a}{j}\pi_n^{bj}\big) = (p-1)p^n\big(a-v_p(j)\big) + bj$. Sei $j = dp^e,\ (d,p) = 1,\ e > 0$. Dann ist

$$\frac{v_p(j)}{j-1} = \frac{e}{dp^e-1} \le \frac{e}{p^e-1} = \frac{1}{p-1}\frac{e}{p^{e-1}+\ldots+1} \le \frac{1}{p-1}.$$

Diese Abschätzung gilt auch für $v_p(j) = e = 0$. Umgeformt ergibt sich $j \ge (p-1)\,v_p(j)+1$ und man kann obige Überlegung fortführen

$$\begin{aligned}\nu_n\Big(\binom{p^a}{j}\pi_n^{bj}\Big) &\ge (p-1)p^n\big(a-v_p(j)\big) + b\big((p-1)v_p(j)+1\big)\\ &= (p-1)(b-p^n)v_p(j) + a(p-1)p^n + b.\end{aligned}$$

Wegen der Voraussetzung an b entspricht der letzte Term der Gleichung einer steigenden Gerade in $v_p(j)$. Der Ausdruck auf der rechten Seite nimmt somit seinen kleinsten Wert für $v_p(j) = 0$ an, also

$$\nu_n\Big(\binom{p^a}{j}\pi_n^{bj}\Big) \ge a(p-1)p^n + b.$$

Damit ist die Behauptung bewiesen.

QED

4.2 Zur Differente von K_n

In diesem Abschnitt wird die Differente der Körpererweiterung $K_n/\mathbb{Q}_p$ berechnet.

Definition 4.3 *Seien L/K eine endliche separable Erweiterung lokaler Körper und $\alpha \in \mathcal{O}_L$ mit Minimalpolynom $f \in \mathcal{O}_K[X]$. Dann ist die Element-Differente von α gemäß*

$$\delta_{L/K}(\alpha) := \begin{cases} f'(\alpha), & \textit{falls } L = K(\alpha)\\ 0, & \textit{sonst}\end{cases}$$

definiert. Die Differente $\mathfrak{D}_{L/K}$ der Körpererweiterung L/K ist dann als das durch alle Element-Differenten $\delta_{L/K}(\alpha)$, $\alpha \in \mathcal{O}_L$, erzeugte Ideal in $\mathcal{O}_K$ definiert. Im Spezialfall $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ gilt also

$$\mathfrak{D}_{L/K} = \big(\delta_{L/K}(\alpha)\big)$$

(vgl. auch [Neu], Kap.III, § 2, Satz (2.4)).

Lemma 4.4 *Für den Bewertungsring $\mathcal{O}_n$ im Körper K_n gilt $\mathcal{O}_n = \mathbb{Z}_p[\pi_n]$.*

Beweis: Sei $e = (p-1)p^n$. Dann läßt sich jedes Element $x \in K_n$ in der Form

$$x = \alpha_0 + \alpha_1\zeta_n + \alpha_2\zeta_n^2 + \ldots + \alpha_{e-1}\zeta_n^{e-1}$$

schreiben, wobei $\alpha_j \in \mathbb{Q}_p$. Unter Ausnutzung der Beziehung $\pi_n = 1 - \zeta_n$ erkennt man, dass man x alternativ auch in der Form

$$x = \beta_0 + \beta_1\pi_n + \beta_2\pi_n^2 + \ldots + \beta_{e-1}\pi_n^{e-1}$$

mit $\beta_j \in \mathbb{Q}_p$ schreiben kann. Damit $x \in \mathcal{O}_n$, muss $\nu_n(x) \geq 0$ gelten, also

$$\nu_n(x) \geq \min\{\nu_n(\beta_0), \nu_n(\beta_1) + 1, \ldots, \nu_n(\beta_{e-1}) + e - 1\} \overset{!}{\geq} 0.$$

Wegen $\nu_n(\beta_j) \in e\,\mathbb{Z}$ ist diese Bedingung nur erfüllbar, wenn $\beta_j \in \mathbb{Z}_p$, d.h. es gilt

$$\mathcal{O}_n = \mathbb{Z}_p[\pi_n].$$

QED

Lemma 4.5 *Für $m \geq n$ gilt $\mathfrak{m}_m^{p^{m-n}} = \pi_n\mathcal{O}_m$.*

Beweis: Diese Beziehung folgt aus der Beziehung $\pi_m^{p^{m-n}} = u\pi_n$ mit einer Einheit $u \in \mathcal{O}_m^*$.

QED

Lemma 4.6 *Für die Differente $\mathfrak{D}_n$ der Körpererweiterung $K_n/\mathbb{Q}_p$ gilt*

$$\mathfrak{D}_n = p^{n+1}\mathfrak{m}_n^{-p^n}.$$

Beweis: Nach Definition 4.3 und Lemma 4.4 ist es ausreichend, die Element-Differente $\delta_{K_n/\mathbb{Q}_p}(\pi_n)$ von π_n zu berechnen. Das Minimalpolynom von ζ_n ist das p^{n+1}-te Kreisteilungspolynom $g(X) = \dfrac{X^{p^{n+1}} - 1}{X^{p^n} - 1}$. Somit ist

$$f(X) = g(1 - X) = \frac{(1-X)^{p^{n+1}} - 1}{(1-X)^{p^n} - 1}$$

das Minimalpolynom für $\pi_n = 1 - \zeta_n$ (vgl. Beweis zum Satz 2.1, Teil (ii)). Für die Ableitung der Funktion f gilt

$$f'(x) = \frac{-p^{n+1}(1-X)^{p^{n+1}-1}\big((1-X)^{p^n}-1\big) + p^n\big((1-X)^{p^{n+1}}-1\big)(1-X)^{p^n-1}}{\big((1-X)^{p^n}-1\big)^2},$$

$$\begin{aligned} f'(\pi_n) &= \frac{-p^{n+1}\zeta_n^{p^{n+1}-1}\big(\zeta_n^{p^n}-1\big) + p^n\big(\zeta_n^{p^{n+1}}-1\big)\zeta_n^{p^n-1}}{\Big(\zeta_n^{p^n}-1\Big)^2} \\ &= -\frac{p^{n+1}}{\zeta_n(\zeta_n^{p^n}-1)} = \frac{p^{n+1}}{\zeta_n(1-\zeta_n^{p^n})} = \frac{p^{n+1}}{\zeta_n(1-\zeta_0)} = p^{n+1}\zeta_n^{-1}\pi_0^{-1}. \end{aligned}$$

Das von $f'(\pi_n)$ erzeugte Ideal ist

$$\mathfrak{D}_n = \big(\delta_n(\pi_n)\big) = p^{n+1}\zeta_n^{-1}\pi_0^{-1}\mathcal{O}_n = p^{n+1}\pi_0^{-1}\mathcal{O}_n = p^{n+1}\pi_n^{-p^n}\mathcal{O}_n = p^{n+1}\mathfrak{m}_n^{-p^n},$$

denn ζ_n ist eine Einheit in $\mathcal{O}_n$.

QED

Aus dem Beweis erkennt man, dass man die Differente $\mathfrak{D}_n$ alternativ auch als $\mathfrak{D}_n = p^{n+1}\pi_0^{-1}\mathcal{O}_n$ schreiben kann.

4.3 Über Spuren und Normen

Für $n \geq 0$ seien S_n und N_n die Spur- bzw. die Normabbildung $K_n \to \mathbb{Q}_p$,

$$S_n(x) = \sum_{\sigma \in G(K_n/\mathbb{Q}_p)} \sigma x \quad \text{und} \quad N_n(x) = \prod_{\sigma \in G(K_n/\mathbb{Q}_p)} \sigma x \quad \text{für} \quad x \in K_n.$$

Bekanntlich kann man die Spur und die Norm eines Elementes an seinem Minimalpolynom ablesen. Gilt allgemein $L = K(\alpha)$ und ist

$$f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$$

das Minimalpolynom von α über K, so gilt für die Spur $S_{L/K}(\alpha)$ bzw. die Norm $N_{L/K}(\alpha)$ von α

$$S_{L/K}(\alpha) = -a_{n-1} \quad \text{und} \quad N_{L/K}(\alpha) = (-1)^n a_0$$

(vgl. [Lor1], § 13, Gleichungen (8) und (9) nach Definition 1). Für $m > n$ bezeichnen S_{mn} und N_{mn} die Spur und die Norm $K_m \to K_n$. Für $m > k > n$ gelten die Kompositionsformeln $S_{mn} = S_{kn} \circ S_{mk}$ und $N_{mn} = N_{kn} \circ N_{mk}$ (vgl. [Lor1], § 13, F5).

Ziel ist es, zu zeigen, dass

$$S_0(\mathfrak{m}_0) = p\,\mathbb{Z}_p \quad \text{und} \quad S_n(\mathfrak{m}_n) = p^n\mathbb{Z}_p \quad \text{für } n \geq 1.$$

Dafür werden zunächst die Spuren und Normen der Elemente ζ_n und π_n berechnet.

Lemma 4.7 *Für $n \geq 0$ gilt*

$$S_n(\zeta_n) = \begin{cases} 0, & n \geq 1, \\ -1, & n = 0, \end{cases} \qquad N_n(\zeta_n) = 1 \quad \textit{für } n \geq 0,$$

und

$$S_n(\pi_n) = \begin{cases} (p-1)p^n, & n \geq 1, \\ p, & n = 0, \end{cases} \qquad N_n(\pi_n) = p \quad \textit{für } n \geq 0.$$

Für $m \geq n$ gilt

$$\begin{array}{rcl} S_{mn}(\zeta_m) & = & 0 \\ N_{mn}(\zeta_m) & = & \zeta_n \end{array} \quad \textit{und} \quad \begin{array}{rcl} S_{mn}(\pi_m) & = & p^{m-n} \\ N_{mn}(\pi_m) & = & \pi_n \end{array} .$$

Beweis: Sei $n \geq 0$. Man betrachte die Minimalpolynome

$$f(X) = 1 + X^{p^n} + X^{2p^n} + \ldots + X^{(p-1)p^n} \quad \text{und} \quad g(X) = f(1-X)$$

von ζ_n bzw. π_n über $\mathbb{Q}_p$. Im Fall $m \geq n$ sind

$$f(X) = X^{p^{m-n}} - \zeta_n \quad \text{und} \quad g(X) = -f(1-X)$$

die Minimalpolynome von ζ_m bzw. π_m über K_n, denn sie sind normiert, haben den richtigen Grad und ζ_m bzw. π_m als Nullstelle.

QED

Lemma 4.8 *Seien $m \geq n \geq 0$. Für $k = ap^e, (a,p) = 1$, gilt*

$$S_n(\zeta_n^k) = \begin{cases} 0, & n > e, \\ -p^n, & n = e, \\ (p-1)p^n, & n < e, \end{cases}$$

$$S_{mn}(\zeta_m^k) = \begin{cases} 0, & 0 \leq e < m-n, \\ p^{m-n}\zeta_{m-e}^a, & m-n \leq e \leq m, \\ p^{m-n}, & m+1 \leq e. \end{cases}$$

Beweis: Sei $k = ap^e$ mit $(a,p) = 1$. Dann gilt $\zeta_n^k = \zeta_{n-e}^a$. Wegen $(a,p) = 1$ ist ζ_{n-e}^a eine p^{n-e+1}-te primitive Einheitswurzel, erfüllt also dasselbe Minimalpolynom wie ζ_{n-e}. Damit folgt

$$S_n(\zeta_n^k) = S_n(\zeta_{n-e}^a) = S_n(\zeta_{n-e}).$$

Mit Hilfe der Kompositionsformel für die Spurabbildung und Lemma 4.7 kann man weiter argumentieren

$$S_n(\zeta_{n-e}) = \left\{ \begin{array}{l} S_{n-e}\big(S_{n,n-e}(\zeta_{n-e})\big) \\ S_0\big(S_{n,0}(\zeta_0)\big) \\ S_n(1) \end{array} \right\} = \left\{ \begin{array}{l} p^e S_{n-e}(\zeta_{n-e}) \\ p^n S_0(\zeta_0) \\ [K_n : \mathbb{Q}_p] \end{array} \right\}$$

$$= \left\{ \begin{array}{ll} 0, & \text{für } n > e, \\ -p^n, & \text{für } n = e, \\ (p-1)p^n, & \text{für } n < e, \end{array} \right.$$

Sei nun $m \geq n$. Ist $e \geq m-n$, so kann man $e = m-n+r$ für ein $r \geq 0$ schreiben. Es gilt $\zeta_m^k = \big(\zeta_m^{m-(n-r)}\big)^a = \zeta_{n-r}^a$. Wegen $\zeta_{n-r} \in K_{n-r} \subseteq K_n$ ist auch $\zeta_{n-r}^a \in K_n$ und es folgt

$$S_{mn}\big(\zeta_m^k\big) = S_{mn}\big(\zeta_{n-r}^a\big) = p^{m-n}\zeta_{n-r}^a = p^{m-n}\zeta_{m-e}^a.$$

Ist dagegen $e < m-n$, so gilt $e = m-n-r$ mit $r > 0$. Man erhält $\zeta_m^k = \big(\zeta_m^{m-(n+r)}\big)^a = \zeta_{n+r}^a \in K_{n+r}$. Für die Spur gilt

$$S_{mn}\big(\zeta_m^k\big) = S_{mn}\big(\zeta_{n+r}^a\big) = S_{n+r,n}\big(S_{m,n+r}(\zeta_{n+r}^a)\big) = p^{m-(n+r)} S_{n+r,n}\big(\zeta_{n+r}^a\big) = 0,$$

da ζ_{n+r}^a wegen $(a,p) = 1$ eine primitive p^{n+r+1}-te Einheitswurzel ist und somit $S_{n+r,n}\big(\zeta_{n+r}^a\big) = S_{n+r,n}\big(\zeta_{n+r}\big) = 0$ ist.

QED

Insbesondere erkennt man mit Hilfe von $\mathcal{O}_n = \mathbb{Z}_p[\pi_n] = \mathbb{Z}_p[\zeta_n]$ (vgl. Lemma 4.4), dass $S_n(\mathcal{O}_n) \equiv 0 \mod p^n$ und $S_{mn}(\mathcal{O}_m) \equiv 0 \mod p^{m-n}$ gilt, dass also

$$S_n(\mathcal{O}_n) = p^n\mathbb{Z}_p \quad \text{und} \quad S_{mn}(\mathcal{O}_m) = p^{m-n}\mathcal{O}_n. \tag{4.1}$$

Mit Hilfe dieser Vorbereitungen ist es nun möglich, den folgenden Satz zu formulieren.

Satz 4.9 *Es gilt* $S_0(\mathfrak{m}_0) = p\,\mathbb{Z}_p$.

Beweis: Es gilt $\mathfrak{m}_0 = \pi_0\mathcal{O}_0$ und $\mathcal{O}_0 = \mathbb{Z}_p[\pi_0]$. Somit ist $\mathfrak{m}_0$ ein $\mathbb{Z}_p$-Modul, erzeugt von den Potenzen von π_0. Aufgrund der $\mathbb{Q}_p$-Linearität der Spurabbildung ist $S_0(\mathfrak{m}_0)$ ein $\mathbb{Z}_p$-Untermodul von $\mathbb{Q}_p$ und hat demnach die Gestalt $S_0(\mathfrak{m}_0) = p^r\mathbb{Z}_p$ für ein $r \in \mathbb{Z}$. Ein beliebiges Element $x \in \mathfrak{m}_0$ lässt sich als

$$x = a_1\pi_0 + a_2\pi_0^2 + a_3\pi_0^3 + \dots\ , \quad a_i \in \mathbb{Z}_p,$$

schreiben. Mit Hilfe der Stetigkeit der Spurabbildung folgt für die Spur von x

$$S_0(x) = a_1 S_0(\pi_0) + a_2 S_0(\pi_0^2) + a_3 S_0(\pi_0^3) + \dots\ .$$

Es ist also notwendig, die Spuren der Potenzen $\pi_0^k,\ k \geq 1$, genauer zu untersuchen. Sei $k = k_0 + p\,k_1,\ k_0 < p$. Dann gilt modulo p

$$\begin{aligned}\pi_0^k = (1-\zeta_0)^{k_0+p\,k_1} &\equiv (1-\zeta_0)^{k_0}(1-\zeta_0^p)^{k_1} \\ &\equiv 0 \mod p, \quad \text{falls } k_1 \neq 0.\end{aligned}$$

In diesem Fall erhält man $\pi_0^k = py$ mit einem $y \in \mathcal{O}_0$. Da $S_0(y) \in \mathbb{Z}_p$ für $y \in \mathcal{O}_0$, ergibt sich für die Spur

$$S_0\big(\pi_0^k\big) = p\,S_0(y) \equiv 0 \mod p.$$

Ist $0 < k < p$, so gilt unter Beachtung von Lemma 4.8

$$\begin{aligned}S_0(\pi_0^k) &= S_0\left(\sum_{j=0}^{k}\binom{k}{j}(-1)^j\zeta_0^j\right) = \sum_{j=0}^{k}\binom{k}{j}(-1)^j S_0(\zeta_0^j) \\ &= S_0(1) + \sum_{j=1}^{k}\binom{k}{j}(-1)^j S_0(\zeta_0^j) = (p-1) + \sum_{j=1}^{k}\binom{k}{j}(-1)^j(-1) \\ &= (p-1) - \sum_{j=0}^{k}\binom{k}{j}(-1)^j + \binom{k}{0}(-1)^0 = (p-1) - (1-1)^k + 1 = p.\end{aligned}$$

Insgesamt folgt somit

$$S_0(x) = \sum_{i=1}^{\infty} a_i S_0(\pi_0^i) \equiv 0 \mod p,$$

d.h. $v_p\big(S_0(x)\big) \geq 1$ für alle $x \in \mathfrak{m}_0$. Damit ist gezeigt, dass $S_0(\mathfrak{m}_0) \subseteq p\,\mathbb{Z}_p$. Wählt man speziell $x = \pi_0$, für welches die Beziehung $S_0(\pi_0) = p$ gilt, so erhält man $S_0(\mathfrak{m}_0) = p\,\mathbb{Z}_p$.

QED

Lemma 4.10 *Sei $d_n = (n+1)(p-1)p^n - p^n$. Dann gilt*

$$\mathfrak{D}_n = \mathfrak{m}_n^{d_n} \quad \textit{und} \quad S_n(\mathfrak{m}_n^{-d_n}) = \mathbb{Z}_p.$$

Beweis: Man rechnet leicht nach, dass

$$\mathfrak{D}_n = p^{n+1}\mathfrak{m}_n^{-p^n} = \pi_n^{(n+1)(p-1)p^n}\pi_n^{-p^n}\mathcal{O}_n = \pi_n^{(n+1)(p-1)p^n - p^n}\mathcal{O}_n = \mathfrak{m}_n^{d_n}.$$

Für die zweite Behauptung gilt unter Verwendung von Gleichung (4.1)

$$\begin{aligned}S_n\big(\mathfrak{m}_n^{-d_n}\big) &= S_n\big(\mathfrak{D}_n^{-1}\big) = p^{-(n+1)}S_n\big(\mathfrak{m}_n^{p^n}\big) \\ &= p^{-(n+1)}S_n(\pi_0\mathcal{O}_n) = p^{-(n+1)}S_0\big(\pi_0 S_{n\,0}(\mathcal{O}_n)\big) \\ &= p^{-1}S_0(\mathfrak{m}_0) = \mathbb{Z}_p,\end{aligned}$$

wobei für die letzte Gleichheit die Beziehung $S_0(\mathfrak{m}_0) = p\,\mathbb{Z}_p$ aus Satz 4.9 benutzt wurde.

QED

Mit dieser Vorbemerkung läßt sich nun der nächste Satz formulieren.

Satz 4.11 *Für $r \in \mathbb{Z}$ gilt $S_n(\mathfrak{m}_n^r) = p^s\mathbb{Z}_p$ mit einem gewissen $s \in \mathbb{Z}$, welches die Ungleichung*

$$e_n s \leq r + d_n < e_n(s+1)$$

erfüllt. Dabei ist $d_n = (n+1)(p-1)p^n - p^n$ wie in Lemma 4.10 definiert und $e_n = (p-1)p^n$ ist der Grad der Erweiterung $K_n/\mathbb{Q}_p$. Insbesondere ergibt sich $S_n(\mathfrak{m}_n) = p^n\mathbb{Z}_p$ für $n \geq 1$.

Beweis: Es gilt $\mathfrak{m}_n^r = \pi_n^r\mathcal{O}_n$ und $\mathcal{O}_n = \mathbb{Z}_p[\pi_n]$. Somit ist $\mathfrak{m}_n^r$ ein $\mathbb{Z}_p$-Modul. Da S_n $\mathbb{Q}_p$-linear ist, ist $S_n(\mathfrak{m}_n^r)$ ein $\mathbb{Z}_p$-Untermodul von $\mathbb{Q}_p$, hat also die Gestalt

$$S_n(\mathfrak{m}_n^r) = p^s\mathbb{Z}_p \quad \text{für ein } s \in \mathbb{Z}.$$

Sei s so gewählt, dass es die Ungleichung des Satzes erfüllt. Wegen $e_n s - d_n \leq r$ gilt dann

$$\mathfrak{m}_n^r \subseteq p^s\mathfrak{m}_n^{-d_n} = \mathfrak{m}_n^{e_n s - d_n}$$

und aufgrund von $r < e_n(s+1) - d_n$ gilt

$$p^{s+1}\mathfrak{m}_n^{-d_n} = \mathfrak{m}_n^{e_n(s+1)-d_n} \subsetneq \mathfrak{m}_n^r.$$

Wendet man auf beide Enthaltenseinsrelationen S_n an und beachtet Lemma 4.10, so erhält man

$$S_n(\mathfrak{m}_n^r) \subseteq p^s S_n(\mathfrak{m}_n^{-d_n}) = p^s\mathbb{Z}_p$$

und

$$p^{s+1}\mathbb{Z}_p \subsetneq S_n(\mathfrak{m}_n^r),$$

also

$$S_n(\mathfrak{m}_n^r) = p^s\mathbb{Z}_p.$$

Setzt man insbesondere $r = 1$, so muss s die Ungleichung $s \leq \frac{1+d_n}{e_n} < s+1$ erfüllen, d.h.

$$s = \left[\frac{1+d_n}{e_n}\right] = \left[n + 1 - \frac{p^n - 1}{(p-1)p^n}\right] = \begin{cases} 1, & n = 0, \\ n, & n \geq 1. \end{cases}$$

Hier bezeichne $[x]$ die kleinste ganze Zahl, die kleiner oder gleich x ist. Insbesondere erhält man $S_n(\mathfrak{m}_n) = p^n\mathbb{Z}_p$ für $n \geq 1$ und $S_0(\mathfrak{m}_0) = p\,\mathbb{Z}_p$, wie bereits in Satz 4.9 gezeigt wurde.

QED

An dieser Stelle sei noch eine oft verwendete Abschätzung angegeben.

Satz 4.12 *Für $x \in K_n$ gilt*

$$\nu_n\big(S_n(x)\big) > \nu_n(x) + d_n - e_n = \nu_n(x) + \big(n(p-1)-1\big)p^n.$$

BEWEIS: Setzt man $r := \nu_n(x)$ und wählt s wie in Satz 4.11, so erhält man $x \in \mathfrak{m}_n^r$ und $S_n(x) \in p^s\mathbb{Z}_p$. Daraus folgt

$$\nu_n\big(S_n(x)\big) \geq e_n s > r + d_n - e_n = \nu_n(x) + d_n - e_n.$$

QED

4.4 Das Potenzrestsymbol

In seinem Artikel [Iwa2] beweist K. Iwasawa eine allgemeine Formel für das p^{n+1}-te Hilbertsymbol im Körper K_n der p^{n+1}-ten Einheitswurzeln. Als Spezialfälle dieser Formel ergeben sich die klassischen Formeln von E. Artin und H. Hasse (siehe [AHa]). Da diese jedoch zum Beweis der allgemeinen Formel benötigt werden, ist es notwendig, zunächst die beiden Ergänzungssätze zu beweisen.

Die beiden Ergänzungssätze werden im bereits erwähnten Artikel [AHa] mit Hilfe des Potenzrestsymbols im Körper der m-ten Einheitswurzeln formuliert. Aus diesem Grund wird in diesem Abschnitt zunächst das Potenzrestsymbol eingeführt.

Seien $F = \mathbb{Q}(\zeta)$ mit einer primitiven m-ten Einheitswurzel ζ und $\mathfrak{p}$ ein Primideal in $\mathcal{O}_F$ prim zu m, d.h. $(m,p) = 1$ wenn $\mathfrak{p}$ über der Primzahl p liegt.

Definition 4.13 *Für $u \in \mathcal{O}_F^*$ ist das m-te Potenzrestsymbol durch*

$$\left(\frac{u}{\mathfrak{p}}\right)_m := (\pi, u)_m = \omega(u)^{\frac{q-1}{m}}$$

definiert. Dabei entspricht die rechte Seite dem m-ten Hilbertsymbol (vgl. Theorem 3.12) in der Komplettierung $F_\mathfrak{p}$ von F bezüglich der zum Primideal $\mathfrak{p}$ gehörenden Bewertung $v_\mathfrak{p}$. Weiter ist q die Elementezahl des Restklassenkörpers von $F_\mathfrak{p}$.

Sei $\mathcal{O}_\mathfrak{p}$ der Bewertungsring von $F_\mathfrak{p}$. Das Primideal $\mathfrak{p} \subseteq \mathcal{O}_F$ wird in $F_\mathfrak{p}$ zum maximalen Ideal $\mathfrak{m} \subseteq \mathcal{O}_\mathfrak{p}$, so dass $q = \big|\mathcal{O}_\mathfrak{p}/\mathfrak{m}\big|$.

Lemma 4.14 *Es gilt $\mathcal{O}_F/\mathfrak{p} \cong \mathcal{O}_\mathfrak{p}/\mathfrak{m}$.*

BEWEIS: Sei $\mathcal{O}_{F,\mathfrak{p}}$ die Lokalisierung von $\mathcal{O}_F$ an $\mathfrak{p}$ und sei $\mathfrak{m}_\mathfrak{p} = \mathfrak{p}\mathcal{O}_{F,\mathfrak{p}}$ das maximale Ideal des Ringes $\mathcal{O}_{F,\mathfrak{p}}$. Dann gilt nach [Neu], Kap.I, § 11, Korollar (11.2),

$$\mathcal{O}_F/\mathfrak{p} \cong \mathcal{O}_{F,\mathfrak{p}}/\mathfrak{m}_\mathfrak{p}.$$

Es bleibt die Beziehung $\mathcal{O}_{F,\mathfrak{p}}/\mathfrak{m}_\mathfrak{p} \cong \mathcal{O}_\mathfrak{p}/\mathfrak{m}$ zu zeigen. Die Bewertung $v_\mathfrak{p}$ von F läßt sich auf $\mathcal{O}_{F,\mathfrak{p}}$ übertragen, indem man die Bewertung für $\frac{a}{b} \in \mathcal{O}_{F,\mathfrak{p}},\ a, b \in \mathcal{O}_F,\ b \notin \mathfrak{p}$, gemäß $v_\mathfrak{p}\left(\frac{a}{b}\right) := v_\mathfrak{p}(a) - v_\mathfrak{p}(b)$ definiert. Wegen $b \notin \mathfrak{p}$ ist $v_\mathfrak{p}(b) = 0$ und somit $v_\mathfrak{p}\left(\frac{a}{b}\right) \geq 0$. Dabei ist $v_p\left(\frac{a}{b}\right) \geq 1$ genau dann, wenn $a \in \mathfrak{p}$, d.h. wenn $\frac{a}{b} \in \mathfrak{m}_\mathfrak{p}$. Somit kann man $\mathcal{O}_{F,\mathfrak{p}}$ als Bewertungsring mit maximalem Ideal $\mathfrak{m}_\mathfrak{p}$ auffassen. Die Bewertung ist dieselbe wie in $\mathcal{O}_F$. Es gilt

$$\mathcal{O}_{F,\mathfrak{p}} \subseteq \mathcal{O}_\mathfrak{p},$$

denn einerseits ist $\mathcal{O}_{F,\mathfrak{p}} \subseteq \operatorname{quot}(\mathcal{O}_F) = F \subseteq F_\mathfrak{p}$, andererseits haben die Elemente x aus $\mathcal{O}_{F,\mathfrak{p}}$ eine Bewertung $v_\mathfrak{p}(x) \geq 0$. Für die Elemente $x \in \mathfrak{m}_\mathfrak{p} \subseteq \mathcal{O}_{F,\mathfrak{p}} \subseteq F_\mathfrak{p}$ gilt $v_\mathfrak{p}(x) \geq 1$, so dass $\mathfrak{m}_\mathfrak{p} \subseteq \mathfrak{m}$. Wegen

$$\mathcal{O}_F \subseteq \mathcal{O}_{F,\mathfrak{p}} \subseteq \mathcal{O}_\mathfrak{p} \quad \text{und} \quad \mathfrak{p} \subseteq \mathfrak{m}_\mathfrak{p} \subseteq \mathfrak{m}$$

folgt, dass $\mathcal{O}_\mathfrak{p}$ die Komplettierung von $\mathcal{O}_{F,\mathfrak{p}}$ und $\mathfrak{m}$ die Komplettierung von $\mathfrak{m}_\mathfrak{p}$ ist. Damit gilt nach [Neu], Kap.II, § 4, Satz (4.3),

$$\mathcal{O}_{F,\mathfrak{p}}/\mathfrak{m}_\mathfrak{p} \cong \mathcal{O}_\mathfrak{p}/\mathfrak{m}.$$

Somit ist das Lemma bewiesen.

QED

Nach Lemma 4.14 kann q nun auch als Norm des Ideals $\mathfrak{p}$ geschrieben werden, so dass

$$\left(\frac{u}{\mathfrak{p}}\right)_m = \omega(u)^{\frac{N\mathfrak{p}-1}{m}}.$$

Nach Theorem 3.12 ist Definition 4.13 unabhängig von der Wahl des Primelements $\pi \in \mathcal{O}_\mathfrak{p}$. Das m-te Potenzrestsymbol von $u \in \mathcal{O}_F^*$ ist, nach Definition von $\omega(u)$, die durch

$$\left(\frac{u}{\mathfrak{p}}\right)_m \equiv u^{\frac{N\mathfrak{p}-1}{m}} \mod \mathfrak{p}$$

charakterisierte m-te Einheitswurzel. Insbesondere gilt für $u = \zeta$, dass $\omega(\zeta) = \zeta$ und mit Definition 4.13 folgt

$$\left(\frac{\zeta}{\mathfrak{p}}\right)_m = \zeta^{\frac{N\mathfrak{p}-1}{m}}.$$

Definition 4.15 *Seien $\mathfrak{b} = \prod \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{b})}$ ein Ideal aus $\mathcal{O}_F$ prim zu m und $a \in \mathcal{O}_F^*$. Dann ist das m-te Potenzrestsymbol gemäß*

$$\left(\frac{a}{\mathfrak{b}}\right)_m := \prod \left(\frac{a}{\mathfrak{p}}\right)_m^{v_\mathfrak{p}(\mathfrak{b})}$$

definiert.

Die Bedingung, $\mathfrak{b}$ sei prim zu m, bedeutet, dass für alle in der Primidealzerlegung von $\mathfrak{b}$ vorkommenden Primideale $\mathfrak{p}$ die Beziehung $\mathfrak{p} \nmid m$ gilt. Dies ist gleichbedeutend damit, dass kein derartiges $\mathfrak{p}$ über einem Primteiler von m liegt.

Satz 4.16 *Für ein zu m teilerfremdes Ideal $\mathfrak{a}$ gilt*

$$\left(\frac{\zeta}{\mathfrak{a}}\right)_m = \zeta^{\frac{N\mathfrak{a}-1}{m}}.$$

Für den Beweis ist es zweckmäßig, das Ideal $\mathfrak{a}$ als $\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i$ zu schreiben. Die Primideale $\mathfrak{p}_i$ sind somit nicht notwendigerweise verschieden. Ausgehend von Definition 4.15 und der dieser Definition vorangegangenen Bemerkung erhält man

$$\left(\frac{\zeta}{\mathfrak{a}}\right)_m = \prod_{i=1}^{r} \zeta^{\frac{N\mathfrak{p}_i-1}{m}} = \zeta^{\frac{1}{m}\sum_{i=1}^{r}(N\mathfrak{p}_i-1)}.$$

Andererseits gilt

$$\zeta^{\frac{N\mathfrak{a}-1}{m}} = \zeta^{\frac{1}{m}\left(\prod_{i=1}^{r} N\mathfrak{p}_i-1\right)}.$$

Es ist also die Gleichheit $\frac{1}{m}(N\mathfrak{p}_1 + \ldots + N\mathfrak{p}_r - r) \equiv \frac{1}{m}(N\mathfrak{p}_1 \cdots N\mathfrak{p}_r - 1) \mod m$ bzw.

$$N\mathfrak{p}_1 \cdots N\mathfrak{p}_r - N\mathfrak{p}_1 - \ldots - N\mathfrak{p}_r + (r-1) \equiv 0 \mod m^2$$

zu zeigen.

Sei $\mathfrak{p}$ ein Primideal aus der Primidealzerlegung von $\mathfrak{a}$. Da $\mathfrak{a}$ teilerfremd zu m ist, ist auch $\mathfrak{p}$ teilerfremd zu m. Das heißt, dass die Primzahl p mit $p\,\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$ kein Teiler von m ist. Nach [Neu], Kap. I, § 10, Korollar (10.4), ist p unverzweigt in F und somit sind $e(\mathfrak{p}/p) = 1$ und $f = f(\mathfrak{p}/p) = [F : \mathbb{Q}] = \varphi(m)$. Es folgt $\mathcal{O}_F/\mathfrak{p} = \mathbb{F}_{p^f}$ und

$$N\mathfrak{p} = p^f = p^{\varphi(m)} \equiv 1 \mod m,$$

da p nach Voraussetzung eine Einheit modulo m ist. Da demnach für ein zu m teilerfremdes $\mathfrak{p}$ gilt, dass $N\mathfrak{p} - 1 \equiv 0 \mod m$, genügt es als Beweis von Satz 4.16, das folgende Lemma zu beweisen.

Lemma 4.17 *Seien $a_1, \ldots, a_r$ beliebige natürliche Zahlen. Dann gilt*

$$a_1 \cdots a_r - a_1 - \ldots - a_r + (r-1) = \sum_{s=2}^{r} \sum_{\substack{\{r_1,\ldots,r_s\} \\ \subseteq\{1,\ldots,r\}}} (a_{r_1} - 1)(\ldots)(a_{r_s} - 1).$$

BEWEIS: Der Beweis erfolgt mittels vollständiger Induktion. Der Induktionsanfang für $r = 2$ lautet

$$a_1 a_2 - a_1 - a_2 + (2-1) = (a_1 - 1)(a_2 - 1).$$

Sei die Formel für r bewiesen, nun ist zu zeigen, dass sie auch für $r+1$ gilt. Dafür seien einige Bezeichnungen eingeführt: $\{\ldots\}_j$ steht für j-elementige Teilmengen von $\{1,\ldots,r+1\}$; $\{\ldots\}_j^-$ steht für j-elementige Teilmengen von $\{1,\ldots,r+1\}$, die $r+1$ nicht enthalten, und $\{\ldots\}_j^+$ steht für j-elementige Teilmengen von $\{1,\ldots,r+1\}$, die $r+1$ enthalten. Außerdem sei das Argument in der Doppelsumme mit $(\ldots)$ abgekürzt. Es gilt

$$\begin{aligned}
&\sum_{s=2}^{r+1} \sum_{\substack{\{r_1,\ldots,r_s\}\\ \subseteq\{1,\ldots,r+1\}}} (a_{r_1}-1)(\ldots)(a_{r_s}-1) = \\
&\quad = \sum_{s=2}^{r} \left(\sum_{\{\ldots\}_s^-} (\ldots) + \sum_{\{\ldots\}_s^+} (\ldots) \right) \;+\; (a_1-1)(\cdots)(a_{r+1}-1) \\
&\quad = \sum_{s=2}^{r} \sum_{\{\ldots\}_s^-} (\ldots) \;+\; \sum_{s=2}^{r} \sum_{\{\ldots\}_{s-1}^-} (\ldots)\cdot(a_{r+1}-1) \;+\; (a_1-1)(\cdots)(a_{r+1}-1) \\
&\quad = \sum_{s=2}^{r} \sum_{\{\ldots\}_s^-} (\ldots) \;+\; (a_{r+1}-1)\left(\sum_{s=2}^{r} \sum_{\{\ldots\}_{s-1}^-} (\ldots) + (a_1-1)(\cdots)(a_r-1) \right) \\
&\quad = \sum_{s=2}^{r} \sum_{\{\ldots\}_s^-} (\ldots) \;+\; (a_{r+1}-1) \sum_{s=2}^{r+1} \sum_{\{\ldots\}_{s-1}^-} (\ldots).
\end{aligned}$$

Durch die Substitution $s-1 \to s$ in der zweiten Doppelsumme erhält man äquivalent zur letzten obigen Zeile

$$\begin{aligned}
&= \sum_{s=2}^{r} \sum_{\{\ldots\}_s^-} (\ldots) \;+\; (a_{r+1}-1) \sum_{s=1}^{r} \sum_{\{\ldots\}_s^-} (\ldots) \\
&= \sum_{s=2}^{r} \sum_{\{\ldots\}_s^-} (\ldots) \;+\; (a_{r+1}-1)\left(\sum_{s=2}^{r} \sum_{\{\ldots\}_s^-} (\ldots) + (a_1-1) + \ldots + (a_r-1) \right) \\
&= \sum_{s=2}^{r} \sum_{\{\ldots\}_s^-} (\ldots) \;+\; a_{r+1} \sum_{s=2}^{r} \sum_{\{\ldots\}_s^-} (\ldots) \;-\; \sum_{s=2}^{r} \sum_{\{\ldots\}_s^-} (\ldots) + \\
&\quad + (a_{r+1}-1)\big((a_1-1) + \ldots + (a_r-1)\big).
\end{aligned}$$

Die erste und die dritte Doppelsumme heben sich gegenseitig auf, für die zweite Doppelsumme kann die Induktionsvoraussetzung eingesetzt werden.

$$\begin{aligned}
&= a_{r+1}\big(a_1\cdots a_r - a_1 - \ldots - a_r + (r-1)\big) + (a_{r+1}-1)\big((a_1-1) + \ldots + (a_r-1)\big) \\
&= a_1\cdots a_r a_{r+1} - a_1 - \ldots - a_r - a_{r+1} + r.
\end{aligned}$$

QED

Für ein Hauptideal $\mathfrak{b} = (b)$ von $\mathcal{O}_F$ schreibt man auch

$$\left(\frac{a}{\mathfrak{b}}\right)_m = \left(\frac{a}{b}\right)_m.$$

Sei S die Menge der Primstellen von F (vgl. [Neu], Kap.III, § 1, Definition (1.1)). Zu $\mathfrak{p} \in S$ gehören eine Bewertung $v_\mathfrak{p}$ und eine Komplettierung $F_\mathfrak{p}$ von F. Um zu verdeutlichen, in welcher Komplettierung von F das Hilbertsymbol $(a,b)_m$ betrachtet wird, schreibt man es auch in der Form $\left(\frac{a,b}{\mathfrak{p}}\right)_m$.

Lemma 4.18 *Für $a,\ b \in F^*$ gilt*

$$\prod_{\mathfrak{p}\in S} \left(\frac{a,b}{\mathfrak{p}}\right)_m = 1.$$

Dabei durchläuft $\mathfrak{p}$ alle endlichen und unendlichen Primstellen von F (vgl. [Neu], Kap.VI, § 8, Theorem (8.1)).

Jedes in dem Produkt vorkommende Hilbertsymbol wird in einem anderen lokalen Körper $F_\mathfrak{p}$ gebildet. Für eine unendliche Primstelle $\mathfrak{p}$ ist die zugehörige Bewertung eine archimedesche, und die Komplettierung $F_\mathfrak{p}$ ist isomorph zu $\mathbb{R}$ oder $\mathbb{C}$.

4.5 Spezielle Eigenschaften des Hilbertsymbols

Im folgenden wird der für diese Arbeit interessierende Spezialfall $m = p^{n+1}$ betrachtet. Es ist also $F = \mathbb{Q}(\zeta_n)$ mit einer primitiven p^{n+1}-ten Einheitswurzel. Das p^{n+1}-te Potenzrestsymbol in F bzw. das p^{n+1}-te Hilbertsymbol in den Komplettierungen von F seien von nun an durch den Index n gekennzeichnet.

Zunächst wird eine Verbindung zwischen dem p^{n+1}-ten Potenzrest- und dem p^{n+1}-ten Hilbertsymbol aufgezeigt, um dann im nächsten Kapitel anhand des Artikels [AHa] die beiden Ergänzungssätze für das Hilbertsymbol beweisen zu können.

Satz 4.19 *Das Hilbertsymbol ist stetig. Damit ist gemeint, dass für eine Folge $\{b_j,\ j \in \mathbb{N}\}$ in $(1+\mathfrak{m}_n)$, die gegen $b \in (1+\mathfrak{m}_n)$ konvergiert, die Folge der Hilbertsymbole $\{(a,b_j)_n,\ j \in \mathbb{N}\}$ für ein festes $a \in K_n^*$ gegen $(a,b)_n$ konvergiert.*

Beweis: Für die Konvergenz der Folge der Hilbertsymbole ist zu zeigen, dass

$$(a,b_j)_n(a,b^{-1})_n = (a,b_j\,b^{-1})_n \longrightarrow 1 \quad \text{für} \quad j \to \infty.$$

Dies bedeutet, da $\mu_{p^{n+1}}$ eine endliche Gruppe ist, dass die Existenz eines j_0 gezeigt werden muss, für welches $(a,b_j\,b^{-1})_n = 1$ für $j \geq j_0$ gilt. Äquivalent dazu ist zu zeigen, dass der Quotient $b_j\,b^{-1}$ für $j \geq j_0$ in $K_n^{*p^{n+1}}$ enthalten ist.

Sei $c_j := \log b_j \in \mathfrak{m}_n$. Aufgrund der Stetigkeit des Logarithmus (vgl. Satz 2.2) ist die Folge $\{c_j,\ j \in \mathbb{N}\}$ konvergent, und zwar gegen $c = \log b \in \mathfrak{m}_n$. Somit ist $\{\log\left(b_j\, b^{-1}\right),\ j \in \mathbb{N}\} = \{c_j - c, j \in \mathbb{N}\}$ eine Nullfolge und für die Bewertung gilt

$$\nu_n(c_j - c) \to \infty.$$

Dann gibt es aber auch ein j_0, so dass $\nu_n(c_j - c) \geq (n+1)(p-1)p^n + p^n + 1$ für $j \geq j_0$, d.h. $c_j - c \in \mathfrak{m}_n^{(n+1)(p-1)p^n+p^n+1}$ für $j \geq j_0$. Auf dieser Gruppe ist die Exponentialfunktion gerade die inverse Abbildung des Logarithmus (vgl. Satz 2.3), so dass

$$\begin{aligned} b_j\, b^{-1} = \exp(c_j - c) \in & \left(1 + \mathfrak{m}_n^{(n+1)(p-1)p^n+p^n+1}\right) \\ & = \left(1 + p^{n+1}\mathfrak{m}_n^{p^n+1}\right) = \left(1 + \mathfrak{m}_n^{p^n+1}\right)^{p^{n+1}} \end{aligned}$$

für $j \geq j_0$. Letztere Gleichheit folgt aus Lemma 4.2. Damit ist gezeigt, dass $b_j\, b^{-1}$ für $j \geq j_0$ eine p^{n+1}-te Potenz ist.

QED

In F ist $\pi_n = 1 - \zeta_n$ ein Primteiler von p, das von diesem erzeugte Primideal in $\mathcal{O}_F$ sei $\mathfrak{p}$. Komplettiert man F bezüglich der zu $\mathfrak{p}$ gehörenden Bewertung $v_\mathfrak{p}$, so erhält man $F_\mathfrak{p} = \mathbb{Q}_p(\zeta_n) = K_n$. In K_n wird $\mathfrak{p}$ zu dem maximalen Ideal $\mathfrak{m}_n$. Sei $\mathfrak{p}' \neq \mathfrak{p}$ eine weitere endliche Primstelle. Diese liegt dann über einer Primzahl $p' \neq p$. Mit $F_{\mathfrak{p}'} = \mathbb{Q}_{p'}(\zeta_n)$ folgt aus Satz 2.1, dass $F_{\mathfrak{p}'}/\mathbb{Q}_{p'}$ eine unverzweigte Erweiterung ist. Somit bleibt p' in $F_{\mathfrak{p}'}$ ein Primelement.

Komplettiert man F bezüglich einer archimedeschen Bewertung v, so ist die Komplettierung F_v isomorph zu $\mathbb{C}$, denn in $\mathbb{R}$ gibt es wegen $p \neq 2$ keine p^{n+1}-ten Einheitswurzeln. Dann gilt $L_v = F_v(\sqrt[p^{n+1}]{F_v^*}) = \mathbb{C}$, so dass $G(L_v/F_v) = \{id\}$ und $G(L_v/F_v)^\times = \{1\}$. Das zu v gehörige Hilbertsymbol ist demnach gleich 1 und taucht in der Formel von Lemma 4.18 gar nicht auf.

Satz 4.20 *Sei $b \in F$ mit $b \in (1+\mathfrak{p})$. Dann gilt folgender Zusammenhang zwischen dem p^{n+1}-ten Potenzrestsymbol in F und dem p^{n+1}-ten Hilbertsymbol in K_n,*

$$\left(\frac{\zeta_n}{b}\right)_n = \left(\frac{\zeta_n, b}{\mathfrak{p}}\right)_n = (\zeta_n, b)_n.$$

Beweis: Da $\mathfrak{p}$ das einzige über p liegende Primideal in $\mathcal{O}_F$ ist, sind aufgrund der Voraussetzung an b alle Primideale $\mathfrak{p}'$, die das Ideal (b) teilen, teilerfremd zu p,

also auch teilerfremd zu p^{n+1}. Damit gilt

$$\left(\frac{\zeta_n}{b}\right)_n = \prod_{\mathfrak{p}'|(b)} \left(\frac{\zeta_n}{\mathfrak{p}'}\right)_n^{v_{\mathfrak{p}'}(b)} = \prod_{\mathfrak{p}'|(b)} \left(\frac{p', \zeta_n}{\mathfrak{p}'}\right)_n^{v_{\mathfrak{p}'}(b)} = \prod_{\mathfrak{p}'|(b)} \left(\frac{b, \zeta_n}{\mathfrak{p}'}\right)_n$$
$$= \left(\prod_{\mathfrak{p}'|(b)} \left(\frac{\zeta_n, b}{\mathfrak{p}'}\right)_n\right)^{-1} = \prod_{\mathfrak{p}' \nmid (b)} \left(\frac{\zeta_n, b}{\mathfrak{p}'}\right)_n.$$

Bisher wurden die Eigenschaften des Hilbertsymbols aus Satz 3.11 und das Lemma 4.18 verwendet. Unter den Primidealen $\mathfrak{p}'$, die (b) nicht teilen, ist auch das Ideal $\mathfrak{p}$. Für alle von $\mathfrak{p}$ verschiedenen Primideale $\mathfrak{p}'$, die (b) nicht teilen, wird das Hilbertsymbol $\left(\frac{\zeta_n, b}{\mathfrak{p}'}\right)_n$ in dem lokalen Körper $F_{\mathfrak{p}'} = \mathbb{Q}_{p'}(\zeta_n)$ mit $p'\mathbb{Z} = \mathfrak{p}' \cap \mathbb{Z}$ betrachtet. Wegen $(p', p) = 1$ kann das explizite Reziprozitätsgesetz Theorem 3.12 angewandt werden, so dass diese Hilbertsymbole, da sowohl ζ_n als auch b Einheiten des jeweiligen Bewertungsringes $\mathcal{O}_{\mathfrak{p}'}$ sind, alle identisch 1 werden. Somit gilt

$$\left(\frac{\zeta_n}{b}\right)_n = \prod_{\mathfrak{p}' \nmid (b)} \left(\frac{\zeta_n, b}{\mathfrak{p}'}\right)_n = \left(\frac{\zeta_n, b}{\mathfrak{p}}\right)_n \cdot \prod_{\substack{\mathfrak{p}' \nmid (b) \\ \mathfrak{p}' \neq \mathfrak{p}}} \left(\frac{\zeta_n, b}{\mathfrak{p}'}\right)_n = \left(\frac{\zeta_n, b}{\mathfrak{p}}\right)_n.$$

QED

Satz 4.21 *Sei b ein Element des lokalen Körpers K_n mit $b \in (1 + \mathfrak{m}_n)$. Dann gilt für das p^{n+1}-te Hilbertsymbol*

$$(\zeta_n, b)_n = \zeta_n^{\frac{N_n(b)-1}{p^{n+1}}}.$$

Beweis: Der globale Körper F liegt dicht in dem Körper K_n, da K_n gerade die Komplettierung von F bezüglich der zu $\mathfrak{p}$ gehörigen Bewertung ist. Genauso liegt auch die Gruppe $(1+\mathfrak{p})$ dicht in der Gruppe $(1+\mathfrak{m}_n)$. Somit läßt sich $b \in (1+\mathfrak{m}_n)$ durch eine Folge $\{b_j,\ j \in \mathbb{N}\} \subseteq (1 + \mathfrak{p})$ approximieren.

Für $b_j \in (1 + \mathfrak{p})$ gilt nach Satz 4.20 und Satz 4.16

$$(\zeta_n, b_j)_n = \left(\frac{\zeta_n}{b_j}\right) = \zeta_n^{\frac{N(b_j)-1}{p^{n+1}}}.$$

Da aber sowohl das Hilbertsymbol (vgl. Satz 4.19) als auch die rechte Seite der Behauptung stetig in b_j sind, folgt die Behauptung auch für den Grenzwert $b \in (1 + \mathfrak{m}_n)$.

QED

Abschließend sei noch eine Eigenschaft des p^{n+1}-ten Hilbertsymbols bewiesen, welche später im Beweis des expliziten Reziprozitätsgesetzes in Kapitel 5.2 verwendet wird.

Satz 4.22 *Sei $m > n$. Dann gilt für $a \in K_m^*,\ b \in K_n^*$ die Gleichheit*

$$\big(N_{mn}(a), b\big)_n = (a, b)_m^{p^{m-n}}.$$

BEWEIS: Für $n \geq 0$ sei $L_n := K_n(\sqrt[p^{n+1}]{K_n^*})$. Nach [Neu], Kap.IV, § 6, Satz (6.4) ist das folgende Diagramm kommutativ,

$$\begin{array}{ccc} K_m^* & \xrightarrow{(\,.\,, L_m/K_m)} & G(L_m/K_m) \\ {\scriptstyle N_{mn}}\downarrow & & \downarrow \\ K_n^* & \xrightarrow[(\,.\,, L_m/K_m)]{} & G(L_n/K_n) \end{array}$$

d.h. für $a \in K_m^*$ gilt $\big(N_{mn}(a), L_n/K_n\big) = \big(a, L_m/K_m\big)_{|_{L_n}}$. Mit Hilfe der Beziehung zwischen Normrestsymbol und Hilbertsymbol aus dem Beweis zu Satz 3.11 erhält man für $b \in K_n^*$

$$\begin{aligned} \big(N_{mn}(a), b\big)_n \,^{p^{n+1}}\!\sqrt{b} &= \big(N_{mn}(a), L_n/K_n\big)\,^{p^{n+1}}\!\sqrt{b} \\ &= \big(a, L_m/K_m\big)\,^{p^{m+1}}\!\sqrt{b^{p^{m-n}}} \\ &= \big(a, b^{p^{m-n}}\big)_m \,^{p^{m+1}}\!\sqrt{b^{p^{m-n}}}. \end{aligned}$$

Daraus folgt

$$\big(N_{mn}(a), b\big)_n = \big(a, b^{p^{m-n}}\big)_m = \big(a, b\big)_m^{p^{m-n}}.$$

QED

Kapitel 5

Das explizite Reziprozitätsgesetz

Das Ziel dieses Kapitels ist es, das explizite Reziprozitätsgesetz im Körper $\mathbb{Q}_p(\zeta_n)$ der p^{n+1}-ten Einheitswurzeln anhand von Iwasawas Artikel [Iwa2] zu beweisen. Wie bereits zu Beginn von Abschnitt 4.4 erwähnt, ist es zuvor jedoch notwendig, die beiden Ergänzungssätze zu beweisen.

Das p^{n+1}-te Hilbertsymbol für $a, b \in K_n$ werde weiterhin mit $(a,b)_n$ bezeichnet. Da der Wert $(a,b)_n$ eine p^{n+1}-te Einheitswurzel ist, kann man auch

$$(a,b)_n = \zeta_n^{f_n(a,b)}$$

mit einem von a, b und n abhängigen Exponenten schreiben. Dieser sei im Folgenden mit $[a,b]_n$ bezeichnet, es gilt also

$$(a,b)_n = \zeta_n^{[a,b]_n}.$$

Aufgrund der in Satz 3.11 angegebenen Eigenschaften des Hilbertsymbols, erhält man für $[\,.\,,\,.\,]_n$ folgende Eigenschaften.

Lemma 5.1

(i) $[\,.\,,\,.\,]_n$ *ist eine ganze p-adische Zahl, die modulo* p^{n+1} *eindeutig bestimmt ist.*

(ii) *Für* $a, a', a'', b, b', b'' \in K_n^*$ *gilt* $\quad [a'a'', b]_n = [a', b]_n + [a'', b]_n,$
$\qquad\qquad\qquad\qquad\qquad\qquad\quad [a, b'b'']_n = [a, b']_n + [a, b'']_n.$

(iii) *Gilt* $[a,b]_n = 0$ *für alle* $b \in K^*$, *so ist* $a \in K^{*p^{n+1}}$.

(iv) *Es gilt* $[a,b]_n = -[b,a]_n$.

5.1 Die beiden Ergänzungssätze

Die Ausführungen in diesem Abschnitt orientieren sich an dem Artikel [AHa] von E. Artin und H. Hasse. Allerdings wird hier der Beweis der beiden Ergänzungssätze nicht wie bei Artin-Hasse in der globalen Situation für das p^{n+1}-te

Potenzrestsymbol, sondern in der lokalen Situation für das p^{n+1}-te Hilbertsymbol erbracht.

Es sei noch darauf hingewiesen, dass ζ_n in dem Artikel von E. Artin und H. Hasse nicht wie in dieser Arbeit eine p^{n+1}-te, sonder eine p^n-te Einheitswurzel bezeichnet.

Nun werden die beiden Ergänzungssätze für den Hilbertsymbol-Exponenten $[.,.]_n$ formuliert.

Theorem 5.2 *Sei $K_n = \mathbb{Q}_p(\zeta_n)$ mit einer primitiven p^{n+1}-ten Einheitswurzel ζ_n und sei $\pi_n = 1 - \zeta_n$ ein Primelement im Bewertungsring $\mathcal{O}_n$ von K_n. Das von π_n erzeugte maximale Ideal in $\mathcal{O}_n$ ist $\mathfrak{m}_n$. Für $\beta \in 1 + \mathfrak{m}_n$ gelten die beiden Ergänzungssätze*

$$[\zeta_n, \beta]_n = \frac{1}{p^{n+1}}\, S_n(\log \beta) \qquad \text{Erster Ergänzungssatz,}$$

$$[\pi_n, \beta]_n = -\frac{1}{p^{n+1}}\, S_n\Big(\frac{\zeta_n}{\pi_n} \log \beta\Big) \qquad \text{Zweiter Ergänzungssatz.}$$

Beweis des ersten Ergänzungssatzes: Sei $\beta \in (1 + \mathfrak{m}_n)$. Nach Satz 4.20 und Satz 4.16 gilt

$$(\zeta_n, \beta)_n = \left(\frac{\zeta_n}{\beta}\right)_n = \zeta_n^{\frac{N_n(\beta)-1}{p^{n+1}}},$$

insbesondere gilt $p^{n+1} \,\big|\, \big(N_n(\beta) - 1\big)$. Es ist also zu zeigen, dass

$$\frac{N_n(\beta) - 1}{p^{n+1}} \equiv \frac{S_n(\log \beta)}{p^{n+1}} \mod p^{n+1}.$$

Zunächst sei bemerkt, dass aus der Reihendarstellung des Logarithmus (vgl. Satz 2.2) die Gleichung $\log N_n(\beta) = S_n(\log \beta)$ folgt. Da für $\beta \in (1 + \mathfrak{m}_n)$ stets die Beziehung

$$N_n(\beta) \equiv 1 \mod p^{n+1}$$

erfüllt ist, gilt

$$S_n(\log \beta) \equiv 0 \mod p^{n+1}.$$

Somit repräsentieren $\frac{N_n(\beta)-1}{p^{n+1}}$ und $\frac{S_n(\log \beta)}{p^{n+1}}$ immer eine ganzzahlige Restklasse modulo p^{n+1} und die Kongruenzen

$$\frac{N_n(\beta) - 1}{p^{n+1}} \equiv 0 \mod p^{n+1} \quad \text{und} \quad \frac{S_n(\log \beta)}{p^{n+1}} \equiv 0 \mod p^{n+1} \tag{5.1}$$

bedingen sich gegenseitig. Betrachtet man die Abbildungen

$$\mathcal{N},\, \mathcal{S} : (1 + \mathfrak{m}_n) \to \mathbb{Z}/p^{n+1}\mathbb{Z}, \quad \mathcal{N}(x) := \frac{N_n(x) - 1}{p^{n+1}}, \quad \mathcal{S}(x) := \frac{S_n(\log x)}{p^{n+1}},$$

so gilt zum einen $\mathcal{N}(xy) = \mathcal{N}(x) + \mathcal{N}(y)$ wegen Lemma 4.17 und zum anderen $\mathcal{S}(xy) = \mathcal{S}(x) + \mathcal{S}(y)$ aufgrund der Funktionalgleichung des Logarithmus. Beide Gruppenhomomorphismen haben wegen Gleichung (5.1) denselben Kern $H := \ker \mathcal{N} = \ker \mathcal{S}$. Da die Faktorgruppe $(1+\mathfrak{m}_n)/H$ isomorph ist zum jeweiligen Bild $\operatorname{im}\mathcal{N}$ von $\mathcal{N}$ bzw. $\operatorname{im}\mathcal{S}$ von $\mathcal{S}$, sind die Bilder ebenfalls isomorph, $G := \operatorname{im}\mathcal{N} \cong \operatorname{im}\mathcal{S}$. Man hat also zwei Isomorphismen

$$\mathcal{N},\, \mathcal{S} : (1+\mathfrak{m}_n)/H \cong G.$$

Wegen $G \subseteq \mathbb{Z}/p^{n+1}\mathbb{Z}$ ist G eine zyklische Gruppe. Somit existiert für jedes $x \in (1+\mathfrak{m}_n)/H$ ein $c_x \in G$, so dass $\mathcal{N}(x) = c_x \mathcal{S}(x)$. Da $\mathcal{N}$ und $\mathcal{S}$ Isomorphismen sind, ist $(1+\mathfrak{m}_n)/H$ zyklisch, und es existiert ein Erzeuger x_0 von $(1+\mathfrak{m}_n)/H$, so dass $\mathcal{N}(x_0)$ bzw. $\mathcal{S}(x_0)$ die Gruppe G erzeugen. Sei $c \in G$ mit $\mathcal{N}(x_0) = c\mathcal{S}(x_0)$. Wählt man nun $x \in (1+\mathfrak{m}_n)/H$ beliebig, so gilt $x = x_0^{r_x}$ mit einem $r_x \in \mathbb{N}$ und man erhält

$$\mathcal{N}(x) = \mathcal{N}(x_0^{r_x}) = r_x \mathcal{N}(x_0) = r_x c\, \mathcal{S}(x_0) = c\, \mathcal{S}(x_0^{r_x}) = c\, \mathcal{S}(x).$$

Damit ist die Beziehung

$$\frac{N_n(x)-1}{p^{n+1}} \equiv c\, \frac{S_n(\log x)}{p^{n+1}} \mod p^{n+1}$$

mit einem von x unabhängigen Faktor c gezeigt.

Dieser Faktor c kann nun bestimmt werden, indem man für x einen speziellen Wert einsetzt. Sei $x_0 = \exp\left(\frac{p}{p-1}\right)$. Wegen $\nu_n\left(\frac{p}{p-1}\right) = (p-1)p^n v_p\left(\frac{p}{p-1}\right) = (p-1)p^n > p^n$ gilt mit Lemma 4.1, dass $\log x_0 = \frac{p}{p-1}$. Somit ist $S_n(\log x_0) = p^{n+1}$ und

$$\frac{S_n(\log x_0)}{p^{n+1}} = 1.$$

Mit $N_n\big(\exp(y)\big) = \exp\big(S_n(y)\big)$ für beliebiges $y \in (1+\mathfrak{m}_n)$ folgt $N_n(x_0) = \exp\left(p^{n+1}\right)$ und

$$\frac{N_n(x_0)-1}{p^{n+1}} = \frac{\exp\left(p^{n+1}\right)-1}{p^{n+1}} = \sum_{k\geq 1} \frac{p^{(k-1)(n+1)}}{k!} = 1 + \sum_{k\geq 2} \frac{p^{(k-1)(n+1)}}{k!}.$$

Nach [Neu], Kap.II, § 5, Lemma (5.6), gilt für eine natürliche Zahl k, dass $v_p(k!) = \frac{k-s_k}{p-1}$, wobei für $k = \sum a_j p^j > 0$ die p-adische Ziffernsumme s_k gemäß $s_k := \sum a_j \geq 1$ definiert ist. Damit folgt nun für einen Summanden aus der Summe über $k \geq 2$

$$\begin{aligned} v_p\Big(\tfrac{p^{(k-1)(n+1)}}{k!}\Big) &= (k-1)(n+1) - \tfrac{k-s_k}{p-1} \geq (k-1)(n+1) - \tfrac{k-1}{p-1} \\ &> (k-1)(n+1) - (k-1) = (k-1)n \geq n, \end{aligned}$$

also $v_p\big(\frac{p^{(k-1)(n+1)}}{k!}\big) \geq n+1$. Somit ist

$$\frac{N_n(x_0)-1}{p^{n+1}} \equiv 1 \mod p^{n+1}.$$

Daraus folgt $c = 1$ und der erste Ergänzungssatz ist bewiesen.

QED

Bevor der zweite Ergänzungssatz bewiesen wird, sei an dieser Stelle an die Möbiussche μ-Funktion erinnert. Sie ist für $r \in \mathbb{N}$ durch die Eigenschaft

$$\sum_{k|r} \mu\Big(\frac{r}{k}\Big) = \sum_{k|r} \mu(k) = \begin{cases} 1, & r = 1 \\ 0, & \text{sonst} \end{cases}$$

definiert (vgl. [Ha2], Kap.I, § 2, S. 15). Mit Hilfe der μ-Funktion kann man folgende Umkehrformel beweisen.

Lemma 5.3 *Für zwei Funktionen F und f gelte die Beziehung*

$$F(x) = \sum_{\substack{m\geq 1 \\ (m,p)=1}} \frac{f(x^m)}{m}.$$

Dann gilt die Umkehrformel

$$f(x) = \sum_{\substack{m\geq 1 \\ (m,p)=1}} \frac{\mu(m)}{m} F(x^m),$$

wobei μ die Möbiussche μ-Funktion bezeichnet.

Beweis: Aus der Voraussetzung folgen die beiden Gleichungen

$$F(x^k) = \sum_{\substack{m\geq 1 \\ (m,p)=1}} \frac{f(x^{km})}{m} \quad \text{und} \quad \sum_{\substack{k\geq 1 \\ (k,p)=1}} \mu(k)\frac{F(x^k)}{k} = \sum_{\substack{k\geq 1 \\ (k,p)=1}} \sum_{\substack{m\geq 1 \\ (m,p)=1}} \mu(k)\frac{f(x^{km})}{km}.$$

Für ein festes $r := km$ auf der rechten Seite der zweiten Gleichung durchläuft k alle Teiler von r. Somit folgt

$$\sum_{\substack{k\geq 1 \\ (k,p)=1}} \mu(k)\frac{F(x^k)}{k} = \sum_{\substack{r\geq 1 \\ (r,p)=1}} \sum_{k|r} \mu(k)\,\frac{f(x^r)}{r}.$$

Aufgrund der definierenden Eigenschaft der Möbiusschen μ-Funktion bleibt in obiger Summe nur der Summand für $r = 1$ übrig,

$$\sum_{\substack{k\geq 1 \\ (k,p)=1}} \mu(k)\frac{F(x^k)}{k} = f(x).$$

Dies entspricht gerade der Behauptung.

QED

Die folgenden beiden Lemmata über Binomialkoeffizienten sind als Hilfssätze am Ende des Artikels [AHa] angegeben.

Lemma 5.4 *Seien $a, b \in \mathbb{N}$ mit $a > 0$ und $a \geq b \geq 0$. Seien $\alpha = v_p(a),\ \beta = v_p(b)$. Dann gilt*

$$\binom{a}{b} \equiv 0 \mod p^{\max\{0,\alpha-\beta\}},$$

d.h. $v_p\big(\binom{a}{b}\big) \geq \max\{0, \alpha - \beta\}$.

Beweis: Falls $\alpha \leq \beta$, so ist $\max\{0, \alpha-\beta\} = 0$ und die Behauptung ist klar, denn wegen $\binom{a}{b} \in \mathbb{N}$ gilt stets $v_p\big(\binom{a}{b}\big) \geq 0$. Falls $\alpha > \beta$, so folgt

$$\begin{aligned} v_p\Big(\binom{a}{b}\Big) &= v_p\Big(\binom{a-1}{b-1}\frac{a}{b}\Big) \\ &= v_p\Big(\binom{a-1}{b-1}\Big) + (\alpha - \beta) \ \geq\ \alpha - \beta \ =\ \max\{0, \alpha - \beta\}. \end{aligned}$$

QED

Lemma 5.5 *Seien $a_0, b \in \mathbb{N}$ mit $(a_0, p) = 1,\ 0 \leq b \leq a_0 p^\alpha$ und $\alpha \geq 1$. Dann gilt*

$$\binom{a_0 p^\alpha}{bp} \equiv \binom{a_0 p^{\alpha-1}}{b} \mod p^{2\alpha}.$$

Beweis: Für $b = 0$ ist die Behauptung klar. Sei also $b > 0$. Dann ist

$$\begin{aligned} \binom{a_0 p^\alpha}{bp} &= a_0 p^\alpha \frac{a_0 p^\alpha - 1}{1} \frac{a_0 p^\alpha - 2}{2} \cdots \frac{a_0 p^\alpha - (bp-1)}{bp-1} \frac{1}{bp} \\ &= \frac{a_0 p^\alpha (a_0 p^\alpha - p) \cdots \big(a_0 p^\alpha - (bp-p)\big)}{p \cdot 2p \cdots (b-1)p \cdot bp} \prod_{\substack{(j,p)=1 \\ j=1\ldots bp}} \frac{a_0 p^\alpha - j}{j}. \end{aligned}$$

Im ersten Faktor läßt sich b-mal der Faktor p aus Zähler und Nenner herauskürzen, so dass man $\binom{a_0 p^{\alpha-1}}{b}$ erhält. Aus dem Produkt wird für jeden der $b(p-1)$ Faktoren der Faktor -1 herausgezogen. Da $b(p-1)$ gerade ist, ergeben diese zusammen $+1$. Man erhält somit

$$\binom{a_0 p^\alpha}{bp} \ =\ \binom{a_0 p^{\alpha-1}}{b} \prod_{\substack{(j,p)=1 \\ j=1\ldots bp}} \Big(1 - \frac{a_0 p^\alpha}{j}\Big).$$

Unter der Annahme $b = b_0 p^{\beta-1},\ (b_0, p) = 1,\ \beta \geq 1$, ergibt sich das obige Produkt zu

$$\prod_{\substack{(j,p)=1\\ j=1\ldots b_0 p^\beta}} \Big(1 - \frac{a_0 p^\alpha}{j}\Big) \ \equiv\ 1 - a_0 p^\alpha \sum_{\substack{(j,p)=1\\ j=1\ldots b_0 p^\beta}} \frac{1}{j} \mod p^{2\alpha}.$$

In der Summe durchläuft j b_0-mal ein primes Restsystem modulo p^β. Somit durchläuft auch $\frac{1}{j}$ b_0-mal ein primes Restsystem modulo p^β. Dieses Restsystem enthält $(p-1)p^{\beta-1}$ Elemente. Da dies eine gerade Anzahl ist, können je zwei entgegengesetzte Restklassen immer zu Null zusammengefasst werden, so dass

$$\sum_{\substack{(j,p)=1\\ j=1\ldots b_0 p^\beta}} \frac{1}{j} \equiv 0 \mod p^\beta \quad \text{bzw.} \quad a_0 p^\alpha \sum_{\substack{(j,p)=1\\ j=1\ldots b_0 p^\beta}} \frac{1}{j} \equiv 0 \mod p^{\alpha+\beta}.$$

Damit ergibt sich

$$\prod_{\substack{(j,p)=1\\ j=1\ldots b_0 p^\beta}} \Big(1 - \frac{a_0 p^\alpha}{j}\Big) \equiv 1 \mod p^{\alpha+\min\{\alpha,\beta\}}.$$

Beachtet man noch, dass nach Lemma 5.4 die beiden Binomialkoeffizienten $\binom{a_0 p^\alpha}{bp}$ und $\binom{a_0 p^{\alpha-1}}{b}$ durch $p^{\max\{0,\alpha-\beta\}} = p^{\max\{\alpha,\beta\}-\beta}$ teilbar sind, so ergibt sich zusammen mit $\min\{\alpha,\beta\} + \max\{\alpha,\beta\} = \alpha + \beta$ aus den letzten Überlegungen

$$\begin{aligned}
\binom{a_0 p^\alpha}{bp} &\equiv \binom{a_0 p^{\alpha-1}}{b} \cdot 1 \mod p^{\alpha+\min\{\alpha,\beta\}} \\
&\equiv \binom{a_0 p^{\alpha-1}}{b} \mod p^{(\alpha+\min\{\alpha,\beta\})+(\max\{\alpha,\beta\}-\beta)} \\
&\equiv \binom{a_0 p^{\alpha-1}}{b} \mod p^{2\alpha}.
\end{aligned}$$

QED

Beweis des zweiten Ergänzungssatzes: Für $\beta \in (1 + \mathfrak{m}_n)$ ist

$$(\pi_n, \beta)_n = \zeta_n^{\frac{1}{p^{n+1}} S_n\left(-\frac{\zeta_n}{\pi_n} \log \beta\right)}$$

zu zeigen. Zunächst wird die Behauptung für $\beta_0 \in \big(1 + \mathfrak{m}_n^{(n+1)(p-1)p^n + p^n + 1}\big)$ bewiesen. Für ein derartiges β_0 gilt mit Lemma 5.19 die Gleichheit $(\pi_n, \beta_0)_n = 1$. Es ist also

$$\frac{1}{p^{n+1}} S_n\Big(-\frac{\zeta_n}{\pi_n} \log \beta_0\Big) \equiv 0 \mod p^{n+1}$$

nachzuweisen. Aufgrund der Voraussetzung an β_0 und Lemma 4.1 gilt $\log \beta_0 \in \mathfrak{m}_n^{(n+1)(p-1)p^n + p^n + 1}$. Daraus folgt $\log \beta_0 \equiv 0 \mod p^{n+1}\pi_0\pi_n$ und

$$-p^{-(n+1)} \frac{\zeta_n}{\pi_n} \log \beta_0 \equiv 0 \mod \pi_0.$$

Somit erhält man

$$-\frac{1}{p^{n+1}}\frac{\zeta_n}{\pi_n}\log\beta_0 = \pi_0 y \quad \text{mit} \quad y \in \mathcal{O}_n.$$

Aufgrund von $S_{n0}(y) \equiv 0 \mod p^n$ für alle $y \in \mathcal{O}_n$ (vgl. Gleichung (4.1)) folgt $p^{-(n+1)}S_{n0}\big(-\frac{\zeta_n}{\pi_n}\log\beta_0\big) \equiv 0 \mod \pi_0 p^n$, d.h. es gilt

$$p^{-(n+1)}S_{n0}\Big(-\frac{\zeta_n}{\pi_n}\log\beta_0\Big) = \pi_0 p^n y_0$$

mit einem $y_0 \in \mathcal{O}_0$. Mit $S_0(\mathfrak{m}_0) = p\mathbb{Z}_p$ (vgl. Satz 4.9) schlussfolgert man schließlich

$$\frac{1}{p^{n+1}}\,S_n\Big(-\frac{\zeta_n}{\pi_n}\log\beta_0\Big) = p^n S_0(y_0\pi_0) \equiv 0 \mod p^{n+1}.$$

Nach dieser Vorarbeit genügt es nun, den zweiten Ergänzungssatz für alle Elemente von

$$H := \{x \in \mathcal{O}_n/\mathfrak{m}_n^{(n+1)(p-1)p^n+p^n+1} : x \equiv 1 \mod \mathfrak{m}_n\}$$

zu beweisen. Nach [Ha2], Kap.II, § 15, (d), Aussage (II), ist $\{1-\pi_n^a,\ 1 \le a \le p^{n+1},$ $(a,p) = 1$ oder $a = p^{n+1}\}$ ein Erzeugendensystem von $(1+\mathfrak{m}_n)$, insbesondere auch ein Erzeugendensystem der Gruppe H. An dieser Stelle soll jedoch ein Erzeugendensystem $\{\tau_a\}$ derart konstruiert werden, dass es der Gleichung

$$\log\tau_a = -\sum_{k=0}^{\infty}\frac{\pi_n^{ap^k}}{p^k} \tag{5.2}$$

genügt. Unter Verwendung der Potenzreihe $g(x) := -\sum_{k=0}^{\infty}\frac{x^{p^k}}{p^k}$ soll für die Elemente des Erzeugendensystem also $\log\tau_a = g(\pi_n^a)$ gelten. Die Gleichung

$$\log(1-x) = -\sum_{r=0}^{\infty}\frac{x^r}{r} = -\sum_{\substack{m\ge1\\(m,p)=1}}\sum_{k=0}^{\infty}\frac{x^{mp^k}}{mp^k} = \sum_{\substack{m\ge1\\(m,p)=1}}\frac{g(x^m)}{m} \tag{5.3}$$

ist eine formale Identität von Potenzreihen. Mit Hilfe von Lemma 5.3 läßt sie sich umkehren zu

$$g(x) = \sum_{\substack{m\ge1\\(m,p)=1}}\frac{\mu(m)}{m}\log(1-x^m) = \log\Big(\prod_{\substack{m\ge1\\(m,p)=1}}(1-x^m)^{\frac{\mu(m)}{m}}\Big). \tag{5.4}$$

Dementsprechend wählt man

$$\tau_a := \prod_{\substack{m\ge1\\(m,p)=1}}(1-\pi_n^{am})^{\frac{\mu(m)}{m}},$$

bzw. die dazu modulo $\mathfrak{m}_n^{(n+1)(p-1)p^n+p^n+1}$ kongruenten Zahlen aus $\mathcal{O}_n$. Wegen $\tau_a \equiv 1-\pi_n^a \mod \pi_n^{a+1}$ bilden die τ_a, $1 \le a \le p^{n+1}$, $(a,p) = 1$ oder $a = p^{n+1}$,

ein Erzeugendensystem von H.

Der zweite Ergänzungssatz wird nun für die Elemente τ_a bewiesen, indem zunächst der Exponent c_a in der Gleichung $(\pi_n, \tau_a)_n = \zeta_n^{c_a}$ bestimmt wird und dann $p^{-(n+1)} S_n\big(-\frac{\zeta_n}{\pi_n}\log\tau_a\big) \equiv c_a \mod p^{n+1}$ nachgewiesen wird.

Es gilt $(\pi_n, 1-\pi_n^a)_n^a = (\pi_n^a, 1-\pi_n^a)_n = 1$, so dass für $(a,p)=1$ die Beziehung $(\pi_n, 1-\pi_n^a)_n = 1$ folgt. Wegen $(am,p)=1$ ergibt sich somit

$$(\pi_n, \tau_a)_n = \prod_{\substack{m\geq 1\\(m,p)=1}} (\pi_n, 1-\pi_n^{am})_n^{\frac{\mu(m)}{m}} = 1.$$

Sei nun $a = p^{n+1}$. Aufgrund von $(\zeta_n^i\pi_n^m, 1-\zeta_n^i\pi_n^m)_n = 1$ gilt allgemein

$$(\pi_n^m, 1-\zeta_n^i\pi_n^m)_n = (\zeta_n^{-i}, 1-\zeta_n^i\pi_n^m)_n = (\zeta_n, 1-\zeta_n^i\pi_n^m)_n^{-i}.$$

Mit Hilfe der Gleichung $1-X^{p^{n+1}} = \prod_{i=0}^{p^{n+1}-1}\big(1-\zeta_n^i X\big)$ erhält man die Identität $1-\pi_n^{mp^{n+1}} = \prod_{i=0}^{p^{n+1}-1}(1-\zeta_n^i\pi_n^m)$. Damit folgt

$$\begin{aligned}(\pi_n, \tau_{p^{n+1}})_n &= \prod_{\substack{m\geq 1\\(m,p)=1}} (\pi_n, 1-\pi_n^{mp^{n+1}})_n^{\frac{\mu(m)}{m}} = \prod_{\substack{m\geq 1\\(m,p)=1}} \prod_{i=0}^{p^{n+1}-1} (\pi_n, 1-\zeta_n^i\pi_n^m)_n^{\frac{\mu(m)}{m}}\\ &= \prod_{\substack{m\geq 1\\(m,p)=1}} \prod_{i=0}^{p^{n+1}-1} (\zeta_n, 1-\zeta_n^i\pi_n^m)_n^{-\frac{i}{m}\frac{\mu(m)}{m}}.\end{aligned}$$

Da es in dem Produkt über i nur auf die Restklasse modulo p^{n+1} ankommt, kann man wegen $(m,p)=1$ auch $i = jm,\ j = 0,\dots,p^{n+1}-1$ schreiben. Unter Verwendung des ersten Ergänzungssatzes ergibt sich

$$\begin{aligned}(\pi_n, \tau_{p^{n+1}})_n &= \prod_{\substack{m\geq 1\\(m,p)=1}} \prod_{j=0}^{p^{n+1}-1} (\zeta_n, 1-\zeta_n^{jm}\pi_n^m)_n^{-j\frac{\mu(m)}{m}}\\ &= \prod_{j=0}^{p^{n+1}-1} \prod_{\substack{m\geq 1\\(m,p)=1}} \zeta_n^{-j\frac{\mu(m)}{m}\frac{1}{p^{n+1}}S_n\left(\log(1-\zeta_n^{jm}\pi_n^m)\right)} = \zeta_n^A\end{aligned}$$

mit

$$A := -\sum_{j=0}^{p^{n+1}-1} \frac{j}{p^{n+1}}\, S_n\Big(\sum_{\substack{m\geq 1\\(m,p)=1}} \frac{\mu(m)}{m}\log(1-\zeta_n^{jm}\pi_n^m)\Big).$$

Mit Hilfe von Gleichung (5.4) und der Definition der Funktion g erhält man

$$A = -\sum_{j=0}^{p^{n+1}-1} \frac{j}{p^{n+1}}\, S_n\big(g(\zeta_n^j\pi_n)\big) = \sum_{k=0}^{\infty}\frac{1}{p^k}\, S_n\Big(\frac{\pi_n^{p^k}}{p^{n+1}}\sum_{j=0}^{p^{n+1}-1} j\zeta_n^{jp^k}\Big).$$

Sei $f(x) := \sum_{j=0}^{p^{n+1}-1} x^j = \frac{x^{p^{n+1}}-1}{x-1}$. Dann gilt

$$\sum_{j=0}^{p^{n+1}-1} j\, x^j = x f'(x) = p^{n+1}\frac{x^{p^{n+1}}}{x-1} - x\,\frac{x^{p^{n+1}}-1}{(x-1)^2},$$

so dass die Beziehung

$$x f'(x)\big|_{x=\zeta_n^{p^k}} = \sum_{j=0}^{p^{n+1}-1} j\,\zeta_n^{jp^k} = \frac{p^{n+1}}{\zeta_n^{p^k}-1} \qquad \text{für} \qquad k \le n$$

folgt. Für $k \ge n+1$ ist $\zeta_n^{jp^k} = 1$ und damit ergibt sich

$$\sum_{j=0}^{p^{n+1}-1} j\,\zeta_n^{jp^k} = \sum_{j=0}^{p^{n+1}-1} j = p^{n+1}\frac{p^{n+1}-1}{2}.$$

Somit schließt man

$$\begin{aligned} A &= \sum_{k=0}^{n} \frac{1}{p^k}\, S_n\Big(\frac{\pi_n^{p^k}}{\zeta_n^{p^k}-1}\Big) + \sum_{k\ge n+1} \frac{1}{p^k}\frac{p^{n+1}-1}{2}\, S_n\big(\pi_n^{p^k}\big) \\ &= \qquad B \qquad + \qquad C \end{aligned}$$

mit $B := \sum_{k=0}^{n} \frac{1}{p^k}\, S_n\Big(\frac{\pi_n^{p^k}}{\zeta_n^{p^k}-1}\Big)$ und $C := \sum_{k\ge n+1} \frac{1}{p^k}\frac{p^{n+1}-1}{2}\, S_n\big(\pi_n^{p^k}\big)$.

Zur Berechnung von B sei zuerst bemerkt, dass für $k \le n$ die Beziehung $\zeta_n^{p^k} - 1 = \zeta_{n-k} - 1 \in K_{n-k}$ gilt. Unter Verwendung von Lemma 4.8 erhält man

$$\begin{aligned} \frac{1}{p^k}\, S_{n,n-k}\Big(\frac{\pi_n^{p^k}}{\zeta_n^{p^k}-1}\Big) &= \frac{1}{p^k}\frac{1}{\zeta_n^{p^k}-1}\, S_{n,n-k}\big(\pi_n^{p^k}\big) \\ &= \frac{1}{p^k}\frac{1}{\zeta_n^{p^k}-1}\, S_{n,n-k}\big((1-\zeta_n)^{p^k}\big) \\ &= \frac{1}{p^k}\frac{1}{\zeta_n^{p^k}-1}\sum_{r=0}^{p^k}\binom{p^k}{r}(-1)^r S_{n,n-k}(\zeta_n^r) \\ &= \frac{1}{p^k}\frac{1}{\zeta_n^{p^k}-1}\,\big(p^k + p^k(-1)^{p^k}\zeta_n^{p^k}\big) \\ &= \frac{1}{\zeta_n^{p^k}-1}\,\big(1-\zeta_n^{p^k}\big) \;=\; -1. \end{aligned}$$

Damit ist $\frac{1}{p^k}\, S_n\big(\frac{\pi_n^{p^k}}{\zeta_n^{p^k}-1}\big) = S_{n-k}(-1) = -(p-1)p^{n-k}$, so dass

$$\begin{aligned} B &= \sum_{k=0}^{n} \frac{1}{p^k}\, S_n\Big(\frac{\pi_n^{p^k}}{\zeta_n^{p^k}-1}\Big) = -(p-1)\sum_{k=0}^{n} p^{n-k} \\ &= -(p-1)\sum_{k=0}^{n} p^k = -(p-1)\frac{p^{n+1}-1}{p-1} = 1-p^{n+1}. \end{aligned}$$

Also

$$B \equiv 1 \mod p^{n+1}.$$

Zur Berechnung von C wird die Größe $S_n\big(\pi_n^{p^k}\big)$ untersucht. Mit Hilfe von Lemma 4.8 ergibt sich

$$\begin{aligned} S_n\big(\pi_n^{p^k}\big) &= \sum_{r=0}^{p^k} \binom{p^k}{r} (-1)^r S_n(\zeta_n^r) \\ &= \sum_{\substack{v_p(r)>n \\ r=0\ldots p^k}} \binom{p^k}{r} (-1)^r (p-1)p^n - \sum_{\substack{v_p(r)=n \\ r=0\ldots p^k}} \binom{p^k}{r} (-1)^r p^n \\ &= p^{n+1} \sum_{\substack{v_p(r)=n+1\ldots k \\ r=0\ldots p^k}} \binom{p^k}{r} (-1)^r - p^n \sum_{\substack{v_p(r)=n\ldots k \\ r=0\ldots p^k}} \binom{p^k}{r} (-1)^r. \end{aligned}$$

Wegen $k > n$ haben r und $p^k - r$ dieselbe p-Bewertung. Somit kommt mit dem Summand zu r auch der Summand zu $p^k - r$ in jeder der beiden Summen vor. Diese beiden Summanden heben sich aber wegen $(-1)^r = -(-1)^{p^k - r}$ weg, so dass sich jede der beiden Summen zu Null ergibt. Damit ist

$$C = 0$$

und $A \equiv 1 \mod p^{n+1}$. Fasst man die bisherigen Ergebnisse zusammen, so ergibt sich

$$\begin{aligned} (\pi_n, \tau_a)_n &= 1, \qquad \text{für} \quad (a,p) = 1 \\ (\pi_n, \tau_{p^{n+1}})_n &= \zeta_n. \end{aligned}$$

Nun sind die Gleichungen

$$\frac{1}{p^{n+1}} S_n\Big(-\frac{\zeta_n}{\pi_n} \log \tau_a \Big) \equiv \left\{ \begin{array}{ll} 0, & (a,p) = 1 \\ 1, & a = p^{n+1} \end{array} \right\} \mod p^{n+1} \tag{5.5}$$

zu zeigen. Dazu wird die Rechnung für beliebiges $a \geq 1$ durchgeführt. Mit $\log \tau_a = g(\pi_n^a)$ (vgl. Gleichung (5.2)) folgt

$$\begin{aligned} p^{-(n+1)} S_n\Big(-\frac{\zeta_n}{\pi_n} \log \tau_a \Big) &= p^{-(n+1)} S_n\Big(-\frac{\zeta_n}{\pi_n} g(\pi_n^a) \Big) \\ &= p^{-(n+1)} S_n\Big(\frac{\zeta_n}{\pi_n} \sum_{k=0}^{\infty} \frac{\pi_n^{ap^k}}{p^k} \Big) \\ &= p^{-(n+1)} \sum_{k=0}^{\infty} \frac{1}{p^k} S_n\big(\zeta_n \pi_n^{ap^k - 1}\big). \end{aligned}$$

Für die Spuren in den Summanden gilt unter Verwendung von Lemma 4.8

$$\begin{aligned}
S_n\big(\zeta_n\pi_n^{ap^k-1}\big) &= S_n\left(\sum_{r=0}^{ap^k-1}\binom{ap^k-1}{r}(-1)^r\zeta_n^{r+1}\right), \qquad r+1\to r\\
&= -\sum_{r=1}^{ap^k}\binom{ap^k-1}{r-1}(-1)^r S_n\big(\zeta_n^r\big)\\
&= -\sum_{r=0}^{ap^k}\binom{ap^k}{r}\frac{r}{ap^k}(-1)^r S_n\big(\zeta_n^r\big)\\
&= p^n\sum_{\substack{v_p(r)=n\\ r=0\ldots ap^k}}\binom{ap^k}{r}\frac{r}{ap^k}(-1)^r-(p-1)p^n\sum_{\substack{v_p(r)>n\\ r=0\ldots ap^k}}\binom{ap^k}{r}\frac{r}{ap^k}(-1)^r\\
&= p^n\sum_{\substack{v_p(r)\geq n\\ r=0\ldots ap^k}}\binom{ap^k}{r}\frac{r}{ap^k}(-1)^r-p^{n+1}\sum_{\substack{v_p(r)>n\\ r=0\ldots ap^k}}\binom{ap^k}{r}\frac{r}{ap^k}(-1)^r.
\end{aligned}$$

Damit kann man obige Rechnung fortsetzen

$$\begin{aligned}
&p^{-(n+1)}S_n\Big(-\frac{\zeta_n}{\pi_n}\log\tau_a\Big)=\\
&\quad= p^{-(n+1)}\sum_{k=0}^{\infty}\frac{1}{p^k}\,S_n\big(\zeta_n\pi_n^{ap^k-1}\big)\\
&\quad= p^{-(n+1)}\sum_{k=0}^{\infty}\left(\frac{p^n}{p^k}\sum_{\substack{v_p(r)\geq n\\ r=0\ldots ap^k}}\binom{ap^k}{r}\frac{r}{ap^k}(-1)^r-\frac{p^{n+1}}{p^k}\sum_{\substack{v_p(r)>n\\ r=0\ldots ap^k}}\binom{ap^k}{r}\frac{r}{ap^k}(-1)^r\right)\\
&\quad= \sum_{k=0}^{\infty}\frac{1}{p^k}\left(\frac{1}{p}\sum_{\substack{v_p(r)\geq n\\ r=0\ldots ap^k}}\binom{ap^k}{r}\frac{r}{ap^k}(-1)^r-\sum_{\substack{v_p(r)>n\\ r=0\ldots ap^k}}\binom{ap^k}{r}\frac{r}{ap^k}(-1)^r\right)\\
&\quad= \sum_{k=0}^{\infty}\sum_{\substack{v_p(r)\geq n\\ r=0\ldots ap^k}}\frac{1}{p^{k+1}}\binom{ap^k}{r}\frac{r}{ap^k}(-1)^r-\\
&\qquad\qquad-\sum_{\substack{v_p(r)>n\\ r=0\ldots a}}\binom{a}{r}\frac{r}{a}(-1)^r-\sum_{k=1}^{\infty}\sum_{\substack{v_p(r)>n\\ r=0\ldots ap^k}}\frac{1}{p^k}\binom{ap^k}{r}\frac{r}{ap^k}(-1)^r.
\end{aligned}$$

Dabei entspricht die zweite Summe dem $(k=0)$-Term der letzten Summe eine Zeile darüber. Nun wird in der ersten Summe eine Substitution $k+1\to k$ vorgenommen, und in der dritten Summe in jedem Summanden ein Faktor p aus r

ausgeklammert. Man erhält

$$\begin{aligned} p^{-(n+1)} S_n\Big(-\frac{\zeta_n}{\pi_n}\log\tau_a\Big) = \\ = \sum_{k=1}^{\infty} \sum_{\substack{v_p(r)\geq n \\ r=0\ldots ap^{k-1}}} \frac{1}{p^k}\binom{ap^{k-1}}{r}\frac{rp}{ap^k}(-1)^r - \\ - \sum_{\substack{v_p(r)>n \\ r=0\ldots a}} \binom{a}{r}\frac{r}{a}(-1)^r - \sum_{k=1}^{\infty} \sum_{\substack{v_p(r)\geq n \\ r=0\ldots ap^{k-1}}} \frac{1}{p^k}\binom{ap^k}{rp}\frac{rp}{ap^k}(-1)^{rp} \\ = -\sum_{\substack{v_p(r)>n \\ r=0\ldots a}} \binom{a}{r}\frac{r}{a}(-1)^r + \sum_{k=1}^{\infty} \sum_{\substack{v_p(r)\geq n \\ r=0\ldots ap^{k-1}}} \frac{1}{p^k}\frac{rp}{ap^k}(-1)^r\left(\binom{ap^{k-1}}{r} - \binom{ap^k}{rp}\right). \end{aligned}$$

Der letzte Schritt gilt wegen $(-1)^r = (-1)^{rp}$. Gilt $v_p(a) = k_0$, so ist die Differenz der Binomialkoeffizienten nach Lemma 5.5 durch p^{2k+2k_0} teilbar. Somit ist jeder Summand in der letzten Summe durch $p^{2k+2k_0+n+1-(2k+k_0)} = p^{k_0+n+1}$, also auch durch p^{n+1} teilbar. Als Endergebnis erhält man

$$\begin{aligned} \frac{1}{p^{n+1}}\, S_n\Big(-\frac{\zeta_n}{\pi_n}\log\tau_a\Big) &\equiv -\sum_{\substack{v_p(r)>n \\ r=0\ldots a}} \binom{a}{r}\frac{r}{a}(-1)^r \mod p^{n+1} \\ &\equiv \begin{cases} 0, & \text{falls} \quad 1 \leq a < p^{n+1} \\ 1, & \text{falls} \quad a = p^{n+1} \end{cases} \mod p^{n+1}. \end{aligned}$$

Mit Blick auf Gleichung (5.5) ist damit der zweite Ergänzungssatz bewiesen.

QED

5.2 Das explizite Reziprozitätsgesetz

Der in diesem Abschnitt dargebotene Beweis des expliziten Reziprozitätsgesetzes orientiert sich an dem Artikel [Iwa2] von K. Iwasawa. Bevor das Theorem formuliert werden kann, besteht die Notwendigkeit des Beweises einiger Lemmata und Sätze.

Satz 5.6 *Es gilt* $S_n\big(\mathfrak{D}_n \log(1+\mathfrak{m}_n)\big) \equiv 0 \mod p^{n+1}$.

Beweis: Es werde die Abbildung

$$\varphi : (1+\mathfrak{m}_n) \to \mathcal{O}_n/\mathfrak{m}_n, \quad 1 + x\pi_n \mapsto x \mod \pi_n$$

betrachtet. Dies ist ein Gruppenhomomorphismus von der multiplikativen Gruppe $(1+\mathfrak{m}_n)$ in die additive Gruppe $\mathcal{O}_n/\mathfrak{m}_n \cong \mathbb{F}_p$ mit dem Kern $(1+\mathfrak{m}_n^2) =$

$\{a \in \mathcal{O}_n : a \equiv 1 \mod \pi_n^2\}$. φ induziert somit einen ebenfalls mit φ bezeichneten Isomorphismus

$$\varphi : (1+\mathfrak{m}_n)/(1+\mathfrak{m}_n^2) \cong \mathcal{O}_n/\mathfrak{m}_n \cong \mathbb{F}_p.$$

Es gilt $\varphi(\zeta_n) = \varphi(1-\pi_n) = -1$. Da -1 ein Erzeuger der additiven Gruppe $\mathbb{F}_p$ ist, ist ζ_n ein Erzeuger der linken Seite. Man kann also

$$(1+\mathfrak{m}_n) = \langle\zeta_n\rangle \times (1+\mathfrak{m}_n^2)$$

schreiben, wobei $\langle\zeta_n\rangle = \mu_{p^{n+1}} = \{\zeta_n^k,\ k \in \mathbb{Z}\}$ die Untergruppe der p^{n+1}-ten Einheitswurzeln bezeichnet. Wegen $\log\zeta_n = 0$ (vgl. Bemerkung zum Satz 2.2) folgt $\log(1+\mathfrak{m}_n) = \log(1+\mathfrak{m}_n^2)$.

Somit genügt es, $S_n(\mathfrak{D}_n \log\alpha) \equiv 0 \mod p^{n+1}$, bzw.

$$\nu_n\big(S_n(\mathfrak{D}_n \log\alpha)\big) \geq (n+1)(p-1)p^n \tag{5.6}$$

für alle $\alpha \in (1+\mathfrak{m}_n^2)$ zu zeigen. Dieser Beweis wird in zwei Schritten erbracht. Im ersten Schritt wird gezeigt, dass die Ungleichung $\nu_n(p^{n+1}\log\alpha) \geq p^{n+1}+p^n$ für $\alpha \in (1+\mathfrak{m}_n^2)$ gilt, und im zweiten Schritt wird bewiesen, dass daraus die behauptete Ungleichung (5.6) folgt.

Zum ersten Schritt: Sei $\alpha = 1-\beta \in (1+\mathfrak{m}_n^2),\ \beta \in \mathfrak{m}_n^2$. Dann läßt sich $\log\alpha$ als

$$\log\alpha = -\sum_{k=1}^{\infty}\frac{\beta^k}{k}$$

schreiben. Es ist zu zeigen, dass $\nu_n\big(p^{n+1}\frac{\beta^k}{k}\big) \geq p^{n+1}+p^n$ für alle $k \geq 1$. Sei p^e die p-Potenz, die k exakt teilt. Dann gilt $k \geq p^e$ und

$$\begin{aligned}\nu_n\Big(p^{n+1}\tfrac{\beta^k}{k}\Big) &= (n+1-e)(p-1)p^n + 2k \\ &\geq (n+1-e)(p-1)p^n + 2p^e \\ &= (n+1-e)p^{n+1} - (n+1-e)p^n + 2p^e \\ &\geq p^{n+1}+p^n.\end{aligned}$$

Die letzte Ungleichung ist äquivalent zu der Ungleichung

$$(n-e)p^{n+1} - (n+2-e)p^n + 2p^e \geq 0.$$

Sei $f(X) := (n-e)X^{n+1} - (n-e+2)X^n + 2X^e$. Es ist die Gültigkeit von

$$f(X) \geq 0 \quad \text{für} \quad X \geq 3$$

zu zeigen. Im Fall $e = n$ ist $f(X) = 0$ und diese Ungleichung ist erfüllt.

Im Fall $e < n$ kann man $f(X)$ als

$$f(X) = X^e\big((n-e)X^{n-e+1} - (n-e+2)X^{n-e} + 2\big) = X^e g(X)$$

mit einer Funktion $g(X) := aX^{a+1} - (a+2)X^a + 2$ und $a := n - e \geq 1$ schreiben. Es gilt $g(3) = 2 \cdot 3^a(a-1) + 2 \geq 0$ und $g'(X) = aX^{a-1}\big((a+1)X - (a+2)\big) \geq 0$ für $X \geq 3$. Somit folgt $g(X) \geq 0$ und auch $f(X) \geq 0$ für $X \geq 3$.

Falls schließlich $e > n$, so läßt sich

$$f(X) = X^n\big((n-e)X - (n-e+2) + 2X^{e-n}\big) = X^n h(X)$$

mit einer Funktion $h(X) := 2X^b - bX - (2-b)$ und $b := e - n \geq 1$ schreiben. Es gilt $h'(X) = b(2X^{b-1} - 1) \geq 0$ für $X \geq 3$. Mit Induktion nach b läßt sich zeigen, dass $h(3) = 2(3^b - b - 1) \geq 0$ gilt. Für $b = 1$ ist $h(3) = 2(3^1 - 1 - 1) = 2 > 0$. Für alle $b \geq 0$ gilt $2 \cdot 3^b \geq 1$, so dass $3^{b+1} \geq 3^b + 1$. Damit folgt für $b > 1$

$$h(3) = 3^{b+1} - (b+1) - 1 = 3^{b+1} - b - 2 \geq 3^b - b - 1 \geq 0.$$

Die letzte Ungleichung gilt aufgrund der Induktionsvoraussetzung. Somit folgt $h(X) \geq 0$ und auch in diesem Fall ist $f(X) \geq 0$ für $X \geq 3$.

Im zweiten Schritt ist nun zu zeigen, dass aus der soeben ermittelten Abschätzung die Ungleichung $\nu_n\big(S_n(\mathfrak{D}_n \log \alpha)\big) \geq (n+1)(p-1)p^n$ für alle $\alpha \in (1 + \mathfrak{m}_n^2)$ folgt. Sei $x \in \mathfrak{D}_n$, d.h. $x = p^{n+1}y$ mit $y \in \mathfrak{m}_n^{-p^n}$. Mit Hilfe von Satz 4.12 folgt

$$\begin{aligned}
\nu_n\big(S_n(x \log \alpha)\big) &> \nu_n(x \log \alpha) + \big(n(p-1) - 1\big)p^n \\
&= \nu_n(p^{n+1} \log \alpha) + \nu_n(y) + \big(n(p-1) - 1\big)p^n \\
&\geq p^{n+1} + p^n - p^n + \big(n(p-1) - 1\big)p^n \\
&= (n+1)(p-1)p^n
\end{aligned}$$

für alle $x \in \mathfrak{D}_n$. Damit ist der Satz bewiesen.

QED

Satz 5.7 *Sei $m \geq n \geq 0$. Dann gilt*

(i) $p^{-(m+1)} S_m\big(\mathfrak{D}_m \log(1 + \mathfrak{m}_n)\big) \equiv 0 \mod p^{n+1}$ *für* $m \geq 2n+1$,

(ii) $p^{-(m+1)} S_m\big(\mathfrak{D}_m \log(1 + \mathfrak{m}_n^{p^n})\big) \equiv 0 \mod p^{n+1}$ *für* $m \geq n+1$,

(iii) $p^{-(m+1)} S_m\big(\mathfrak{D}_m \log(1 + \mathfrak{m}_n^{2p^n})\big) \equiv 0 \mod p^{n+1}$ *für* $m \geq n$.

Beweis von (i): Unter Verwendung der dem Lemma 4.6 nachfolgenden Bemerkung und der Gleichung (4.1) gilt

$$S_{mn}(\mathfrak{D}_m) = S_{mn}(p^{m+1}\pi_0^{-1}\mathcal{O}_m) = p^{m+1}\pi_0^{-1} S_{mn}(\mathcal{O}_m) = p^{m+1}p^{m-n}\pi_0^{-1}\mathcal{O}_n,$$

welches für $m \geq 2n+1$ wegen $p^{n+1} \,|\, p^{m-n}$ in $p^{m+1}p^{n+1}\pi_0^{-1}\mathcal{O}_n = p^{m+1}\mathfrak{D}_n$ enthalten ist. Damit ergibt sich

$$\begin{aligned} p^{-(m+1)} S_m\big(\mathfrak{D}_m \log(1+\mathfrak{m}_n)\big) &= p^{-(m+1)} S_n\big(S_{mn}(\mathfrak{D}_m)\log(1+\mathfrak{m}_n)\big) \\ &\subseteq S_n\big(\mathfrak{D}_n \log(1+\mathfrak{m}_n)\big) \end{aligned}$$

und die Aussage folgt aus Satz 5.6.

Beweis von (ii): Zum Beweis der zweiten Aussage werde der Isomorphismus

$$\varphi : (1+\mathfrak{m}_n^{p^n})/(1+\mathfrak{m}_n^{p^n+1}) \to \mathcal{O}_n/\mathfrak{m}_n \cong \mathbb{F}_p, \quad 1 + x\pi_n^{p^n} \mapsto x \mod \pi_n$$

betrachtet (vgl. Beweis zu Satz 5.6). Für $\zeta_n^{p^n} = \zeta_0 = 1 - \pi_0 = 1 - u\pi_n^{p^n}$ mit einer Einheit $u \in \mathcal{O}_n^*$ gilt $\varphi(\zeta_n^{p^n}) = -u$. Wegen $u \notin \mathfrak{m}_n$ ist u ein Erzeuger von $\mathcal{O}_n/\mathfrak{m}_n$. Somit ist $\zeta_n^{p^n}$ ein Erzeuger der linken Seite, d.h. man kann $(1+\mathfrak{m}_n^{p^n}) \cong \langle \zeta_n^{p^n} \rangle \times (1+\mathfrak{m}_n^{p^n+1})$ schreiben. Die Gleichheit $\log(\zeta_n^{p^n}) = 0$ impliziert

$$\log\left(1+\mathfrak{m}_n^{p^n}\right) = \log\left(1+\mathfrak{m}_n^{p^n+1}\right) = \mathfrak{m}_n^{p^n+1}.$$

Die letzte Gleichheit ergibt sich aus Lemma 4.1. Mit Hilfe von $\mathfrak{m}_m^{-p^m} = \pi_0^{-1}\mathcal{O}_m = \pi_n^{-p^n}\mathcal{O}_m$ folgt $\mathfrak{D}_m = p^{m+1}\mathfrak{m}_m^{-p^m} = p^{m+1}\pi_n^{-p^n}\mathcal{O}_m$ und

$$\begin{aligned} p^{-(m+1)} S_m\big(\mathfrak{D}_m \log(1+\mathfrak{m}_n^{p^n})\big) &= p^{-(m+1)} S_m(p^{m+1}\pi_n^{-p^n}\mathcal{O}_m\mathfrak{m}_n^{p^n+1}) \\ &= S_m(\pi_n\mathcal{O}_m) = S_n\big(\pi_n S_{mn}(\mathcal{O}_m)\big) \\ &= p^{m-n} S_n(\mathfrak{m}_n) = p^{m-n}p^n\mathbb{Z}_p \\ &= p^m\mathbb{Z}_p \equiv 0 \mod p^{n+1} \end{aligned}$$

für $m \geq n+1$. Bei dieser Rechnung wurde $S_n(\mathfrak{m}_n) = p^n\mathbb{Z}_p$ (vgl. Satz 4.11) verwendet.

Beweis von (iii): Nach Lemma 4.1 gilt $\log\left(1+\mathfrak{m}_n^{2p^n}\right) = \mathfrak{m}_n^{2p^n} = \pi_0^2\mathcal{O}_n$. Analog zu obigen Überlegungen folgt daraus

$$\begin{aligned} p^{-(m+1)} S_m\big(\mathfrak{D}_m \log(1+\mathfrak{m}_n^{2p^n})\big) &= p^{-(m+1)} S_m(p^{m+1}\pi_0^{-1}\mathcal{O}_m\pi_0^2\mathcal{O}_n) = S_m(\pi_0\mathcal{O}_m) \\ &= S_0(\pi_0 S_{m0}(\mathcal{O}_m)) = p^m S_0(\mathfrak{m}_0) \\ &= p^m p\,\mathbb{Z}_p \equiv 0 \mod p^{m+1}. \end{aligned}$$

Damit gilt Aussage (iii) für $m \geq n$.

QED

Sei $\mathbb{Z}_p[[T]]$ der Ring der formalen Potenzreihen über $\mathbb{Z}_p$. Wegen $\mathcal{O}_n = \mathbb{Z}_p[\pi_n]$ existiert für jedes $x \in \mathcal{O}_n$ eine Potenzreihe

$$f(T) = \sum_{j=s}^{\infty} a_j T^j, \quad a_j \in \mathbb{Z}_p, \quad s = \nu_n(x) \geq 0$$

mit $f(\pi_n) = x$. Eine solche Potenzreihe wird Potenzreihe für x genannt. Diese ist durch x nicht eindeutig bestimmt. So kann man eine gegebene Potenzreihe mit einer Potenzreihe $g(T)$ mit $g(\pi_n) = 1$ multiplizieren. Beispielsweise hat $g(T) = (1-T)\sum_{j\geq 0} T^j$ diese Eigenschaft.

Definition 5.8 *Seien $x \in \mathcal{O}_n$, $x \neq 0$, und $f(T)$ eine Potenzreihe für x. So definiert man*

$$\delta_n(x) = \delta_n(f)(x) := \frac{\zeta_n}{x} f'(\pi_n) \in K_n.$$

Da $f(T)$ nicht eindeutig durch x bestimmt ist, sind auch $f'(\pi_n)$ und $\delta_n(x)$ nicht eindeutig durch x bestimmt. Betrachtet man jedoch $\delta_n(x)$ als Funktion auf $\mathcal{O}_n$, dann gilt folgender Satz.

Satz 5.9 *Sei $x \in \mathcal{O}_n$ fest. Dann liegen alle möglichen Werte $\delta_n(x)$ in derselben Restklasse von $\mathfrak{m}_n^{-1} \mod \mathfrak{D}_n$, d.h. sie repräsentieren dort alle dasselbe Element. Man kann also δ_n als Funktion $\mathcal{O}_n \to \mathfrak{m}_n^{-1}/\mathfrak{D}_n$ auffassen.*

Beweis: Zuerst wird gezeigt, dass $\delta_n(x)$ für $x \in \mathcal{O}_n$ immer in $\mathfrak{m}_n^{-1}$ liegt. Ist $f(T)$ eine Potenzreihe für x und ist $\nu_n(x) = s \geq 1$, so ist $\nu_n\big(f'(\pi_n)\big) = s-1$ und man erhält

$$\begin{aligned}\nu_n\big(\delta_n(x)\big) &= \nu_n\left(\tfrac{\zeta_n}{x} f'(\pi_n)\right) \\ &= \nu_n(\zeta_n) - \nu_n(x) + \nu_n\big(f'(\pi_n)\big) = 0 - s + (s-1) = -1.\end{aligned}$$

Ist dagegen $\nu_n(x) = s = 0$, ist x also eine Einheit, so ist $\nu_n\big(f'(\pi_n)\big) \geq 0$ und es gilt

$$\nu_n\big(\delta_n(x)\big) = \nu_n\big(f'(\pi_n)\big) - \nu_n(x) \geq 0 > -1.$$

Damit ist $\delta_n(x) \in \mathfrak{m}_n^{-1}$ gezeigt.

Seien nun $f(T)$ und $g(T)$ zwei Potenzreihen für x. Dann ist π_n eine Nullstelle der Differenz $f(T) - g(T)$, d.h. diese ist durch das Minimalpolynom $d(T)$ von π_n teilbar. Man kann also

$$f(T) = g(T) + u(T)d(T), \quad d(T) = \sum_{k=0}^{p-1} (1-T)^{kp^n}, \quad u(T) \in \mathbb{Z}_p[[T]]$$

schreiben. Durch Differentiation erhält man $f'(\pi_n) = g'(\pi_n) + u(\pi_n)d'(\pi_n)$. Da $\mathfrak{D}_n$ das von $d'(\pi_n)$ erzeugte Ideal ist (vgl. Definition 4.3), folgt

$$f'(\pi_n) \equiv g'(\pi_n) \mod u(\pi_n)\mathfrak{D}_n$$

bzw. $\frac{\zeta_n}{x} f'(\pi_n) \equiv \frac{\zeta_n}{x} g'(\pi_n) \mod \frac{\zeta_n}{x} u(\pi_n)\mathfrak{D}_n$. Es bleibt $\frac{\zeta_n}{x} u(\pi_n)\mathfrak{D}_n \subseteq \mathfrak{D}_n$ zu zeigen.

In f und g verschwinden alle Koeffizienten a_i für $0 \leq i < s = \nu_n(x)$. Da dies in $d(T)$ nicht der Fall ist, es gilt nämlich $d(0) = p$, muss es in $u(T)$ so sein. Damit folgt $\nu_n\big(u(\pi_n)\big) \geq s$ bzw. $\nu_n\big(\frac{\zeta_n}{x}u(\pi_n)\big) \geq s - s = 0$, was bedeutet, dass $\frac{\zeta_n}{x}u(\pi_n) \in \mathcal{O}_n$. Daraus folgt schließlich $\frac{\zeta_n}{x}u(\pi_n)\mathfrak{D}_n \subseteq \mathfrak{D}_n$ und somit $\delta_n(f)(x) \equiv \delta_n(g)(x) \mod \mathfrak{D}_n$.

QED

An dieser Stelle seien für $x = \zeta_n$ und für $x = \pi_n$ spezielle Werte der Funktion δ_n berechnet. Das Polynom $f(T) = 1-T$ ist eine Potenzreihe für ζ_n mit $f'(T) = -1$. Somit gilt

$$\delta_n(\zeta_n) \equiv \frac{\zeta_n}{\zeta_n} f'(\pi_n) \equiv -1 \mod \mathfrak{D}_n. \tag{5.7}$$

Es ist $g(T) = T$ eine Potenzreihe für π_n. Wegen $g'(T) = 1$ folgt

$$\delta_n(\pi_n) \equiv \frac{\zeta_n}{\pi_n} g'(\pi_n) \equiv \frac{\zeta_n}{\pi_n} \mod \mathfrak{D}_n. \tag{5.8}$$

Lemma 5.10 *Seien $K := \bigcup_{n=0}^{\infty} K_n$ und $\sigma \in G(K/\mathbb{Q}_p)$. Dann gibt es eine eindeutig bestimmte p-adische Einheit $\kappa(\sigma)$, so dass*

$$\sigma(\zeta_n) = \zeta_n^{\kappa(\sigma)} \quad \textit{für alle} \quad n \geq 0.$$

Beweis: Sei $\sigma \in G(K/\mathbb{Q}_p)$ fest gewählt und sei $\kappa = \kappa(\sigma)$. Für $n \geq 0$ sei $\kappa_n \in \mathbb{Z}/p^{n+1}\mathbb{Z}$ mit $\sigma(\zeta_n) = \zeta_n^{\kappa_n}$. Der Exponent κ_n ist eindeutig bestimmt, da σ durch seine Wirkung auf ζ_n eindeutig bestimmt ist. Für $n = 0$ gilt wegen $\sigma(\zeta_0) \neq 1$ sogar $\kappa_0 \in (\mathbb{Z}/p\mathbb{Z})^*$. Abschließend bleibt zu zeigen, dass $\kappa = (\ldots, \kappa_n, \ldots, \kappa_2, \kappa_1, \kappa_0)$ ein Element des projektiven Limes $\mathbb{Z}_p$ ist, d.h. dass für $m \geq n$ die Beziehung $\kappa_m \equiv \kappa_n \mod p^{n+1}$ gilt. Sei $m \geq n$. Dann ist

$$\zeta_n^{\kappa_n} = \sigma(\zeta_n) = \sigma(\zeta_m^{p^{m-n}}) = \sigma(\zeta_m)^{p^{m-n}} = \zeta_m^{\kappa_m p^{m-n}} = \zeta_n^{\kappa_m},$$

und somit folgt $\kappa_m \equiv \kappa_n \mod p^{n+1}$. Wegen $\kappa_0 \in (\mathbb{Z}/p\,\mathbb{Z})^*$ ist κ eine p-adische Einheit. Da alle κ_n eindeutig bestimmt sind, ist auch κ eindeutig bestimmt.

QED

Satz 5.11

(i) *Für $x, y \in \mathcal{O}_n$, $x, y \neq 0$, gilt*

$$\delta_n(xy) \equiv \delta_n(x) + \delta_n(y) \mod \mathfrak{D}_n.$$

(ii) *Für $x \in \mathcal{O}_n$ und $\sigma \in G(K/\mathbb{Q}_p)$, gilt*

$$\delta_n\big(\sigma(x)\big) \equiv \kappa(\sigma)\sigma\big(\delta_n(x)\big) \mod \mathfrak{D}_n,$$

wobei $\kappa(\sigma)$ die eindeutig bestimmte p-adische Einheit aus Lemma 5.10 ist.

(iii) *Für $m \geq n$ und eine Einheit x aus $\mathcal{O}_n$ gilt*

$$\delta_m(x) \equiv p^{m-n}\delta_n(x) \mod \mathfrak{D}_m.$$

Beweis von (i): Seien $f(T)$ und $g(T)$ Potenzreihen für x bzw. y, d.h. es gilt $f(\pi_n) = x$ und $g(\pi_n) = y$. Dann ist $f(T)g(T)$ eine Potenzreihe für xy und man kann schlussfolgern

$$\begin{aligned}\delta_n(xy) &\equiv \frac{\zeta_n}{xy}\big(f(\pi_n)g(\pi_n)\big)' \equiv \frac{\zeta_n}{xy}\big(f'(\pi_n)g(\pi_n) + f(\pi_n)g'(\pi_n)\big)\\ &\equiv \frac{\zeta_n}{x}f'(\pi_n) + \frac{\zeta_n}{y}g'(\pi_n) \equiv \delta_n(x) + \delta_n(y) \mod \mathfrak{D}_n.\end{aligned}$$

Beweis von (ii): Seien $x \in \mathcal{O}_n$ und $\sigma \in G(K/\mathbb{Q}_p)$ fest vorgegeben, sei $\kappa = \kappa(\sigma)$ und sei $u(T) = 1-(1-T)^\kappa = \kappa T + \dots$. Dann gilt $u(\pi_n) = 1-(1-\pi_n)^\kappa = 1-\sigma(\zeta_n) = \sigma(1-\zeta_n) = \sigma(\pi_n)$, d.h. $u(T)$ ist eine Potenzreihe für $\sigma(\pi_n)$. Außerdem ist $u'(T) = \kappa(1-T)^{\kappa-1}$ und $u'(\pi_n) = \kappa\frac{\sigma(\zeta_n)}{\zeta_n}$.
Sei $f(T)$ eine Potenzreihe für x. Dann gilt $f\big(u(\pi_n)\big) = f\big(\sigma(\pi_n)\big) = \sigma\big(f(\pi_n)\big) = \sigma(x)$, d.h. $f\big(u(T)\big)$ ist eine Potenzreihe für $\sigma(x)$. Somit ergibt sich

$$\begin{aligned}\delta_n\big(\sigma(x)\big) &\equiv \frac{\zeta_n}{\sigma(x)}f'\big(u(\pi_n)\big)u'(\pi_n) \equiv \frac{\zeta_n}{\sigma(x)}\sigma\big(f'(\pi_n)\big)\kappa\frac{\sigma(\zeta_n)}{\zeta_n}\\ &\equiv \kappa\,\sigma\left(\frac{\zeta_n}{x}f'(\pi_n)\right) \equiv \kappa\,\sigma\big(\delta_n(x)\big) \mod \mathfrak{D}_n.\end{aligned}$$

Beweis von (iii): Sei x eine Einheit aus $\mathcal{O}_n$. Dann ist x auch eine Einheit in $\mathcal{O}_m$ und jede Potenzreihe $g(T)$ mit $g(\pi_m) = x$ ist eine Potenzreihe für $x \in \mathcal{O}_m$. Sei $f(T)$ eine Potenzreihe für x in $\mathcal{O}_n$, d.h. $f(\pi_n) = x$. Wegen $\pi_n = 1-\zeta_n = 1-\zeta_m^{p^{m-n}} = 1-(1-\pi_m)^{p^{m-n}}$ ist $g(T) = f\big(1-(1-T)^{p^{m-n}}\big)$ eine Potenzreihe für $x \in \mathcal{O}_m$. Es folgt modulo $\mathfrak{D}_m$

$$\begin{aligned}\delta_m(x) &\equiv \frac{\zeta_m}{x}f'\big(1-(1-\pi_m)^{p^{m-n}}\big)p^{m-n}(1-\pi_m)^{p^{m-n}-1}\\ &\equiv p^{m-n}\frac{\zeta_m}{x}f'(\pi_n)\zeta_m^{p^{m-n}-1}\\ &\equiv p^{m-n}\frac{\zeta_n}{x}f'(\pi_n) \equiv p^{m-n}\delta_n(x).\end{aligned}$$

Da $\delta_n(x)$ eindeutig bestimmt ist modulo $\mathfrak{D}_n$ und $p^{m-n}\mathfrak{D}_n = p^{m-n}p^{n+1}\pi_0^{-1}\mathcal{O}_n \subseteq p^{m-n}p^{n+1}\pi_0^{-1}\mathcal{O}_m = \mathfrak{D}_m$ gilt, sind beide Seiten der Kongruenz wohlbestimmt modulo $\mathfrak{D}_m$.

QED

Man kann δ_n zu einer Funktion auf ganz K_n^* ausdehnen, indem man für $x = \frac{x_1}{x_2} \neq 0$, $x_1, x_2 \in \mathcal{O}_n$, den Wert $\delta_n(x)$ als

$$\delta_n(x) := \delta_n(x_1) - \delta_n(x_2)$$

definiert. Aus der Definition erkennt man, dass die Werte von δ_n weiterhin in einer Restklasse von $\mathfrak{m}_n^{-1} \mod \mathfrak{D}_n$ liegen, und dass die Aussagen (i) und (ii) des Satzes 5.11 gelten. Man hat also einen Homomorphismus

$$\delta_n : K_n^* \to \mathfrak{m}_n^{-1}/\mathfrak{D}_n.$$

Satz 5.12 *Seien $m \geq n$ und $x \in K_m^*$. Dann gilt*

$$\delta_n\big(N_{mn}(x)\big) \equiv p^{-(m-n)} S_{mn}\big(\delta_m(x)\big) \mod \mathfrak{D}_n.$$

Beweis: Die linke Seite ist wohlbestimmt modulo $\mathfrak{D}_n$, die rechte Seite ist wohlbestimmt modulo $p^{-(m-n)} S_{mn}(\mathfrak{D}_m) = p^{-(m-n)} S_{mn}(p^{m+1}\pi_0^{-1}\mathcal{O}_m) = p^{n+1}\pi_0^{-1} p^{m-n}\mathcal{O}_n$ $= p^{m-n}\mathfrak{D}_n \subseteq \mathfrak{D}_n$. Somit sind beide Seiten wohlbestimmt modulo $\mathfrak{D}_n$.

Sei $x = u\pi_m^s \in K_m^*$ mit $u \in \mathcal{O}_m^*$. Dann gilt wegen Lemma 5.11, Punkt (i), für die linke Seite der Kongruenz

$$\delta_n\big(N_{mn}(x)\big) = \delta_n\big(N_{mn}(u) N_{mn}(\pi_m)^s\big) \equiv \delta_n\big(N_{mn}(u)\big) + s\,\delta_n\big(N_{mn}(\pi_m)\big)$$

und für die rechte Seite gilt

$$\begin{aligned} p^{-(m-n)} S_{mn}\big(\delta_m(x)\big) &\equiv p^{-(m-n)} S_{mn}\big(\delta_m(u) + s\delta_m(\pi_m)\big) \\ &\equiv p^{-(m-n)} \Big(S_{mn}\big(\delta_m(u)\big) + s\, S_{mn}\big(\delta_m(\pi_m)\big)\Big) \\ &\equiv p^{-(m-n)} \Big(S_{mn}\big(\delta_m(u)\big) + s\, S_{mn}\big(\delta_m(\pi_m)\big)\Big) \end{aligned}$$

modulo $\mathfrak{D}_n$. Somit genügt es, die Aussage für $x = \pi_m$ und eine Einheit $u \in \mathcal{O}_m^*$ zu beweisen.

Sei $x = \pi_m$. Mit Lemma 4.7 hat man $N_{mn}(\pi_m) = \pi_n$ und nach Gleichung (5.8) auf Seite 53 gilt $\delta_n(\pi_n) = \frac{\zeta_n}{\pi_n}$ und $\delta_m(\pi_m) = \frac{\zeta_m}{\pi_m}$. Somit verbleibt die Berechnung von $S_{mn}\big(\frac{\zeta_m}{\pi_m}\big)$. Wegen

$$\begin{aligned} \left(\frac{\zeta_n}{\pi_n} + \frac{1}{\pi_n} \sum_{k=1}^{p^{m-n}-1} \zeta_m^k\right) \pi_m &= \zeta_n \frac{\pi_m}{\pi_n} + \frac{1}{\pi_n} \sum_{k=1}^{p^{m-n}-1} (1-\zeta_m)\zeta_m^k \\ &= \zeta_n \frac{\pi_m}{\pi_n} + \frac{1}{\pi_n} \Big(\sum_{k=1}^{p^{m-n}-1} \zeta_m^k - \sum_{k=1}^{p^{m-n}-1} \zeta_m^{k+1} \Big) \end{aligned}$$

$$\begin{aligned}
&= \zeta_n \frac{\pi_m}{\pi_n} + \frac{1}{\pi_n}\Bigg(\zeta_m + \sum_{k=2}^{p^{m-n}-1} \zeta_m^k - \sum_{k=2}^{p^{m-n}-1} \zeta_m^k - \zeta_n\Bigg) \\
&= \zeta_n \frac{\pi_m}{\pi_n} + \frac{1}{\pi_n}(\zeta_m - \zeta_n) \;=\; \frac{\zeta_n}{\pi_n}(\pi_m - 1) + \frac{\zeta_m}{\pi_n} \\
&= -\zeta_n \frac{\zeta_m}{\pi_n} + \frac{\zeta_m}{\pi_n} \;=\; \zeta_m
\end{aligned}$$

ergibt sich für $\frac{\zeta_m}{\pi_m}$ die Darstellung

$$\frac{\zeta_m}{\pi_m} = \frac{\zeta_n}{\pi_n} + \frac{1}{\pi_n} \sum_{k=1}^{p^{m-n}-1} \zeta_m^k.$$

Für die Spur gilt somit

$$S_{mn}\left(\frac{\zeta_m}{\pi_m}\right) = S_{mn}\left(\frac{\zeta_n}{\pi_n}\right) + \frac{1}{\pi_n} \sum_{k=1}^{p^{m-n}-1} S_{mn}\big(\zeta_m^k\big).$$

Nach Lemma 4.8 sind die Summanden der Summe alle gleich Null, so dass

$$S_{mn}\left(\frac{\zeta_m}{\pi_m}\right) = S_{mn}\left(\frac{\zeta_n}{\pi_n}\right) = p^{m-n}\frac{\zeta_n}{\pi_n}.$$

Damit gilt

$$\delta_n\big(N_{mn}(\pi_m)\big) = \delta_n(\pi_n) = \frac{\zeta_n}{\pi_n} = p^{-(m-n)} S_{mn}\left(\frac{\zeta_m}{\pi_m}\right) = p^{-(m-n)} S_{mn}\big(\delta_m(\pi_m)\big)$$

und der Satz ist für $x = \pi_m$ bewiesen.

Seien nun $x = u$ eine Einheit aus $\mathcal{O}_m$ und $\sigma \in G(K_m/K_n)$. Mit Hilfe von Satz 5.11 folgt

$$p^{m-n}\delta_n\big(N_{mn}(u)\big) \equiv \delta_m\big(N_{mn}(u)\big) \equiv \sum_\sigma \delta_m\big(\sigma(u)\big) \equiv \sum_\sigma \kappa(\sigma)\sigma\big(\delta_m(u)\big) \mod \mathfrak{D}_m.$$

Die Anwendung von $p^{-(m-n)}S_{mn}$ auf beide Seiten des obigen Ausdrucks lässt die linke Seite unverändert, so dass man mit $p^{-(m-n)}S_{mn}(\mathfrak{D}_m) = p^{m-n}\mathfrak{D}_n$ (vgl. Beginn des Beweises von Satz 5.12) die Gleichheit

$$\begin{aligned}
p^{m-n}\delta_n\big(N_{mn}(u)\big) &\equiv p^{-(m-n)} \sum_\sigma \kappa(\sigma) S_{mn}\Big(\sigma\big(\delta_m(u)\big)\Big) \\
&\equiv p^{-(m-n)} S_{mn}\big(\delta_m(u)\big) \sum_\sigma \kappa(\sigma) \mod p^{m-n}\mathfrak{D}_n
\end{aligned}$$

erhält. Für $y \in K_m$ und $\sigma \in G(K_m/K_n)$ wurde dabei $S_{mn}\big(\sigma(y)\big) = S_{mn}(y)$ verwendet. Nun erfolgt die Berechnung von $\sum_\sigma \kappa(\sigma)$. Aus dem Beweis zu Lemma 5.10 erkennt man, dass die zu σ gehörige p-adische Einheit $\kappa(\sigma)$ durch

$$\kappa(\sigma) \equiv \kappa_r \mod p^{r+1} \quad \text{und} \quad \sigma(\zeta_r) = \zeta_r^{\kappa_r}$$

charakterisiert ist. Wegen $\sigma \in G(K_m/K_n)$ gilt $\sigma(\zeta_r) = \zeta_r$ für $r \leq n$, denn in diesem Fall ist $\zeta_r \in K_n$. Somit hat $\kappa(\sigma)$ die Gestalt

$$\begin{aligned}\kappa(\sigma) &= 1 + a_1 p^{n+1} + a_2 p^{n+2} + \ldots + a_{m-n} p^m + \ldots \\ &\equiv 1 + p^{n+1}(a_1 + a_2 p + \ldots + a_{m-n} p^{m-n-1}) \mod p^{m+1}.\end{aligned}$$

Jedes $\kappa(\sigma)$ für $\sigma \in G(K_m/K_n)$ hat also die Gestalt $\kappa(\sigma) \equiv 1 + jp^{n+1}$ mit $j \in \{0, \ldots, p^{m-n} - 1\}$, so dass man

$$\begin{aligned}\sum_\sigma \kappa(\sigma) \equiv \sum_{j=0}^{p^{m-n}-1} (1 + jp^{n+1}) &\equiv p^{m-n} + p^{n+1} \sum_{j=0}^{p^{m-n}-1} j \\ &\equiv p^{m-n} + p^{n+1} \frac{1}{2} (p^{m-n} - 1) p^{m-n} \\ &\equiv p^{m-n} + p^{m+1} \frac{1}{2} (p^{m-n} - 1) \equiv p^{m-n} \mod p^{m+1}\mathbb{Z}_p\end{aligned}$$

erhält. Im Beweis von Satz 5.9 hat sich ergeben, dass für eine Einheit u die Beziehung $\delta_m(u) \in \mathcal{O}_m$ gilt. Beachtet man dies und zusätzlich die Tatsache, dass $p^{m+1}\mathbb{Z}_p \subseteq p^{m-n}\mathfrak{D}_n$, so kann man obige Rechnung fortführen

$$\begin{aligned}p^{m-n}\delta_n\big(N_{mn}(u)\big) &\equiv p^{-(m-n)} S_{mn}\big(\delta_m(u)\big) \sum_\sigma \kappa(\sigma) \\ &\equiv p^{-(m-n)} S_{mn}\big(\delta_m(u)\big) p^{m-n} \\ &\equiv S_{mn}\big(\delta_m(u)\big) \mod p^{m-n}\mathfrak{D}_n.\end{aligned}$$

Multipliziert man diese Gleichung mit $p^{-(m-n)}$, so erhält man die Behauptung des Satzes.

QED

Definition 5.13 *Für $n \geq 0$, $\alpha \in K_n^*$ und $\beta \in (1+\mathfrak{m}_n)$ definiert man das Produkt*

$$\langle \alpha, \beta \rangle_n := -\frac{1}{p^{n+1}} S_n\big(\delta_n(\alpha) \log \beta\big).$$

Dieses Produkt ist abhängig vom gewählten Wert für $\delta_n(\alpha)$. Es gilt jedoch der folgende Satz.

Satz 5.14 *Seien $m \geq n$ und $\alpha \in K_m^*$. In den Fällen*

$$\begin{array}{lll} \text{(i)} & m \geq 2n+1, & \beta \in 1 + \mathfrak{m}_n, \\ \text{(ii)} & m \geq n+1, & \beta \in 1 + \mathfrak{m}_n^{p^n}, \\ \text{(iii)} & m \geq n, & \beta \in 1 + \mathfrak{m}_n^{2p^n} \end{array}$$

ist $\langle \alpha, \beta \rangle_m$ eindeutig bestimmt modulo p^{n+1}.

BEWEIS: Da $\delta_m(\alpha)$ wohlbestimmt ist modulo $\mathfrak{D}_m$, ist der Satz eine Folgerung aus Satz 5.7.

QED

Sind für $m \geq n,\ \alpha, \alpha_1, \alpha_2 \in K_m^*$ und $\beta, \beta_1, \beta_2 \in (1 + \mathfrak{m}_n)$ die Bedingungen eines der drei Punkte aus Satz 5.14 erfüllt, so gilt

$$\begin{aligned} \langle \alpha_1 \alpha_2, \beta \rangle_m &\equiv \langle \alpha_1, \beta \rangle_m + \langle \alpha_2, \beta \rangle_m \mod p^{n+1}, \\ \langle \alpha, \beta_1 \beta_2 \rangle_m &\equiv \langle \alpha, \beta_1 \rangle_m + \langle \alpha, \beta_2 \rangle_m \mod p^{n+1}. \end{aligned}$$

Die zweite Äquivalenz ist aufgrund der Funktionalgleichung des Logarithmus (vgl. Satz 2.2) erfüllt.

Satz 5.15 *Seien $l \geq m \geq n$, $\alpha \in K_l^*$ und $\beta \in (1 + \mathfrak{m}_n)$, wobei m und β einer der drei Bedingungen aus Satz 5.14 genügen. Dann gilt*

$$\langle N_{lm}(\alpha), \beta \rangle_m \equiv \langle \alpha, \beta \rangle_l \mod p^{n+1}.$$

BEWEIS: Wendet man Satz 5.12 auf obige Situation an, so erhält man

$$\delta_m\big(N_{lm}(\alpha)\big) \equiv p^{-(l-m)} S_{lm}\big(\delta_l(\alpha)\big) \mod \mathfrak{D}_m.$$

Multipliziert man diese Gleichung mit $-\log \beta$ und wendet dann $p^{-(m+1)} S_m$ an, so ergibt sich

$$-p^{-(m+1)} S_m\big(\delta_m\big(N_{lm}(\alpha)\big) \log \beta\big) \equiv -p^{-(l+1)} S_m\big(S_{lm}\big(\delta_l(\alpha)\big) \log \beta\big)$$

modulo $-p^{-(m+1)} S_m(\mathfrak{D}_m \log \beta)$. Wegen $p^{-(m+1)} S_m(\mathfrak{D}_m \log \beta) \equiv 0 \mod p^{n+1}$ (vgl. Satz 5.7) folgt

$$\begin{aligned} \langle N_{lm}(\alpha), \beta \rangle_m &\equiv -p^{-(m+1)} S_m\big(\delta_m\big(N_{lm}(\alpha)\big) \log \beta\big) \\ &\equiv -p^{-(l+1)} S_l\big(\delta_l(\alpha) \log \beta\big) \\ &\equiv \langle \alpha, \beta \rangle_l \mod p^{n+1}, \end{aligned}$$

womit die Behauptung bewiesen ist.

QED

Definition 5.16 *Für $i \geq 1$ und $n \geq 0$ definiert man*

$$\eta_i^{(n)} := 1 - \pi_n^i \in K_n.$$

Die Elemente $\eta_i^{(n)}$ erzeugen $(1+\mathfrak{m}_n)$ topologisch. Nach [Ha2], Kap.II, § 15, (d), Aussage (II), bilden sogar schon die Elemente $\{1-\pi_n^a,\ 1 \le a \le p^{n+1}, (a,p)=1$ oder $a = p^{n+1}\}$ ein Erzeugendensystem der Gruppe $(1+\mathfrak{m}_n)$.

Da die anschließenden Betrachtungen stets im Körper K_n erfolgen, wird der hochgestellte Index an den $\eta_i^{(n)}$ im folgenden weggelassen.

Um in Satz 5.21 eine Beziehung zwischen dem Produkt $\langle \eta_i, \eta_j \rangle_n$ und dem Hilbertsymbol-Exponenten $[\eta_i, \eta_j]_n$ angegeben zu können, werden zuvor einige Lemmata bewiesen. Diese Aussagen finden sich auch bei [Ha1].

Lemma 5.17 *Für $\alpha, \beta, \gamma \in K_n^*$ mit $\alpha + \beta = \gamma$ gilt*

$$(\alpha, \beta)_n = (\alpha, \gamma)_n (\gamma, \beta)_n.$$

Beweis: Nach Satz 3.11 gilt für $x \in K_n,\ x \neq 0$, die Gleichung $(1-x, x)_n = 1$. Für $x = \frac{\beta}{\gamma}$ und $1 - x = \frac{\alpha}{\gamma}$ folgt damit

$$\begin{aligned} 1 = (\alpha\gamma^{-1}, \beta\gamma^{-1})_n &= (\alpha, \beta\gamma^{-1})_n (\gamma^{-1}, \beta\gamma^{-1})_n \\ &= (\alpha,\beta)_n (\alpha,\gamma^{-1})_n (\gamma^{-1},\beta)_n (\gamma^{-1},\gamma^{-1})_n = (\alpha,\beta)_n (\alpha,\gamma)_n^{-1} (\gamma,\beta)_n^{-1} (\gamma,\gamma)_n. \end{aligned}$$

Somit erhält man

$$(\alpha,\beta)_n = (\alpha,\gamma)_n (\gamma,\beta)_n (\gamma,\gamma)_n^{-1} = (\alpha,\gamma)_n (\gamma,\beta)_n (-1,\gamma)_n^{-1} (-\gamma,\gamma)_n^{-1}.$$

Es bleibt zu zeigen, dass die beiden letzten Hilbertsymbole gleich 1 sind. Aufgrund von Satz 3.11, Teil (v), ist $(-\gamma,\gamma)_n = 1$. Um $(-1,\gamma)_n = 1$ zu zeigen, ist zu begründen, dass -1 eine Norm der Erweiterung $K_n(\sqrt[p^{n+1}]{\gamma})/K_n$ ist. Diese Erweiterung habe den Grad d. Da d ein Teiler von p^{n+1} ist, ist es insbesondere ungerade. Somit kann man -1 als Norm von -1 schreiben,

$$N_{K_n(\sqrt[p^{n+1}]{\gamma})/K_n}(-1) = (-1)^d = -1.$$

Somit folgt $(\alpha,\beta)_n = (\alpha,\gamma)_n (\gamma,\beta)_n$.

QED

Für Elemente η_i und η_j gilt $\eta_i \pi_n^j + \eta_j = (1-\pi_n^i)\pi_n^j + (1-\pi_n^j) = 1 - \pi_n^{i+j} = \eta_{i+j}$, also

$$\eta_i \pi_n^j + \eta_j = \eta_{i+j}.$$

Für das Hilbertsymbol der beiden Summanden gilt mit der Aussage des obigen Lemmas $(\eta_i \pi_n^j, \eta_j)_n = (\eta_i \pi_n^j, \eta_{i+j})_n (\eta_{i+j}, \eta_j)_n$. Ausnutzung der Bimultiplikativität liefert $(\eta_i,\eta_j)_n (\pi_n^j,\eta_j)_n = (\eta_i,\eta_{i+j})_n (\pi_n^j,\eta_{i+j})_n (\eta_{i+j},\eta_j)_n$. Wegen $(\pi_n^j,\eta_j)_n = (\pi_n^j, 1-\pi_n^j)_n = 1$ ergibt sich als Endergebnis

$$(\eta_i,\eta_j)_n = (\eta_i,\eta_{i+j})_n (\pi_n,\eta_{i+j})_n^j (\eta_{i+j},\eta_j)_n. \tag{5.9}$$

Wendet man die Formel (5.9) iterativ auf jedes in ihr vorkommende Hilbertsymbol $(\eta_r, \eta_s)_n$ an, so erhält man weitere Iterationsformeln

$$\begin{aligned}(\eta_i, \eta_j)_n = {} & (\eta_i, \eta_{2i+j})_n (\pi_n, \eta_{2i+j})_n^{i+j} (\eta_{2i+j}, \eta_{i+j})_n \cdot \\ & \cdot (\pi_n, \eta_{i+j})_n^j \cdot \\ & \cdot (\eta_{i+j}, \eta_{i+2j})_n (\pi_n, \eta_{i+2j})_n^j (\eta_{i+2j}, \eta_j)_n\end{aligned} \tag{5.10}$$

und

$$\begin{aligned}(\eta_i, \eta_j)_n = {} & (\eta_i, \eta_{3i+j})_n (\pi_n, \eta_{3i+j})_n^{2i+j} (\eta_{3i+j}, \eta_{2i+j})_n \cdot \\ & \cdot (\pi_n, \eta_{2i+j})_n^{i+j} \cdot \\ & \cdot (\eta_{2i+j}, \eta_{3i+2j})_n (\pi_n, \eta_{3i+2j})_n^{i+j} (\eta_{3i+2j}, \eta_{i+j})_n \cdot \\ & \cdot (\pi_n, \eta_{i+j})_n^j \cdot \\ & \cdot (\eta_{i+j}, \eta_{2i+3j})_n (\pi_n, \eta_{2i+3j})_n^{i+2j} (\eta_{2i+3j}, \eta_{i+2j})_n \cdot \\ & \cdot (\pi_n, \eta_{i+2j})_n^j \cdot \\ & \cdot (\eta_{i+2j}, \eta_{i+3j})_n (\pi_n, \eta_{i+3j})_n^j (\eta_{i+3j}, \eta_j)_n.\end{aligned} \tag{5.11}$$

Den Formeln (5.9), (5.10) und (5.11) kann man die Bruchfolgen

$$\frac{1}{0}\ \frac{1}{1}\ \frac{0}{1}, \tag{5.12}$$

$$\frac{1}{0}\ \frac{2}{1}\ \frac{1}{1}\ \frac{1}{2}\ \frac{0}{1}, \tag{5.13}$$

und

$$\frac{1}{0}\ \frac{3}{1}\ \frac{2}{1}\ \frac{3}{2}\ \frac{1}{1}\ \frac{2}{3}\ \frac{1}{2}\ \frac{1}{3}\ \frac{0}{1} \tag{5.14}$$

zuordnen, in denen nebeneinander stehende Brüche $\frac{r}{s}$ und $\frac{r'}{s'}$ einen Faktor $(\eta_{ri+sj}, \eta_{r'i+s'j})_n$ symbolisieren. Jedem inneren Bruch $\frac{r}{s}$ entspricht ein Hilbertsymbol $(\pi_n, \eta_{ri+sj})_n^{r'i+s'j}$, wobei $\frac{r'}{s'}$ der rechte Nachbar von $\frac{r}{s}$ in der Bruchfolge ist, in der $\frac{r}{s}$ zum ersten Mal vorkommt. Aus der Iterationsvorschrift (5.9) erkennt man, dass man die $(k+1)$-te Bruchfolge aus der k-ten Bruchfolge erhält, indem man zwischen zwei Brüche $\frac{r}{s}$ und $\frac{r'}{s'}$ den sogenannten Medianten $\frac{r+r'}{s+s'}$ einschiebt. Die auf diese Art und Weise entstehende Folge von Bruchfolgen hat folgende Eigenschaften.

Lemma 5.18

(i) *Für die in der k-ten Bruchfolge neu hinzukommenden $\frac{r}{s}$ wird die Summe $r+s$ für hinreichend großes k beliebig groß.*

(ii) *Die Zahlen r, r', s, s' in den Ausdrücken $(\pi_n, \eta_{ri+sj})_n^{r'i+s'j}$ erfüllen die Gleichung $rs' - r's = 1$.*

(iii) *Für $k \to \infty$ geht die k-te Bruchfolge in die Menge aller positiven, gekürzten Brüche $\neq \frac{1}{0}, \frac{0}{1}$ über.*

Beweis von (i): Diese Aussage folgt direkt aus der Bildungsvorschrift (Mediantenteinschub).

Beweis von (ii): Nach Konstruktion genügt es zu beweisen, dass in jeder Bruchfolge für zwei benachbarte Brüche $\frac{r}{s}$ und $\frac{r'}{s'}$ die Gleichung $rs' - r's = 1$ gilt. Dies geschieht mittels Induktion. Die Bruchfolge (5.12), in der diese Beziehung gilt, dient als Induktionsanfang. Seien $\frac{r}{s}$ und $\frac{r'}{s'}$ benachbarte Brüche in der k-ten Bruchfolge, es gilt also $rs' - r's = 1$. Es ist zu zeigen, dass die Beziehung auch für die benachbarten Brüche $\frac{r}{s}$ und $\frac{r+r'}{s+s'}$ sowie $\frac{r+r'}{s+s'}$ und $\frac{r'}{s'}$ in der $(k+1)$-ten Bruchfolge gilt. Man berechnet

$$\begin{aligned} r(s+s') - (r+r')s &= rs' - r's = 1, \\ (r+r')s' - r'(s+s') &= rs' - r's = 1. \end{aligned}$$

Damit ist die zweite Aussage bewiesen.

Beweis von (iii): Per Induktion überzeugt man sich zuerst davon, dass alle in der k-ten Bruchfolge vorkommenden Brüche $\frac{r}{s} \neq \frac{1}{0}, \frac{0}{1}$, reduziert sind, d.h. dass $(r,s) = 1$ gilt. Für die erste Bruchfolge (5.12) ist dies ersichtlich. Seien $\frac{r}{s}$ und $\frac{r'}{s'}$ gekürzte benachbarte Brüche der k-ten Bruchfolge. Es ist zu zeigen, dass $\frac{r+r'}{s+s'}$ ein gekürzter Bruch ist. Nach Eigenschaft (ii) gilt

$$r(s+s') - (r+r')s = 1.$$

Da jede Linearkombination von $r+r'$ und $s+s'$ durch den größten gemeinsamen Teiler von $r+r'$ und $s+s'$ teilbar ist, folgt $(r+r', s+s') = 1$.
Sei $\frac{a}{b} \neq 1$ eine beliebige positive reduzierte gebrochene Zahl. Es ist zu zeigen, dass diese Zahl in irgendeiner Bruchfolge auftritt. Die Idee zu diesem Beweis ist [Hal], Lemme I, entnommen. Zunächst kann man $\frac{a}{b}$ als Summe von a Summanden $\frac{1}{0}$ und b Summanden $\frac{0}{1}$ schreiben,

$$\frac{a}{b} = \underbrace{\frac{1}{0} + \ldots + \frac{1}{0}}_{a} + \underbrace{\frac{0}{1} + \ldots + \frac{0}{1}}_{b},$$

wobei mit "+" hier und im folgenden immer die Mediantenbildung gemeint ist. Ohne Einschränkung sei $a > b$, ansonsten betrachte man $\frac{b}{a}$. Dann kann man die b Summanden $\frac{0}{1}$ mit b Stück von den Summanden $\frac{1}{0}$ addieren und erhält

$$\frac{a}{b} = \underbrace{\frac{1}{0} + \ldots + \frac{1}{0}}_{a-b} + \underbrace{\frac{1}{1} + \ldots + \frac{1}{1}}_{b}.$$

Falls jetzt $a - b > b$ gilt, so kann man die b Summanden $\frac{1}{1}$ mit b Stück von den Summanden $\frac{1}{0}$ addieren. Führt man den Algorithmus fort, so ergibt sich

$$\frac{a}{b} = \underbrace{\frac{1}{0} + \ldots + \frac{1}{0}}_{a-mb} + \underbrace{\frac{m}{1} + \ldots + \frac{m}{1}}_{b},$$

wobei m der ganze Teil von $\frac{a}{b}$ ist. Es sei bemerkt, dass die beiden vorkommenden Summanden $\frac{1}{0}$ und $\frac{m}{1}$ in der entsprechenden Bruchfolge benachbart sind. Es gilt $a - mb < b$. Addiert man nun die $a - mb$ Summanden $\frac{1}{0}$ zu $a - mb$ von den Summanden $\frac{m}{1}$, so erreicht man, dass auf der rechten Seite alle Nenner 1 sind,

$$\frac{a}{b} = \underbrace{\frac{m}{1} + \ldots + \frac{m}{1}}_{b-(a-mb)} + \underbrace{\frac{m+1}{1} + \ldots + \frac{m+1}{1}}_{a-mb}.$$

Falls nun die Gleichheit $a - mb = b - (a - mb)$ gilt, also $a = mb + \frac{b}{2}$ ist, muss b gerade sein. Damit ist $\frac{b}{2}$ ein Teiler von a und b. Dies steht nur dann nicht im Widerspruch zur Teilerfremdheit von a und b, wenn $\frac{b}{2} = 1$, also $b = 2$ gilt. In diesem Fall folgt jedoch $a - mb = b - (a - mb) = 1$, so dass man $\frac{a}{b}$ bereits an dieser Stelle als Summe zweier benachbarter Brüche einer Bruchfolge dargestellt hat.
Gilt $a - mb \neq b - (a - mb)$, so seien $a' := \max\{a - mb, b - (a - mb)\}$ und $b' := \min\{a - mb, b - (a - mb)\}$. Wiederholt man nun obige Schritte mit a' anstelle von a und b' anstelle von b, so erhält man

$$\frac{a}{b} = \underbrace{\frac{m}{1} + \ldots + \frac{m}{1}}_{a'-m'b'} + \underbrace{\frac{m'm+1}{m'} + \ldots + \frac{m'm+1}{m'}}_{b'}$$

oder

$$\frac{a}{b} = \underbrace{\frac{m}{1} + \ldots + \frac{m}{1}}_{b'} + \underbrace{\frac{m'm+1}{m'} + \ldots + \frac{m'm+1}{m'}}_{a'-m'b'}$$

mit m' als ganzem Teil von $\frac{a'}{b'}$. Wieder sind die beiden vorkommenden Summanden benachbarte Brüche einer entsprechenden Bruchfolge. Setzt man dieses Verfahren fort, so liefert es nach endlich vielen Schritten die Darstellung

$$\frac{a}{b} = \frac{r}{s} + \frac{r'}{s'},$$

in der die beiden Summanden rechts benachbarte Brüche in einer Bruchfolge sind. Somit ist $\frac{a}{b}$ Element der darauffolgenden Bruchfolge.

QED

Lemma 5.19 *Es gilt*

$$(\eta_i, \eta_j)_n = 1 \quad \textit{für} \quad \max(i,j) \geq (n+1)(p-1)p^n + p^n + 1,$$
$$(\pi_n, \eta_j)_n = 1 \quad \textit{für} \quad j \geq (n+1)(p-1)p^n + p^n + 1.$$

BEWEIS: Sei $j \geq (n+1)(p-1)p^n + p^n + 1$. Dann gilt unter Verwendung von Lemma 4.2 mit $a = n+1$ und $b = p^n + 1$

$$\eta_j = 1 - \pi_n^j \in \left(1 + \mathfrak{m}_n^{(n+1)(p-1)p^n + p^n + 1}\right) = \left(1 + p^{n+1}\mathfrak{m}_n^{p^n+1}\right) = \left(1 + \mathfrak{m}_n^{p^n+1}\right)^{p^{n+1}}.$$

Dies bedeutet, dass η_j eine p^{n+1}-te Potenz eines Elementes aus $1 + \mathfrak{m}_n^{p^n+1}$ ist und somit $K_n(\sqrt[p^{n+1}]{\eta_j}) = K_n$. Mit Hilfe der Eigenschaft (iii) des Hilbertsymbols im Satz 3.11 folgt $(x, \eta_j)_n = 1$ für alle $x \in K_n^*$, insbesondere auch für $x = \eta_i$ oder $x = \pi_n$.
Falls $i = \max(i,j) \geq (n+1)(p-1)p^n + p^n + 1$, so verwende man $(\eta_i, \eta_j)_n = (\eta_j, \eta_i)_n^{-1}$.

QED

Lemma 5.20 *Für das p^{n+1}-te Hilbertsymbol von $\eta_i, \eta_j \in K_n$ gilt*

$$(\eta_i, \eta_j)_n = \prod_{\substack{r,s \geq 1 \\ (r,s)=1}} (\pi_n, \eta_{ir+js})_n^{ir'+js'},$$

wobei $r', s' \in \mathbb{N}$ mit $rs' - r's = 1$. Eine alternative Formulierung der Behauptung ist

$$[\eta_i, \eta_j]_n = \sum_{\substack{r,s \geq 1 \\ (r,s)=1}} (ir' + js')[\pi_n, \eta_{ir+js}].$$

BEWEIS: In jedem Faktor $(\eta_a, \eta_b)_n$ der k-ten Iterationsformel, vgl. (5.9) bis (5.11), entspricht einer der beiden Indizes a oder b einem in der k-ten Bruchfolge, vgl. (5.12) bis (5.14), neu hinzugekommenen $\frac{r}{s}$, also $a = ri + sj$ oder $b = ri + sj$. Wegen $ri + sj \geq r + s$ und Lemma 5.18, Teil (i), wird dieser Index für hinreichend große k beliebig groß. Nach Lemma 5.19 werden also die Faktoren $(\eta_a, \eta_b)_n$ für hinreichend großes k gleich 1. Ebenfalls nach Lemma 5.19 und Punkt (i) von Lemma 5.18 werden ab einem bestimmten k auch alle neu hinzukommenden $(\pi_n, \eta_a)_n^x$ gleich 1. Somit kann die Iteration unendlich oft ausgeführt werden, das entstehende unendliche Produkt konvergiert. Man erhält

$$(\eta_i, \eta_j)_n = \prod_{\substack{r,s \geq 1 \\ (r,s)=1}} (\pi_n, \eta_{ir+js})_n^{ir'+js'}.$$

Der Bereich, über den sich das Produkt erstreckt, ergibt sich aus Punkt (iii) von Lemma 5.18. Nach Punkt (ii) dieses Lemmas sind die r', s' so zu wählen, dass $rs' - r's = 1$. Dabei ist es unerheblich, welche konkrete Lösung r', s' gewählt wurde, denn jede andere Lösung r'', s'' ergibt sich aus ersterer durch $r'' = r' + cr$ und $s'' = s' + cs$ mit einer beliebigen natürlichen Zahl c. Es gilt

$$(\pi_n, \eta_{ir+js})_n^{ir''+js''} = (\pi_n, \eta_{ir+js})_n^{ir'+js'} (\pi_n, \eta_{ir+js})_n^{c(ir+js)}$$

und $$(\pi_n, \eta_{ir+js})_n^{c(ir+js)} = (\pi_n^{ir+js}, \eta_{ir+js})_n^c = (\pi_n^{ir+js}, 1 - \pi_n^{ir+js})_n^c = 1.$$

Damit ist das Lemma bewiesen.

QED

Mit dieser Vorarbeit ist es nun möglich, den angekündigten Satz über die Beziehung zwischen $[\eta_j, \eta_k]_n$ und $\langle \eta_j, \eta_k \rangle_n$ zu formulieren.

Satz 5.21 *Für $n \geq 0,\ j \geq 1$ und $k \geq \big((n+2)(p-1)+1\big)p^{n-1}$ gilt*

$$[\eta_j, \eta_k]_n \equiv \langle \eta_j, \eta_k \rangle_n \mod p^{n+1}.$$

BEWEIS: Die linke Seite $[\eta_j, \eta_k]_n$ ist nach Definition wohlbestimmt modulo p^{n+1}. Zuerst muss gezeigt werden, dass auch $\langle \eta_j, \eta_k \rangle_n$ wohlbestimmt ist modulo p^{n+1}. Nach Aussage (iii) von Satz 5.14, entspricht dies dem Nachweis von $\eta_k \in 1 + \mathfrak{m}_n^{2p^n}$ bzw. $k \geq 2p^n$. Für $n = 0$ gilt nach Voraussetzung $k \geq (2p-1)p^{-1} = 2 - \frac{1}{p}$, d.h. $k \geq 2 = 2p^0$. Für $n > 0$ folgt

$$k \geq \big((n+2)(p-1)+1\big)p^{n-1} = 2p^n + (np - n - 1)p^{n-1} \geq 2p^n,$$

wobei die letzte Ungleichung äquivalent zu $np - n - 1 \geq 0$ bzw. $p - 1 \geq \frac{1}{n}$ ist. Dies ist für $n > 0$ erfüllt.

Somit genügt es, die Behauptung des Lemmas für einen speziellen Wert von $\delta_n(\eta_j)$ zu beweisen. Es ist $f(T) = 1 - T^j$ eine Potenzreihe für η_j. Somit gilt

$$\delta_n(\eta_j) = \frac{\zeta_n}{\eta_j} f'(\pi_n) = -\zeta_n j \frac{\pi_n^{j-1}}{1 - \pi_n^j}.$$

Wegen $\frac{\pi_n^{j-1}}{1-\pi_n^j} = \frac{1}{\pi_n} \frac{\pi_n^j}{1-\pi_n^j}$ und $\frac{\pi_n^j}{1-\pi_n^j} = \frac{1}{1-\pi_n^j} - 1 = \sum_{r=1}^{\infty} (\pi_n^j)^r$ ergibt sich

$$\delta_n(\eta_j) = -\zeta_n \sum_{r=1}^{\infty} j \pi_n^{jr-1}.$$

Mit $\log \eta_k = -\sum_{s=1}^{\infty} \frac{\pi_n^{ks}}{s}$ (vgl. Definition 5.16) folgt

$$\langle \eta_j, \eta_k \rangle_n = -\frac{1}{p^{n+1}} S_n\big(\delta_n(\eta_j) \log \eta_k\big) = -\frac{1}{p^{n+1}} \sum_{r,s \geq 1} \frac{j}{s} S_n(\zeta_n \pi_n^{ks+jr-1}).$$

Sei $u = \mathrm{ggT}\,(r,s)$ für jedes Paar (r,s) und seien $r = ur', s = us'$ mit $(r', s') = 1$. Dann kann man die Argumentation fortsetzen,

$$\langle \eta_j, \eta_k \rangle_n = -\frac{1}{p^{n+1}} \sum_{\substack{r',s' \geq 1 \\ (r',s')=1}} \sum_{u \geq 1} \frac{j}{us'} S_n\big(\zeta_n \pi_n^{u(ks'+jr')-1}\big),$$

und nach einer Rückbenennung $r' \to r, s' \to s$ erhält man

$$\langle \eta_j, \eta_k \rangle_n = -\frac{1}{p^{n+1}} \sum_{\substack{r,s\geq 1\\(r,s)=1}} \sum_{u\geq 1} \frac{j}{us} S_n\big(\zeta_n \pi_n^{u(ks+jr)-1}\big). \tag{5.15}$$

Andererseits gilt nach Lemma 5.20

$$[\eta_j, \eta_k]_n = \sum_{\substack{r,s\geq 1\\(r,s)=1}} (jr'+ks')[\pi_n, \eta_{jr+ks}]_n,$$

wobei $r', s' \in \mathbb{N}$ so zu wählen sind, dass $rs' - r's = 1$ erfüllt ist. Mit der Formel $[\pi_n, \beta]_n = -p^{-(n+1)} S_n\big(\frac{\zeta_n}{\pi_n} \log \beta\big)$ für $\beta \in (1+\mathfrak{m}_n)$ aus dem zweiten Ergänzungssatz von Artin-Hasse, Theorem 5.2, folgt

$$\begin{aligned}
[\eta_j, \eta_k]_n &= -\frac{1}{p^{n+1}} \sum_{\substack{r,s\geq 1\\(r,s)=1}} (jr'+ks') S_n\left(\frac{\zeta_n}{\pi_n} \log \eta_{jr+ks}\right) \\
&= \frac{1}{p^{n+1}} \sum_{\substack{r,s\geq 1\\(r,s)=1}} (jr'+ks') \sum_{u\geq 1} \frac{1}{u}\, S_n\left(\frac{\zeta_n}{\pi_n} \pi_n^{u(jr+ks)}\right) \\
&= \frac{1}{p^{n+1}} \sum_{\substack{r,s\geq 1\\(r,s)=1}} \sum_{u\geq 1} \frac{jr'+ks'}{u}\, S_n\big(\zeta_n \pi_n^{u(jr+ks)-1}\big).
\end{aligned} \tag{5.16}$$

Mit $rs' - r's = 1$ schließt man aus (5.15) und (5.16)

$$\begin{aligned}
[\eta_j, \eta_k]_n - \langle \eta_j, \eta_k \rangle_n &= \frac{1}{p^{n+1}} \sum_{\substack{r,s\geq 1\\(r,s)=1}} \sum_{u\geq 1} \Big(\frac{j}{us} + \frac{jr'+ks'}{u}\Big)\, S_n\big(\zeta_n \pi_n^{u(jr+ks)-1}\big) \\
&= \frac{1}{p^{n+1}} \sum_{\substack{r,s\geq 1\\(r,s)=1}} \sum_{u\geq 1} \frac{s'(jr+ks)}{us}\, S_n\big(\zeta_n \pi_n^{u(jr+ks)-1}\big) \\
&= \sum_{\substack{r,s\geq 1\\(r,s)=1}} \frac{s'}{s}\Big(\frac{1}{p^{n+1}} \sum_{u\geq 1} \frac{jr+ks}{u}\, S_n\big(\zeta_n \pi_n^{u(jr+ks)-1}\big)\Big).
\end{aligned}$$

Für festes r und s gilt jedoch

$$\begin{aligned}
&\frac{1}{p^{n+1}} \sum_{u\geq 1} (jr+ks) \frac{1}{u}\, S_n\big(\zeta_n \pi_n^{u(jr+ks)-1}\big) = \\
&\quad = -\frac{1}{p^{n+1}} (jr+ks) S_n\left(\frac{\zeta_n}{\pi_n} \log \eta_{jr+ks}\right) \\
&\quad = (jr+ks)[\pi_n, \eta_{jr+ks}]_n = [\pi_n^{jr+ks}, 1-\pi_n^{jr+ks}]_n \equiv 0 \mod p^{n+1},
\end{aligned}$$

so dass in obiger Summe, da s und s' teilerfremd sind, modulo p^{n+1} nur die Summanden übrig bleiben, in denen s ein Vielfaches von p ist. Somit erhält man

$$[\eta_j, \eta_k]_n - \langle \eta_j, \eta_k \rangle_n \equiv \frac{1}{p^{n+1}} \sum_{\substack{r,s\geq 1\\(r,s)=1\\p\mid s}} \sum_{u\geq 1} \frac{s'(jr+ks)}{us}\, S_n\big(\zeta_n \pi_n^{u(jr+ks)-1}\big) \mod p^{n+1}.$$

Es verbleibt der Nachweis, dass jeder Summand auf der rechten Seite gleich Null modulo p^{n+1} ist. Äquivalent dazu ist die Gültigkeit der Ungleichung

$$\nu_n\Big(\frac{1}{p^{n+1}}\frac{s'(jr+ks)}{us}\,S_n\big(\zeta_n\pi_n^{u(jr+ks)-1}\big)\Big) \geq (n+1)(p-1)p^n.$$

Mit Hilfe der Abschätzung aus Satz 4.12 erhält man

$$\begin{aligned}
&\nu_n\Big(\frac{1}{p^{n+1}}\frac{s'(jr+ks)}{us}\,S_n\big(\zeta_n\pi_n^{u(jr+ks)-1}\big)\Big) \;= \\
&\qquad= \nu_n\Big(S_n\Big(\frac{1}{p^{n+1}}\frac{s'(jr+ks)}{us}\zeta_n\pi_n^{u(jr+ks)-1}\Big)\Big) \\
&\qquad> \nu_n\Big(\frac{1}{p^{n+1}}\frac{s'(jr+ks)}{us}\zeta_n\pi_n^{u(jr+ks)-1}\Big) + \big(n(p-1)-1\big)p^n \\
&\qquad= \nu_n\Big(\frac{\zeta_n}{p^{n+1}us}\pi_n^{u(jr+ks)-1}\Big) + \nu_n\big(s'(jr+ks)\big) + \big(n(p-1)-1\big)p^n.
\end{aligned}$$

Nun werden die beiden ersten Summanden jeder für sich abgeschätzt.
Sei e die p-Potenz, die us exakt teilt. Dann gilt $e \geq 1$ aufgrund der Voraussetzung an s, und es folgt $us \geq p^e$. Mit der Voraussetzung an k ergibt sich für den ersten Summanden

$$\begin{aligned}
\nu_n\Big(\frac{\zeta_n}{p^{n+1}us}\pi_n^{u(jr+ks)-1}\Big) &= u(jr+ks) - 1 - (n+1+e)(p-1)p^n \\
&\geq \big((n+2)(p-1)+1\big)p^{n-1+e} - (n+1+e)(p-1)p^n.
\end{aligned}$$

Betrachtet man die rechte Seite der Ungleichung als Funktion $f(e)$, so gilt $f(e) \geq p^n$ für alle $e \geq 1$. Dies ist wegen $f(1) = p^n$ und $f'(e) \geq 0$ für $e \geq 1$ erfüllt.

Die Beziehung $p \mid s$ liefert für den zweiten Summanden

$$\nu_n\big(s'(jr+ks)\big) \geq \nu_n(jr+ks) \geq \nu_n(s) \geq (p-1)p^n.$$

Abschließend folgt

$$\begin{aligned}
\nu_n\Big(\frac{1}{p^{n+1}}\frac{s'(jr+ks)}{us}\,S_n\big(\zeta_n\pi_n^{u(jr+ks)-1}\big)\Big) &\geq p^n + (p-1)p^n + \big(n(p-1)-1\big)p^n \\
&= (n+1)(p-1)p^n,
\end{aligned}$$

womit der Beweis erbracht ist.

QED

Satz 5.22 *Für $m \geq 3n+1$, $\alpha \in K_m^*$, $\beta \in (1+\mathfrak{m}_n)$ gilt*

$$[N_{mn}(\alpha), \beta]_n = \langle \alpha, \beta \rangle_m.$$

BEWEIS: Nach Definition ist die linke Seite eindeutig bestimmt modulo p^{n+1}. Da die rechte Seite nach Satz 5.14, Teil (i), ebenfalls wohlbestimmt ist modulo p^{n+1}, genügt es, die Gleichheit modulo p^{n+1} zu zeigen.

Da jeder Körper K_m den Körper $\mathbb{F}_p$ als Restklassenkörper hat, gilt nach [Lor2], § 25, F6, die Zerlegung $K_m^* = \langle \pi_m \rangle \times \mu_{p-1} \times (1 + \mathfrak{m}_m)$. Dabei bezeichnen μ_{p-1} die Gruppe der $(p-1)$-ten Einheitswurzeln und $\langle \pi_m \rangle = \{\pi_m^r, r \in \mathbb{Z}\}$. Somit ist es ausreichend, das Lemma für $\alpha = \pi_m,\ \alpha = \xi \in \mu_{p-1}$ und $\alpha \in (1+\mathfrak{m}_m)$ zu beweisen.

Sei $\alpha = \pi_m$. Dann gilt nach Lemma 4.7 die Gleichung $N_{mn}(\pi_m) = \pi_n$. Die Gleichung (5.8) von Seite 53 und der Beweis von Satz 5.12 liefern

$$\delta_m(\pi_m) \equiv \frac{\zeta_m}{\pi_m} \mod \mathfrak{D}_m \quad \text{und} \quad S_{mn}\Big(\frac{\zeta_m}{\pi_m}\Big) = p^{m-n}\frac{\zeta_n}{\pi_n}.$$

Somit ergibt sich

$$\begin{aligned}
\langle \pi_m, \beta \rangle_m &= -\frac{1}{p^{m+1}}\, S_m\big(\delta_m(\pi_m)\log\beta\big) \\
&\equiv -\frac{1}{p^{m+1}}\, S_m\Big(\frac{\zeta_m}{\pi_m}\log\beta\Big) \mod -\frac{1}{p^{m+1}}\, S_m(\mathfrak{D}_m \log\beta) \\
&= -\frac{1}{p^{m+1}}\, S_n\Big(S_{mn}\Big(\frac{\zeta_m}{\pi_m}\Big)\log\beta\Big) = -\frac{1}{p^{n+1}}\, S_n\Big(\frac{\zeta_n}{\pi_n}\log\beta\Big) \\
&= [\pi_n, \beta]_n = [N_{mn}(\pi_m), \beta]_n,
\end{aligned}$$

wobei die vorletzte Gleichheit durch den zweiten Ergänzungssatz von Artin-Hasse, Theorem 5.2, gegeben ist. Es verbleibt der Nachweis von

$$\frac{1}{p^{m+1}}\, S_m(\mathfrak{D}_m \log\beta) \equiv 0 \mod p^{n+1}.$$

Zunächst kann man den Ausdruck unter Verwendung der Gleichheiten $S_{mn}(\mathfrak{D}_m) = p^{m+1}p^{m-n}\pi_0^{-1}\mathcal{O}_n$ (vgl. Beweis von Punkt (i) von Satz 5.7) und $p^{n+1}\pi_0^{-1}\mathcal{O}_n = \mathfrak{D}_n$ (vgl. Bemerkung am Ende von Abschnitt 4.2) umformen zu

$$\begin{aligned}
p^{-(m+1)}S_m(\mathfrak{D}_m\log\beta) &= p^{-(m+1)}S_n\big(S_{mn}(\mathfrak{D}_m)\log\beta\big) \\
&= p^{-(m+1)}S_n(p^{m+1}p^{m-n}\pi_0^{-1}\mathcal{O}_n\log\beta) \\
&= p^{m-n}p^{-(n+1)}S_n(\mathfrak{D}_n\log\beta).
\end{aligned}$$

Nach Satz 5.6 gilt $S_n(\mathfrak{D}_n\log\beta) \equiv 0 \mod p^{n+1}$, so dass der obige Ausdruck durch p^{m-n} teilbar ist. Wegen der Voraussetzung $m \geq 3n+1$ ist er somit auch durch p^{n+1} teilbar. Damit ist die Formel für den Fall $\alpha = \pi_m$ bewiesen.

Sei nun $\alpha = \xi \in \mu_{p-1}$. Für ein beliebiges $\beta \in (1+\mathfrak{m}_n)$ gilt $\langle 1, \beta\rangle_m = 0$ und $[1,\beta]_m = 0$. Zum einen schließt man daraus $0 = \langle \xi^{p-1}, \beta\rangle_m \equiv (p-1)\langle \xi, \beta\rangle_m \mod p^{n+1}$, also

$$\langle \xi, \beta\rangle_m \equiv 0 \mod p^{n+1}.$$

Zum anderen kann $0 = [N_{mn}(\xi^{p-1}), \beta]_n = [N_{mn}(\xi)^{p-1}, \beta]_n \equiv (p-1)[N_{mn}(\xi), \beta]_n \mod p^{n+1}$ gefolgert werden, so dass

$$[N_{mn}(\xi), \beta]_n \equiv 0 \mod p^{n+1}.$$

Insgesamt ist somit $[N_{mn}(\xi), \beta]_n \equiv \langle \xi, \beta\rangle_m \mod p^{n+1}$ gezeigt.

Für $\alpha \in (1+\mathfrak{m}_m)$ genügt es, $\alpha = \eta_l^{(m)} = 1-\pi_m^l,\ l \geq 1$, zu betrachten, da $(1+\mathfrak{m}_m)$ von diesen Elementen topologisch erzeugt wird. Bevor jedoch diese Betrachtung erfolgen kann, müssen die Potenzen von β genauer untersucht werden.

Sei $k = \big((m-2n)(p-1)+1\big)p^m$. Wegen $p \geq 3$ und der Voraussetzung an m folgt $p(m-2n) \geq 3(m-2n) \geq 2(n+1) + (m-2n) = m+2$ und

$$k \geq \big((m+2)(p-1)+1\big)p^{m-1}.$$

Dies entspricht gerade einer der Bedingungen von Satz 5.21. Jedes $\beta \in (1+\mathfrak{m}_n)$ besitzt eine Darstellung $\beta = 1+\pi_n y$ mit $y \in \mathcal{O}_n$. Nun soll gezeigt werden, dass $\beta^{p^n} \in \big(1+\mathfrak{m}_n^{p^n}\big)$ gilt. Zunächst ist

$$\beta^{p^n} = (1+\pi_n y)^{p^n} = 1 + \sum_{j=1}^{p^n} \binom{p^n}{j} \pi_n^j\, y^j$$

und es gilt

$$\begin{aligned}\nu_n(\beta^{p^n}-1) &\geq \min\left\{\nu_n\left(\binom{p^n}{j}\right) + j + \nu_n(y^j),\ 1 \leq j \leq p^n\right\}\\ &\geq \min\left\{\nu_n\left(\binom{p^n}{j}\right) + j,\ 1 \leq j \leq p^n\right\}.\end{aligned}$$

Es ist also der Nachweis zu erbringen, dass

$$\nu_n\Big(\binom{p^n}{j}\Big) + j \geq p^n$$

für alle $j = 1, \ldots, p^n$ gilt. Dazu muss die Bewertung des Binomialkoeffizienten abgeschätzt werden. Analog zum Beweis von Lemma 4.2 erhält man

$$v_p\Big(\binom{p^n}{j}\Big) = n - v_p(j).$$

Damit folgt $\nu_n\big(\binom{p^n}{j}\big) + j = (p-1)p^n\big(n-v_p(j)\big) + j$. Für festes $v_p(j) = e$ hat j die Gestalt $j = ap^e \geq p^e$ und es ist $(p-1)p^n(n-e) + j \geq (p-1)p^n(n-e) + p^e$. Die

Ausdrücke $(p-1)p^n(n-e)+p^e$ werden, solange $e \leq n$, für wachsendes e immer kleiner, denn es gilt

$$\begin{aligned} & (p-1)p^n(n-e)+p^e \geq (p-1)p^n\big(n-(e+1)\big)+p^{e+1} \\ \iff \quad & (p-1)p^n\big((n-e)-(n-(e+1))\big) \geq p^{e+1}-p^e \\ \iff \quad & (p-1)p^n \geq (p-1)p^e \\ \iff \quad & p^n \geq p^e \\ \iff \quad & n \geq e. \end{aligned}$$

Folglich nimmt der Ausdruck $\nu_n\big(\binom{p^n}{j}\big)+j$ seinen kleinsten Wert für $v_p(j)=n$, also für $j=p^n$, an. Dies impliziert

$$\nu_n\Big(\binom{p^n}{j}\Big)+j \geq (p-1)p^n v_p\Big(\binom{p^n}{p^n}\Big)+p^n = p^n$$

und somit ist $\beta^{p^n} \in \big(1+\mathfrak{m}_n^{p^n}\big)$ gezeigt. Nun kann man schlussfolgern, dass

$$\beta^{p^{m-n}} = \big(\beta^{p^n}\big)^{p^{m-2n}} \in \big(1+\mathfrak{m}_n^{p^n}\big)^{p^{m-2n}}.$$

Aufgrund von Lemma 4.2 und der Voraussetzung an m folgt

$$\beta^{p^{m-n}} \in \big(1+p^{m-2n}\mathfrak{m}_n^{p^n}\big).$$

Es ist

$$\begin{aligned} 1+p^{m-2n}\mathfrak{m}_n^{p^n} &= 1+\mathfrak{m}_n^{(m-2n)(p-1)p^n+p^n} = 1+\pi_n^{(m-2n)(p-1)p^n+p^n} \\ &\subseteq 1+\pi_m^{p^{m-n}((m-2n)(p-1)p^n+p^n)}\mathcal{O}_m = 1+\mathfrak{m}_m^k \end{aligned}$$

und somit

$$\beta^{p^{m-n}} \in \big(1+\mathfrak{m}_m^k\big).$$

Da $(1+\mathfrak{m}_m)$ von den Elementen $\eta_j^{(m)} = 1-\pi_m^j$ topologisch erzeugt wird, ist $\beta^{p^{m-n}}$ Grenzwert einer Folge gewisser Produkte von Potenzen von Elementen $\eta_j^{(m)}$, $j \geq \big((m+2)(p-1)+1\big)p^{m-1}$.

Mit Satz 5.21 und Satz 5.14 gilt daher $[\eta_l^{(m)}, \beta^{p^{m-n}}]_n \equiv \langle \eta_l^{(m)}, \beta^{p^{m-n}}\rangle_n \mod p^{n+1}$. Aus Satz 4.22 folgt nun

$$\begin{aligned} \big(N_{mn}(\eta_l^{(m)}),\beta\big)_n &= \big(\eta_l^{(m)},\beta\big)_m^{p^{m-n}} = \big(\eta_l^{(m)},\beta^{p^{m-n}}\big)_m \\ &= \zeta_m^{[\eta_l^{(m)},\beta^{p^{m-n}}]_m} = \zeta_m^{\langle \eta_l^{(m)},\beta^{p^{m-n}}\rangle_m} \\ &= \zeta_m^{p^{m-n}\langle \eta_l^{(m)},\beta\rangle_m}. \end{aligned}$$

Der Ausdruck $\big(\eta_l^{(m)},\beta\big)_m^{p^{m-n}}$ hinter dem ersten Gleichheitszeichen ist eine p^{n+1}-te Einheitswurzel. Daraus folgt

$$p^{n+1}p^{m-n}\langle \eta_l^{(m)},\beta\rangle_m \equiv 0 \mod p^{m+1}$$

und man erkennt, dass $\langle \eta_l^{(m)}, \beta \rangle_m$ eine ganze p-adische Zahl ist. Somit gilt

$$\zeta_m^{p^{m-n}\langle \eta_l^{(m)}, \beta \rangle_m} = \zeta_n^{\langle \eta_l^{(m)}, \beta \rangle_m}$$

und damit ist $[N_{mn}(\eta_l^{(m)}), \beta]_n = \langle \eta_l^{(m)}, \beta \rangle_m$ für alle $l \geq 1$ gezeigt.

QED

Bevor die explizite Formel für das Reziprozitätsgesetz angegeben und bewiesen werden kann, muss noch eine Bezeichnung eingeführt werden. Es sei

$$K_n' := \bigcap_{m \geq n} N_{mn}(K_m^*) \tag{5.17}$$

die Menge der universellen Normen von K_n.

Lemma 5.23 *Für $m \geq n$ gilt $K_n' = N_{mn}(K_m')$.*

Beweis: Aufgrund der Kompositionsformel für die Normabbildung gilt für $m \geq r \geq n$, dass $N_{mn}(K_m^*) \subseteq N_{rn}(K_r^*)$ und folglich $\bigcap_{r=n}^m N_{rn}(K_r^*) = N_{mn}(K_m^*)$. Daraus folgt

$$\begin{aligned} K_n' = \bigcap_{r \geq n} N_{rn}(K_r^*) &= \bigcap_{r=n}^{m} N_{rn}(K_r^*) \cap \bigcap_{r>m} N_{rn}(K_r^*) \\ &= N_{mn}(K_m^*) \cap \bigcap_{r>m} N_{rn}(K_r^*) \\ &= \bigcap_{r \geq m} N_{rn}(K_r^*) = \bigcap_{r \geq m} N_{mn}\big(N_{rm}(K_r^*)\big) \\ &= N_{mn}\Big(\bigcap_{r \geq m} N_{rm}(K_r^*) \Big) = N_{mn}(K_m'). \end{aligned}$$

QED

Somit existiert für jedes $\alpha \in K_n'$ und jedes $m \geq n$ ein $\alpha_m \in K_m'$ mit $\alpha = N_{mn}(\alpha_m)$.

Theorem 5.24 (Explizites Reziprozitätsgesetz) *Für $\alpha \in K_n'$ sei $\alpha_m \in K_m'$ mit $N_{mn}(\alpha_m) = \alpha$. Mit $\beta \in (1 + \mathfrak{m}_n)$ gilt*

$$[\alpha, \beta]_n = \langle \alpha_m, \beta \rangle_m \quad \text{für alle} \quad m \geq 2n+1.$$

Explizit lautet die Behauptung

$$(\alpha, \beta)_n = \zeta_n^{-\frac{1}{p^{m+1}} S_m\left(\delta_m(\alpha_m) \log \beta\right)},$$

wobei $\delta_m(\alpha_m) = \frac{\zeta_m}{\alpha_m} f'(\pi_m)$ mit einer Potenzreihe $f \in \mathbb{Z}_p[[T]]$ für α_m ist.

BEWEIS: Seien $l \geq m \geq 2n+1$, $l \geq 3n+1$ und $\alpha_l \in K_l'$, $\alpha_m \in K_m'$ mit $N_{lm}(\alpha_l) = \alpha_m$ und $N_{mn}(\alpha_m) = \alpha$. Dann gilt nach Satz 5.22

$$[\alpha, \beta]_n = \langle \alpha_l, \beta \rangle_l,$$

und nach Satz 5.15

$$\langle \alpha_m, \beta \rangle_m \equiv \langle \alpha_l, \beta \rangle_l \mod p^{n+1}.$$

Da $[\alpha, \beta]_n$ nur modulo p^{n+1} bestimmt ist, erhält man die Gleichheit

$$[\alpha, \beta]_n = \langle \alpha_m, \beta \rangle_m.$$

QED

Wählt man $\alpha = \zeta_n$ so ist nach Lemma 4.7 $\alpha_m = \zeta_m$ ein Urbild von ζ_n unter der Normabbildung N_{mn}. Nach Gleichung (5.7) von Seite 53 gilt $\delta_m(\zeta_m) = -1$. Damit folgt für $m \geq 2n+1$

$$(\zeta_n, \beta)_n = \zeta_n^{-\frac{1}{p^{m+1}} S_m(-\log \beta)}.$$

Wegen $\log \beta \in K_n$ ist $S_m(\log \beta) = p^{m-n} S_n(\log \beta)$ und es gilt

$$(\zeta_n, \beta)_n = \zeta_n^{\frac{1}{p^{n+1}} S_n(\log \beta)}.$$

Dies ist die Aussage des ersten Ergänzungssatzes von Artin-Hasse (vgl. Theorem 5.2).

Das Element $\alpha_m = \pi_m$ ist aufgrund von $N_{mn}(\pi_m) = \pi_n$ ein Urbild von $\alpha = \pi_n$. Mit Gleichung (5.8) von Seite 53 erhält man $\delta_m(\pi_m) = \frac{\zeta_m}{\pi_m}$. Damit folgt für $m \geq 2n+1$

$$(\pi_n, \beta)_n = \zeta_n^{-\frac{1}{p^{m+1}} S_m\left(\frac{\zeta_m}{\pi_m} \log \beta\right)}.$$

Da $S_{mn}\left(\frac{\zeta_m}{\pi_m}\right) = p^{m-n} \frac{\zeta_n}{\pi_n}$ gilt (vgl. Beweis zu Satz 5.12) und $\log \beta \in K_n$ ist, kann man die Argumentation fortsetzen,

$$(\pi_n, \beta)_n = \zeta_n^{-\frac{1}{p^{n+1}} S_n\left(\frac{\zeta_n}{\pi_n} \log \beta\right)}.$$

Dies ist gerade der zweite Ergänzungssatz von Artin-Hasse (vgl. Theorem 5.2).

In seinem Artikel [Kudo] beweist A. Kudo für den Fall $p = 2$ die Formel

$$(\alpha, \beta)_n = \zeta_n^{-\frac{1}{2^{m+1}} S_m\left(\delta_m(\alpha_m) \log \beta\right)}$$

für das 2^{n+1}-te Hilbertsymbol im Körper $\mathbb{Q}_2(\zeta_n)$. Der Beweis verläuft analog zu dem hier vorgestellten Beweis von K. Iwasawa.

5.3 Weitere Resultate

In diesem Abschnitt werden einige weiterführende Aussagen aus dem Artikel [Iwa2] von K. Iwasawa zusammengetragen. Insbesondere geht es um einen Homomorphismus ψ_n, für den $[\alpha,\beta]_n = S_n\big(\psi_n(\alpha)\log\beta\big)$ gilt. Diesen Homomorphismus unter den Charakteren der Galoisgruppe zu zerlegen, ist das Ziel von Kapitel 6.

Für die Ausführungen in diesem Abschnitt wurde der Artikel [Iwa1] von K. Iwasawa herangezogen.

Sei

$$\mathfrak{X}_n := \big\{x \in K_n : S_n\big(x\log(1+\mathfrak{m}_n)\big) \equiv 0 \mod \mathbb{Z}_p\big\}. \tag{5.18}$$

Dies ist eine Untergruppe der additiven Gruppe K_n. Nach [Iwa1], § 3, Proposition 14, gilt der folgende Satz.

Satz 5.25 *Für alle $n \geq 0$ existiert genau ein Homomorphismus*

$$\psi_n : K_n' \to \mathfrak{X}_n/p^{n+1}\mathfrak{X}_n,$$

so dass für alle $\alpha \in K_n'$ und $\beta \in (1+\mathfrak{m}_n)$ die Gleichung

$$(\alpha,\beta)_n = \zeta_n^{S_n(\psi_n(\alpha)\log\beta)}$$

erfüllt ist. Dieser Homomorphismus ψ_n ist surjektiv.

Die im nachstehenden Theorem angegebene explizite Vorschrift für ψ_n findet sich bei [Iwa2], Theorem 3.

Theorem 5.26 *Der Homomorphismus ψ_n aus Satz 5.25 ist für $m \geq 2n+1$ durch die Vorschrift*

$$\psi_n(x) = -\frac{1}{p^{m+1}}\, S_{mn}\big(\delta_m(x_m)\big), \qquad x \in K_n'$$

gegeben. Dabei ist $x_m \in K_m'$ ein Element mit $N_{mn}(x_m) = x$ und δ_m ist die Abbildung aus Definition 5.8 .

Lemma 5.27 *Der Homomorphismus ψ_n aus Theorem 5.26 hat die Eigenschaft*

$$\psi_n\big(\sigma(x)\big) = \kappa(\sigma)\sigma\big(\psi_n(x)\big),$$

wobei $x \in K_n'$, $\sigma \in G(K_n/\mathbb{Q}_p)$ und $\kappa(\sigma)$ die eindeutig bestimmte p-adische Einheit aus Lemma 5.10 ist.

BEWEIS: Sei $\sigma \in G(K_n/\mathbb{Q}_p)$. Für $x \in K_n'$ sei $x_m \in K_m^*$ ein Element für das $N_{mn}(x_m) = x$ gilt. Betrachtet man die Elemente $\tau \in G(K_m/K_n)$ und $\sigma \in G(K_n/\mathbb{Q}_p)$ mit Hilfe der exakten Sequenz

$$1 \to G(K_m/K_n) \to G(K_m/\mathbb{Q}_p) \to G(K_n/\mathbb{Q}_p) \to 1$$

als Elemente von $G(K_m/\mathbb{Q}_p)$, so gilt aufgrund der Kommutativität von $G(K_m/\mathbb{Q}_p)$

$$\sigma(x) = \sigma\big(N_{mn}(x_m)\big) = \sigma\Big(\prod_\tau \tau(x_m)\Big) = \prod_\tau \tau\big(\sigma(x_m)\big) = N_{mn}\big(\sigma(x_m)\big).$$

Somit ist $\sigma(x_m)$ ein Normurbild von $\sigma(x)$. Nach Satz 5.11, Teil (ii), gilt

$$\delta_m\big(\sigma(x_m)\big) \equiv \kappa(\sigma)\sigma\big(\delta_m(x_m)\big) \mod \mathfrak{D}_m. \tag{5.19}$$

Da man σ auch mit der Spurabbildung S_{mn} vertauschen kann, folgt

$$\psi_n\big(\sigma(x)\big) = -\frac{1}{p^{m+1}}\kappa(\sigma)\sigma\big(S_{mn}(\delta_m(x_m))\big) = \kappa(\sigma)\sigma\big(\psi_n(x)\big).$$

In Gleichung (5.19) gilt eine Äquivalenz modulo $\mathfrak{D}_m$. Demnach muss noch die Relation

$$-\frac{1}{p^{m+1}}S_{mn}(\mathfrak{D}_m) \subseteq p^{n+1}\mathfrak{X}_n \quad \text{für} \quad m \geq 2n+1$$

nachgewiesen werden. Aus der Definition von $\mathfrak{X}_n$ in Gleichung (5.18) folgt die Darstellung

$$p^{n+1}\mathfrak{X}_n = \big\{x \in K_n : S_n\big(x\log(1+\mathfrak{m}_n)\big) \equiv 0 \mod p^{n+1}\big\}.$$

Somit ist die Identität

$$S_n\Big(-\frac{1}{p^{m+1}}S_{mn}(\mathfrak{D}_m)\log(1+\mathfrak{m}_n)\Big) \equiv 0 \mod p^{n+1}$$

zu zeigen. Es gilt $S_{mn}(\mathfrak{D}_m) = p^{m+1}\pi_0^{-1}S_{mn}(\mathcal{O}_m) = p^{m-n}p^{m+1}\pi_0^{-1}\mathcal{O}_n = p^{2(m-n)}\mathfrak{D}_n$, so dass

$$\begin{aligned} S_n\big(-\frac{1}{p^{m+1}}S_{mn}(\mathfrak{D}_m)\log(1+\mathfrak{m}_n)\big) &= -\frac{1}{p^{m+1}}S_n\big(S_{mn}(\mathfrak{D}_m)\log(1+\mathfrak{m}_n)\big) \\ &= -\frac{1}{p^{m+1}}S_n\big(p^{2(m-n)}\mathfrak{D}_n\log(1+\mathfrak{m}_n)\big) \\ &= -\frac{p^{2(m-n)}}{p^{m+1}}S_n\big(\mathfrak{D}_n\log(1+\mathfrak{m}_n)\big). \end{aligned}$$

Die Gleichung $S_n(\mathfrak{D}_n\log(1+\mathfrak{m}_n)) \equiv 0 \mod p^{n+1}$ aus Satz 5.6 und die Beziehung $\frac{p^{2(m-n)}}{p^{m+1}} \in \mathbb{Z}_p$ implizieren die Behauptung.

QED

Damit man ψ_n unter den Charakteren der Galoisgruppe $G(K_n/\mathbb{Q}_p)$ zerlegen kann, ist es notwendig, die Gruppen K_n' und $\mathfrak{X}_n$ genauer zu untersuchen.

Lemma 5.28 *Für die additive Gruppe $\mathfrak{X}_n$ gilt*

$$\begin{aligned}\mathfrak{X}_n &= \left\{ \frac{1}{p^{n+1}}\,\delta_n(x),\ x \in K_n^* \right\} \\ &= \left\{ \sum_{\sigma\in G} c_\sigma \sigma(\mu_n) + \sum_{\sigma\in G} d_\sigma \sigma(\theta_n),\ c_\sigma,\, d_\sigma \in \mathbb{Z}_p,\ \sum_{\sigma\in G} d_\sigma = 0 \right\}.\end{aligned}$$

Dabei bezeichnet G die Galoisgruppe $G(K_n/\mathbb{Q}_p)$ der Erweiterung $K_n/\mathbb{Q}_p$, die Elemente μ_n und θ_n sind durch

$$\mu_n := \frac{1}{p^{n+1}}\,\frac{\zeta_n}{\pi_n} \quad \textit{und} \quad \theta_n := \frac{1}{p^{n+1}} \sum_{j=0}^{n} \zeta_j^{-1}$$

gegeben.

Die erste Charakterisierung findet sich bei [Iwa2], Theorem 4. Die zweite Darstellung ist im Prinzip durch [Iwa1], § 1, Theorem 1, gegeben, findet sich allerdings als Zusammenfassung auch auf Seite 164 von [Iwa2].

Lemma 5.29 *Für die multiplikative Gruppe K_n' gilt*

$$\begin{aligned}K_n' &= \{x \in K_n^* : N_n(x) = p^k \textit{ für ein } k \in \mathbb{Z}\} \\ &= \langle \pi_n \rangle \times \mu_{p-1} \times (1+\mathfrak{m}_n)',\end{aligned}$$

wobei $(1+\mathfrak{m}_n)' = \big\{x \in (1+\mathfrak{m}_n) : N_n(x) = 1\big\}$.

Beweis: Für die multiplikative Gruppe K_n^* gilt

$$K_n^* = \langle \pi_n \rangle \times \mu_{p-1} \times (1+\mathfrak{m}_n).$$

Für π_n ist $N_n(\pi_n) = p$, für $\xi \in \mu_{p-1}$ ist $N_n(\xi) = \xi^{(p-1)p^n} = 1$. Da die Elemente $\beta \in (1+\mathfrak{m}_n)$ teilerfremd sind zu π_n, sind auch die Normen $N_n(\beta)$ teilerfremd zu p. Zusammen mit der ersten Darstellung für K_n' folgt somit die zweite Darstellung.

Es werde nun die erste Darstellung bewiesen. Zunächst zeigt man für $x \in K_n^*$ die Gültigkeit der Äquivalenz

$$N_n(x) \in N_m(K_m^*) \Longleftrightarrow x \in N_{mn}(K_m^*).$$

Sei $L_m := K_m(\sqrt[p^{m+1}]{K_m^*})$. Dann gilt $K_n \subseteq K_m \subseteq L_m$. Nach [Neu], Kap.IV, § 6, Satz (6.4) ist das folgende Diagramm kommutativ,

$$\begin{array}{ccc} K_n^* & \xrightarrow{(\,.\,, L_m/K_n)} & G(L_m/K_n) \\ {\scriptstyle N_n}\downarrow & & \downarrow \\ \mathbb{Q}_p^* & \xrightarrow[(\,.\,, K_m/\mathbb{Q}_p)]{} & G(K_m/\mathbb{Q}_p) \end{array}$$

d.h. für $x \in K_n^*$ gilt $\big(N_n(x), K_m/\mathbb{Q}_p\big) = \big(x, L_m/K_n\big)_{|_{K_m}} = \big(x, K_m/K_n\big)$. Damit ergibt sich die gewünschte Äquivalenz

$$\begin{aligned} N_n(x) \in N_m(K_m^*) &\iff \big(N_n(x), K_m/\mathbb{Q}_p\big) = id \\ &\iff \big(x, K_m/K_n\big) = id \\ &\iff x \in N_{mn}(K_m^*). \end{aligned}$$

Mit Satz 3.9, Teil (ii), folgt nun

$$x \in K_n' \iff x \in \bigcap_{m \geq n} N_{mn}(K_m^*) \iff N_n(x) \in \bigcap_{m \geq n} N_m(K_m^*) = \{p^k, k \in \mathbb{Z}\}.$$

QED

Kapitel 6

Zerlegung unter Charakteren

In diesem Kapitel geht es darum, den in Theorem 5.26 eingeführten Homomorphismus ψ_n mit Hilfe von Charakteren der Galoisgruppe zu zerlegen.

6.1 Allgemeines

Zunächst werden einige allgemeine Aussagen über die Zerlegung von G-Moduln und von Abbildungen zwischen G-Moduln unter Charakteren angegeben.

Seien G eine endliche abelsche Gruppe, E ein Ring, der die $|G|$-ten Einheitswurzeln enthält und M ein E-Modul. Die abelsche Gruppe von M heißt G-Modul, wenn G auf ihr operiert, d.h. wenn man eine Abbildung

$$G \times M \to M, \qquad (\sigma, m) \mapsto \sigma(m)$$

hat. Ein Charakter von G ist ein Gruppenhomomorphismus

$$\chi : G \to E^*.$$

Da G endlich ist, sind die Werte von χ $|G|$-te Einheitswurzeln, d.h man hat

$$\chi : G \to \mu_{|G|}(E).$$

Die Menge der Charaktere von G bildet eine Gruppe, die Charaktergruppe $G^\times$. Man kann $G^\times$ mit $\mathrm{Hom}\big(G, \mu_{|G|}(E)\big)$ identifizieren. Nach [Lor1], § 14, F3, gilt $|G| = |G^\times|$. Für die Summe über die Werte eines Charakters gilt folgendes Lemma.

Lemma 6.1 *Es gilt*

$$\sum_{\sigma \in G} \chi(\sigma) = \begin{cases} |G| & , \chi = 1, \\ 0 & , \chi \neq 1. \end{cases}$$

Dabei bezeichnet $\chi = 1$ den Eins-Charakter, der alles auf die 1 abbildet.

BEWEIS: Für $\chi = 1$ ist die Aussage offensichtlich. Sei nun $\chi \neq 1$. Dann gibt es ein $\tau \in G$ mit $\chi(\tau) \neq 1$. Für dieses τ gilt

$$\sum_{\sigma\in G} \chi(\sigma) = \sum_{\sigma\in G} \chi(\tau\sigma) = \sum_{\sigma\in G} \chi(\tau)\chi(\sigma) = \chi(\tau) \sum_{\sigma\in G} \chi(\sigma).$$

Wegen $\chi(\tau) \neq 1$ folgt die Behauptung.

QED

An den Werte-Ring E sei die Forderung $\frac{1}{|G|} \in E$ gestellt. Dann kann man auf M einen Projektor P_χ definieren.

Definition 6.2 *Sei M ein additiver G-Modul, d.h. M ist eine additive Gruppe und E operiert durch Multiplikation. Für einen Charakter χ von G ist der Projektor P_χ gemäß*

$$P_\chi(m) := \frac{1}{|G|} \sum_{\sigma\in G} \chi(\sigma)\sigma^{-1}(m), \quad m \in M,$$

definiert.

Die Projektoren P_χ sind Gruppenhomomorphismen $P_\chi : M \to M$, man kann sie auch als Elemente von $E[G]$ auffassen. Für sie gelten folgende Aussagen.

Lemma 6.3

(i) *Für $\sigma \in G$ und $m \in M$ gilt $P_\chi\big(\sigma(m)\big) = \chi(\sigma)P_\chi(m)$.*

(ii) *Für $\sigma \in G$ und $m' = P_\chi(m)$ mit $m \in M$ gilt $\sigma(m') = \chi(\sigma)m'$.*

(iii) *Für Projektoren P_χ und $P_{\chi'}$ gilt*

$$P_\chi \circ P_{\chi'} = \begin{cases} P_\chi, & \text{falls } \chi = \chi', \\ 0, & \text{falls } \chi \neq \chi'. \end{cases}$$

BEWEIS von (i): Mit Hilfe der Variablensubstitution $\rho^{-1} = \tau^{-1}\sigma$ gilt

$$\begin{aligned} P_\chi\big(\sigma(m)\big) &= \frac{1}{|G|} \sum_{\tau\in G} \chi(\tau)\tau^{-1}\big(\sigma(m)\big) \\ &= \frac{1}{|G|} \sum_{\rho\in G} \chi(\sigma\rho)\rho^{-1}(m) \\ &= \frac{\chi(\sigma)}{|G|} \sum_{\rho\in G} \chi(\rho)\rho^{-1}(m) = \chi(\sigma)P_\chi(m). \end{aligned}$$

BEWEIS von (ii): Aus der Definition von P_χ und der Kommutativität von G folgt $\sigma\big(P_\chi(m)\big) = P_\chi\big(\sigma(m)\big)$. Somit ist (ii) eine direkte Konsequenz aus (i).

BEWEIS von (iii): Unter Verwendung von Teil (i), der Eigenschaft $\chi(\sigma^{-1}) = \chi^{-1}(\sigma)$ für Charaktere und Lemma 6.1 folgt

$$\begin{aligned} P_\chi\big(P_{\chi'}(m)\big) = P_\chi\Big(\frac{1}{|G|}\sum_{\sigma\in G}\chi'(\sigma)\sigma^{-1}(m)\Big) &= \frac{1}{|G|}\sum_{\sigma\in G}\chi'(\sigma)P_\chi\big(\sigma^{-1}(m)\big) \\ = \frac{1}{|G|}\sum_{\sigma\in G}\chi'(\sigma)\chi(\sigma^{-1})P_\chi(m) &= \frac{P_\chi(m)}{|G|}\sum_{\sigma\in G}\chi'(\sigma)\chi^{-1}(\sigma) \\ = \begin{cases} P_\chi(m), & \text{falls } \chi' = \chi, \\ 0, & \text{falls } \chi' \neq \chi. \end{cases} & \end{aligned}$$

QED

Man hat somit eine Zerlegung

$$M = \bigoplus_{\chi\in G^\times} M(\chi)$$

von M in Eigenräume $M(\chi) := P_\chi(M)$. Man sagt, M wurde unter den Charakteren von G zerlegt. Nach Lemma 6.3, Teil (ii), operiert G auf den Eigenräumen durch Multiplikation mit der jeweiligen Einheitswurzel $\chi(\sigma)$.
Insbesondere folgt für $m \in M$ aus $P_\chi(m) = m$ oder $\sigma(m) = \chi(\sigma)m$ für alle $\sigma \in G$, dass $m \in M(\chi)$.

Ist N ein multiplikativer G-Modul, d.h. N ist eine multiplikative Gruppe und E operiert durch Potenzierung, so kann man für einen Charakter χ von G den Projektor $\widetilde{P}_\chi$,

$$\widetilde{P}_\chi(n) := \Big(\prod_{\sigma\in G}\big(\sigma^{-1}(n)\big)^{\chi(\sigma)}\Big)^{\frac{1}{|G|}}, \quad n \in N,$$

definieren. Diese Projektoren haben Eigenschaften, die zu den Eigenschaften der Projektoren P_χ in Lemma 6.3 analog sind. Somit erhält man auch für N eine Zerlegung in Eigenräume

$$N = \prod_{\chi\in G^\times} N(\chi).$$

Auf den Eigenräumen $N(\chi) := \widetilde{P}_\chi(N)$ operiert G durch Potenzierung mit der jeweiligen Einheitswurzel $\chi(\sigma)$.

Hat man schließlich einen Gruppenhomomorphismus

$$f : M \to N$$

zwischen (additiven oder multiplikativen) G-Moduln M und N, auf denen Projektoren P_χ oder $\widetilde{P}_\chi$ definiert sind, so kann man die durch f induzierten Abbildungen

$$f(\chi) : M(\chi) \to N(\chi'), \quad \chi,\ \chi' \in G^\times,$$

betrachten, in denen die Charaktere χ und χ' verschieden sein können. Man sagt, f wurde unter Charakteren zerlegt.

6.2 Der Spezialfall $n = 0$

In diesem Abschnitt geht es darum, den eindeutig bestimmten Homomorphismus ψ_n im Spezialfall $n = 0$ genauer zu untersuchen. Es seien $K_0 = \mathbb{Q}_p(\zeta_0)$ mit einer primitiven p-ten Einheitswurzel ζ_0 und $G := G(K_0/\mathbb{Q}_p)$. Der Bewertungsring von K_0 und sein maximales Ideal seien, wie im letzten Kapitel, mit $\mathcal{O}_0$ bzw. $\mathfrak{m}_0$ bezeichnet. Das Primelement ist weiterhin $\pi_0 = 1 - \zeta_0$.

Die in Theorem 5.26 angegebene Abbildung ist

$$\psi_0 : K_0' \to \mathfrak{X}_0/p\,\mathfrak{X}_0, \qquad x \mapsto -\frac{1}{p^{m+1}}\, S_{m0}\big(\delta_m(x_m)\big),\ m \geq 1.$$

Das weitere Vorgehen ergibt sich folgendermaßen. Zunächst werden die Gruppe G und ihre Charaktergruppe $G^\times$ untersucht. Beim Versuch, die Projektoren P_χ und $\widetilde{P}_\chi$ auf den Gruppen $\mathfrak{X}_0/p\mathfrak{X}_0$ und K_0' zu definieren, zeigt es sich, dass man von K_0' erst zur Komplettierung X_0 übergehen muss, bevor man die Projektoren $\widetilde{P}_\chi$ anwenden kann. Schließlich werden die Eigenräume der Gruppen $\mathfrak{X}_0/p\mathfrak{X}_0$ und X_0 bestimmt und die Abbildungen $\psi_0(\chi)$ auf den Eigenräumen untersucht.

Lemma 6.4 *Es gilt $G = G(K_0/\mathbb{Q}_p) = \big(\mathbb{Z}/p\mathbb{Z}\big)^*$. Insbesondere ist $|G^\times| = p - 1$.*

Beweis: Ein Element der Galoisgruppe $G(K_0/\mathbb{Q}_p)$ ist durch seine Wirkung auf ζ_0 eindeutig festgelegt. Jedes $a \in (\mathbb{Z}/p\,\mathbb{Z})^*$ definiert durch $\zeta_0 \mapsto \zeta_0^a$ einen Automorphismus $\sigma_a \in G(K_0/\mathbb{Q}_p)$. Somit gilt $(\mathbb{Z}/p\mathbb{Z})^* \subseteq G(K_0/\mathbb{Q}_p)$. Wegen $\big|(\mathbb{Z}/p\mathbb{Z})^*\big| = p - 1$ und $|G(K_0/\mathbb{Q}_p)| = [K_0 : \mathbb{Q}_p] = p - 1$ (vgl. Satz 2.1) folgt die Gleichheit $(\mathbb{Z}/p\mathbb{Z})^* = G(K_0/\mathbb{Q}_p)$.

QED

Die Werte $\chi(\sigma)$ der Charaktere $\chi \in G^\times$ sind $(p-1)$-te Einheitswurzeln, nach Satz 2.1 sind diese in $\mathbb{Q}_p$ enthalten. Sei $\xi \in \mathbb{Q}_p$ eine $(p-1)$-te Einheitswurzel. Dann gilt

$$0 = v_p(1) = v_p(\xi^{p-1}) = (p-1)v_p(\xi),$$

also $v_p(\xi) = 0$. Deshalb sind die $(p-1)$-ten Einheitswurzeln bereits in $\mathbb{Z}_p$ enthalten, und man kann die Charaktere von G als Homomorphismen

$$\chi : G(K_0/\mathbb{Q}_p) \to \mathbb{Z}_p$$

betrachten.

Die $(p-1)$-ten Einheitswurzeln sind, modulo p betrachtet, paarweise verschieden, denn die Gleichung

$$X^{p-1} - 1 = 0$$

hat $p-1$ verschiedene Lösungen in $\mathbb{F}_p$.

Definition 6.5 *Der Teichmüller-Charakter ist der Homomorphismus*

$$\omega : \big(\mathbb{Z}/p\,\mathbb{Z}\big)^* \to \mu_{p-1} \subseteq \mathbb{Z}_p,$$

der durch $\omega(a) \equiv a \mod p$ *charakterisiert ist.*

Der Teichmüller-Charakter hat die Ordnung $p-1$, ist also ein erzeugendes Element der Charaktergruppe,

$$G^\times = \{\omega^k,\ k = 0, 1, \ldots, p-2\}.$$

Ausgehend von der Definition 5.18 und Lemma 5.28 erhält man für $\mathfrak{X}_0$ die Charakterisierungen

$$\begin{aligned}
\mathfrak{X}_0 &= \Big\{ x \in K_0 : S_0\big(x \log(1+\mathfrak{m}_0)\big) \equiv 0 \mod \mathbb{Z}_p \Big\} \\
&= \Big\{ \frac{1}{p}\,\delta_0(x),\ x \in K_0^* \Big\} \qquad (6.1) \\
&= \Big\{ \sum_{\sigma\in G} c_\sigma \sigma(\mu_0) + \sum_{\sigma\in G} d_\sigma \sigma(\theta_0),\ c_\sigma,\, d_\sigma \in \mathbb{Z}_p,\ \sum_{\sigma\in G} d_\sigma = 0 \Big\}.
\end{aligned}$$

Hier ist $G = G(K_0/\mathbb{Q}_p)$ und

$$\mu_0 = \frac{1}{p}\,\frac{\zeta_0}{\pi_0}, \qquad \theta_0 = \frac{1}{p}\,\zeta_0^{-1}. \qquad (6.2)$$

Lemma 6.6 *Die additive Gruppe* $\mathfrak{X}_0/p\,\mathfrak{X}_0$ *ist ein* G*-Modul.*

Beweis: Seien $\tau \in G$ und $x = \sum_{\sigma\in G} c_\sigma \sigma(\mu_0) + \sum_{\sigma\in G} d_\sigma \sigma(\theta_0) \in \mathfrak{X}_0$. Dann gilt

$$\tau(x) = \sum_{\sigma\in G} c_\sigma \tau(\sigma(\mu_0)) + \sum_{\sigma\in G} d_\sigma \tau(\sigma(\theta_0)) = \sum_{\rho\in G} c_{\tau^{-1}\rho}\rho(\mu_0) + \sum_{\rho\in G} d_{\tau^{-1}\rho}\rho(\theta_0).$$

Wegen $\sum_{\rho\in G} d_{\tau^{-1}\rho} = \sum_{\sigma\in G} d_\sigma = 0$ ist $\tau(x)$ ein Element von $\mathfrak{X}_0$. Somit operiert G auf $\mathfrak{X}_0$. Mit einer analogen Rechnung kann man zeigen, dass G auch auf $p\,\mathfrak{X}_0$ operiert. Außerdem kann kein Element x aus $\mathfrak{X}_0$, das kein Vielfaches von p ist, durch ein $\sigma \in G$ nach $p\,\mathfrak{X}_0$ abgebildet werden. Wäre dies der Fall, so ergäbe sich die Relation

$$x = \sigma^{-1}\sigma(x) \in \sigma^{-1}(p\,\mathfrak{X}_0) \subseteq p\,\mathfrak{X}_0.$$

Das ist ein Widerspruch. Somit operiert G auch auf dem Quotienten $\mathfrak{X}_0/p\,\mathfrak{X}_0$.

QED

Lemma 6.7 *Die multiplikative Gruppe K_0' ist ein G-Modul.*

BEWEIS: Nach Lemma 5.29 besteht K_0' aus denjenigen Elementen $x \in K_0^*$, für die $N_0(x)$ eine p-Potenz ist. Da für $\sigma \in G$ die Gleichung $N_0\big(\sigma(x)\big) = N_0(x)$ gilt, ist gezeigt, dass $\sigma(x) \in K_0'$, dass also G auf K_0' operiert.

QED

Für $\chi \in G^\times$ ergeben sich die Projektoren P_χ zu

$$P_\chi = \frac{1}{p-1}\sum_{\sigma\in G} \chi(\sigma)\sigma^{-1}.$$

Wegen $\frac{1}{p-1} = -\sum_{k\geq 0} p^k \in \mathbb{Z}_p$ ist $P_\chi \in \mathbb{Z}_p[G]$. Da in $\mathfrak{X}_0$ die Multiplikation mit Elementen aus $\mathbb{Z}_p$ erklärt ist, ist die Anwendung von P_χ auf $\mathfrak{X}_0$ definiert.

Lemma 6.8 *Es gilt $(\mathfrak{X}_0/p\,\mathfrak{X}_0)(\chi) = \mathfrak{X}_0(\chi)/p\,\mathfrak{X}_0(\chi)$.*

BEWEIS: Sei $x \in \mathfrak{X}_0$. Die Restklasse von x in $\mathfrak{X}_0/p\mathfrak{X}_0$ werde als $x+p\mathfrak{X}_0$ geschrieben. Dann gilt

$$P_\chi(x + p\,\mathfrak{X}_0) = P_\chi(x) + pP_\chi(\mathfrak{X}_0)$$

und die Behauptung ist bewiesen.

QED

Nach den soeben gewonnenen Ergebnissen genügt es vorerst, die Eigenräume von $\mathfrak{X}_0$ zu bestimmen.

Lemma 6.9 *In $\mathfrak{X}_0$ besteht zwischen μ_0 und θ_0 die Beziehung*

$$\mu_0 = \frac{1}{p}\sum_{a=1}^{p-1} a\sigma_a(\theta_0),$$

wobei mit σ_a der Automorphismus $\sigma_a : \zeta_0 \mapsto \zeta_0^a$ bezeichnet ist.

BEWEIS: Ausgehend von Gleichung (6.2) ist zu zeigen, dass

$$\frac{\zeta_0}{\pi_0} = \frac{1}{p}\sum_{a=1}^{p-1} a\zeta_0^{-a} \quad \text{bzw.} \quad \zeta_0 = \frac{\pi_0}{p}\sum_{a=1}^{p-1} a\zeta_0^{-a} = \frac{1}{p}\sum_{a=1}^{p-1} a(1-\zeta_0)\zeta_0^{-a}.$$

Die Summe auf der rechten Seite der zweiten Gleichung läßt sich unter Verwendung der Variablensubstitution $-b = 1-a$ und von $S_0(\zeta_0) = -1$ (vgl. Lemma 4.7) zu

$$\begin{aligned}
\sum_{a=1}^{p-1} a(1-\zeta_0)\zeta_0^{-a} &= \sum_{a=1}^{p-1} a\zeta_0^{-a} - \sum_{a=1}^{p-1} a\zeta_0^{1-a} = \sum_{a=1}^{p-1} a\zeta_0^{-a} - \sum_{b=0}^{p-2}(1+b)\zeta_0^{-b} \\
&= \sum_{a=1}^{p-2} a\zeta_0^{-a} + (p-1)\zeta_0^{-(p-1)} - \sum_{b=1}^{p-2} b\zeta_0^{-b} - \sum_{b=0}^{p-2}\zeta_0^{-b} \\
&= (p-1)\zeta_0 - \zeta_0\sum_{b=1}^{p-1}\zeta_0^{-b} = (p-1)\zeta_0 - \zeta_0 S_0(\zeta_0) \\
&= (p-1)\zeta_0 + \zeta_0 = p\,\zeta_0
\end{aligned}$$

umformen. Damit ist das Lemma bewiesen.

QED

Satz 6.10 *Für die Eigenräume von $\mathfrak{X}_0$ gilt*

$$P_\chi(\mathfrak{X}_0) = \left\{ \begin{array}{ll} \frac{1}{p}\,\mathbb{Z}_p, & \textit{für } \chi = 1 \\ \frac{1}{p}\,\mathbb{Z}_p P_\chi(\theta_0), & \textit{für } \chi = \omega^{-1} \\ \mathbb{Z}_p P_\chi(\theta_0), & \textit{sonst} \end{array} \right\} = \left\{ \begin{array}{ll} \frac{1}{p}\,\mathbb{Z}_p, & \textit{für } \chi = 1 \\ \mathbb{Z}_p P_\chi(\mu_0), & \textit{für } \chi = \omega^{-1} \\ \mathbb{Z}_p P_\chi(\theta_0), & \textit{sonst} \end{array} \right\}.$$

BEWEIS: Sei $\chi \in G^\times$. Aus

$$P_\chi(\mu_0) = \frac{1}{p-1}\sum_{\sigma\in G}\chi(\sigma)\sigma^{-1}(\mu_0) = \sum_{\sigma\in G}\frac{\chi(\sigma^{-1})}{p-1}\,\sigma(\mu_0)$$

und

$$P_\chi(\theta_0) = \sum_{\sigma\in G}\frac{\chi(\sigma^{-1})}{p-1}\,\sigma(\theta_0)$$

folgt zusammen mit Lemma 6.1 über die Summe der Werte eines Charakters und der Charakterisierung von $\mathfrak{X}_0$ in Gleichung (6.1) vor Lemma 6.6, dass

$$P_\chi(\mu_0) \in \mathfrak{X}_0 \quad \text{für alle } \chi \in G^\times$$

und

$$P_\chi(\theta_0) \in \mathfrak{X}_0 \quad \text{für } \chi \neq 1.$$

Über die Zugehörigkeit von $P_1(\theta_0)$ zu $\mathfrak{X}_0$ kann zunächst keine Aussage gemacht werden.

Seien $\chi \in G^\times$ und $x = \sum_{\sigma\in G} c_\sigma \sigma(\mu_0) + \sum_{\sigma\in G} d_\sigma \sigma(\theta_0) \in \mathfrak{X}_0$. Dann gilt unter Verwendung von Lemma 6.3

$$\begin{aligned} P_\chi(x) &= \sum_{\sigma\in G} c_\sigma P_\chi\big(\sigma(\mu_0)\big) + \sum_{\sigma\in G} d_\sigma P_\chi\big(\sigma(\theta_0)\big) \\ &= \Big(\sum_{\sigma\in G} c_\sigma \chi(\sigma)\Big) P_\chi(\mu_0) + \Big(\sum_{\sigma\in G} d_\sigma \chi(\sigma)\Big) P_\chi(\theta_0). \end{aligned} \tag{6.3}$$

Zunächst werden die Eigenräume $P_\chi(\mathfrak{X}_0)$ für $\chi \neq 1$ bestimmt. Die beiden Vorfaktoren vor $P_\chi(\mu_0)$ und $P_\chi(\theta_0)$ sind aus $\mathbb{Z}_p$. Daraus und aus den Vorbemerkungen folgt

$$P_\chi(\mathfrak{X}_0) \ \subseteq \ \mathbb{Z}_p P_\chi(\mu_0) + \mathbb{Z}_p P_\chi(\theta_0) \ \subseteq \ \mathfrak{X}_0.$$

Andererseits liegt jedes Element $cP_\chi(\mu_0) + dP_\chi(\theta_0)$ mit $c, d \in \mathbb{Z}_p$ in $P_\chi(\mathfrak{X}_0)$, denn für $\chi' \neq \chi$ gilt, ebenfalls nach Lemma 6.3,

$$P_{\chi'}\big(cP_\chi(\mu_0) + dP_\chi(\theta_0)\big) = cP_{\chi'}\big(P_\chi(\mu_0)\big) + dP_{\chi'}\big(P_\chi(\theta_0)\big) = 0.$$

Man hat also

$$P_\chi(\mathfrak{X}_0) = \mathbb{Z}_p P_\chi(\mu_0) + \mathbb{Z}_p P_\chi(\theta_0).$$

Wegen Lemma 6.9 sind $P_\chi(\mu_0)$ und $P_\chi(\theta_0)$ jedoch nicht $\mathbb{Z}_p$-linear unabhängig, sondern es gilt

$$P_\chi(\mu_0) = \frac{1}{p}\sum_{a=1}^{p-1} aP_\chi\big(\sigma_a(\theta_0)\big) = \frac{1}{p}\Big(\sum_{a=1}^{p-1} a\chi(\sigma_a)\Big) P_\chi(\theta_0).$$

Der Faktor $\sum_{a=1}^{p-1} a\chi(\sigma_a)$ wird für $\chi = \omega^{k-1},\ k = 2, \ldots, p-1$, modulo p betrachtet,

$$\sum_{a=1}^{p-1} a\chi(\sigma_a) = \sum_{a=1}^{p-1} a\omega^{k-1}(a) \equiv \sum_{a=1}^{p-1} a^k \mod p.$$

Für $k = p-1$, also $\chi = \omega^{-1}$, gilt $a^{p-1} \equiv 1 \mod p$, also

$$\sum_{a=1}^{p-1} a\omega^{-1}(\sigma_a) \equiv \sum_{a=1}^{p-1} a^{p-1} \equiv p-1.$$

Im Fall $k < p-1$ ist die Summe $\sum_{a=1}^{p-1} a^k \equiv \sum_{a=1}^{p} a^k \mod p$ zu betrachten. Allgemein gilt nach [TTB], Kap. 0.1.10.4,

$$\sum_{a=1}^{n} a^k = \frac{n^{k+1}}{k+1} + \frac{n^k}{2} + \frac{B_2}{2}\binom{k}{1} n^{k-1} + \frac{B_3}{3}\binom{k}{2} n^{k-2} + \ldots + \frac{B_k}{k}\binom{k}{k-1} n, \tag{6.4}$$

mit der Bezeichnung B_j für die j-te Bernoulli-Zahl. Nach [Was], Chap. 5, § 5.2, Theorem 5.10, enthält B_j im Nenner keinen Faktor p, wenn $(p-1) \nmid j$. Wegen

$k < p-1$ tritt also in keinem der B_j in obiger Formel (6.4) ein Faktor p im Nenner auf. Setzt man in Gleichung (6.4) $n = p$ ein, so folgt

$$\sum_{a=1}^{p-1} a\chi(\sigma_a) \equiv \sum_{a=1}^{p} a^k \equiv 0 \mod p.$$

Insgesamt ergibt sich somit

$$\sum_{a=1}^{p-1} a\chi(\sigma_a) \in \begin{cases} \mathbb{Z}_p, & \text{für } \chi = \omega^{-1}, \\ p\,\mathbb{Z}_p, & \text{für } \chi \neq 1, \omega^{-1}, \end{cases}$$

bzw.

$$\frac{1}{p}\sum_{a=1}^{p-1} a\chi(\sigma_a) \in \begin{cases} \frac{1}{p}\mathbb{Z}_p, & \text{für } \chi = \omega^{-1}, \\ \mathbb{Z}_p, & \text{für } \chi \neq 1, \omega^{-1}. \end{cases}$$

Im Fall $\chi = \omega^{-1}$ ist demnach $c := \frac{1}{p}\sum_{a=1}^{p-1} a\chi(\sigma_a) \notin \mathbb{Z}_p$. Dann gilt jedoch $c^{-1} \in \mathbb{Z}_p$, so dass man $P_\chi(\theta_0) = c^{-1}P_\chi(\mu_0) \in \mathbb{Z}_p P_\chi(\mu_0)$ erhält. Abschließend ergibt sich für die Struktur der Eigenräume,

$$P_\chi(\mathfrak{X}_0) = \left\{ \begin{array}{ll} \frac{1}{p}\mathbb{Z}_p P_\chi(\theta_0), & \text{für } \chi = \omega^{-1} \\ \mathbb{Z}_p P_\chi(\theta_0), & \text{für } \chi \neq 1, \omega^{-1} \end{array} \right\} = \left\{ \begin{array}{ll} \mathbb{Z}_p P_\chi(\mu_0), & \text{für } \chi = \omega^{-1} \\ \mathbb{Z}_p P_\chi(\theta_0), & \text{für } \chi \neq 1, \omega^{-1} \end{array} \right\}.$$

Zuletzt muss noch der Eigenraum $P_1(\mathfrak{X}_0)$ bestimmt werden. Der Vorfaktor vor $P_\chi(\theta_0)$ in Gleichung (6.3) ergibt sich zu $\sum_\sigma d_\sigma \chi(\sigma) = \sum_\sigma d_\sigma = 0$, so dass man aus Gleichung (6.3) die Gleichung

$$P_1(x) = \sum_{\sigma \in G} c_\sigma P_1(\mu_0)$$

erhält. Daraus folgt $P_1(\mathfrak{X}_0) \subseteq \mathbb{Z}_p P_1(\mu_0) \subseteq \mathfrak{X}_0$ und mit derselben Argumentation wie oben kann man

$$P_1(\mathfrak{X}_0) = \mathbb{Z}_p P_1(\mu_0)$$

schlussfolgern. Zur Berechnung von $P_1(\mu_0)$ sei an Lemma 6.9 und an Gleichung $S_0(\zeta_0^{-1}) = -1$ aus Lemma 4.8 erinnert.

$$\begin{aligned} P_1(\mu_0) &= \frac{1}{p-1} S_0(\mu_0) = \frac{1}{p\,(p-1)} S_0\Big(\sum_{a=1}^{p-1} a\sigma_a(\theta_0)\Big) \\ &= \frac{1}{p^2(p-1)} \sum_{a=1}^{p-1} a S_0(\zeta_0^{-1}) = -\frac{1}{2p} \end{aligned}$$

Damit erhält man den Eigenraum

$$P_1(\mathfrak{X}_0) = \frac{1}{p}\,\mathbb{Z}_p.$$

Der Vollständigkeit halber sei noch erwähnt, dass auch $P_1(\theta_0) \in \mathfrak{X}_0$, denn es gilt

$$\begin{aligned} P_1(\theta_0) = \frac{1}{p-1}\, S_0(\theta_0) \;&=\; \frac{1}{p\,(p-1)}\, S_0(\zeta_0^{-1}) \\ = -\frac{1}{p\,(p-1)} \;&=\; \frac{2}{p-1} P_1(\mu_0) \qquad \in\; \mathfrak{X}_0. \end{aligned}$$

QED

Die Gruppe $\mathfrak{X}_0$ wurde somit in $p-1$ Eigenräume von $\mathbb{Z}_p$-Rang 1 zerlegt. Die Zerlegung $\mathfrak{X}_0 = \bigoplus \mathfrak{X}_0(\chi)$ impliziert

$$\operatorname{rk}_{\mathbb{Z}_p} \mathfrak{X}_0 = \sum_{\chi \in G^\times} \operatorname{rk}_{\mathbb{Z}_p} \mathfrak{X}_0(\chi) = p-1.$$

Die Eigenräume der Faktorgruppe $\mathfrak{X}_0/p\,\mathfrak{X}_0$ ergeben sich zu

$$(\mathfrak{X}_0/p\,\mathfrak{X}_0)(\chi) = \begin{cases} \frac{1}{p}\,\mathbb{F}_p, & \text{für } \chi = 1, \\ \mathbb{F}_p P_\chi(\mu_0), & \text{für } \chi = \omega^{-1}, \\ \mathbb{F}_p P_\chi(\theta_0), & \text{sonst.} \end{cases} \tag{6.5}$$

Damit ist die Zerlegung von $\mathfrak{X}_0/p\,\mathfrak{X}_0$ angegeben. Nun wird es um die Zerlegung von K_0' gehen.

Die Projektoren $\widetilde{P}_\chi$ sind gemäß

$$\widetilde{P}_\chi = \Big(\prod_{\sigma \in G} (\sigma^{-1})^{\chi(\sigma)} \Big)^{\frac{1}{p-1}}$$

definiert. Allerdings können sie nicht auf Elemente aus K_0' angewandt werden, da in K_0' die Potenzierung mit Zahlen aus $\mathbb{Z}_p$ nicht definiert ist. Der Lösung dieses Problems widmen sich die nächsten Überlegungen.

Die Gruppen $K_0'/K_0'^{p^r}$, $r \geq 1$, bilden bezüglich der natürlichen Projektionen

$$K_0'/K_0'^{p^r} \to K_0'/K_0'^{p^s}, \quad r \geq s,$$

ein projektives System. Sei $X_0 := \varprojlim_r K_0'/K_0'^{p^r}$ der Limes dieses Systems. Dann gilt der folgende Satz.

Satz 6.11 *Der projektive Limes X_0 besitzt die Darstellung*

$$X_0 = \langle\langle \pi_0 \rangle\rangle \times (1 + \mathfrak{m}_0)'$$

mit $\langle\langle \pi_0 \rangle\rangle = \{\pi_0^a,\ a \in \mathbb{Z}_p\}$.

BEWEIS: Für eine $(p-1)$-te Einheitswurzel ξ gilt $\xi^{p^r} = \xi$, denn es ist $p^r - 1 = (p-1)(1+p+p^2+\ldots+p^{r-1}) \equiv 0 \mod (p-1)$, also $p^r \equiv 1 \mod (p-1)$. Somit ist die Gruppe μ_{p-1} der $(p-1)$-ten Einheitswurzeln ein direkter Faktor jeder der Gruppen $K_0'^{p^r}$. Mit Lemma 5.29 folgt

$$K_0'/K_0'^{p^r} = \langle\pi_0\rangle/\langle\pi_0\rangle^{p^r} \times (1+\mathfrak{m}_0)'/(1+\mathfrak{m}_0)'^{p^r}.$$

Da man die Bildung des projektiven Limes mit der Bildung von direkten Produkten vertauschen kann, genügt es, die Identitäten

$$\langle\langle\pi_0\rangle\rangle = \varprojlim_r \langle\pi_0\rangle/\langle\pi_0\rangle^{p^r} \quad \text{und} \quad (1+\mathfrak{m}_0)' = \varprojlim_r (1+\mathfrak{m}_0)'/(1+\mathfrak{m}_0)'^{p^r}$$

nachzuweisen.

Zum Beweis der ersten Identität wird folgende Abbildung betrachtet,

$$\begin{aligned} \varphi: \quad \langle\langle\pi_0\rangle\rangle &\longrightarrow \varprojlim_r \langle\pi_0\rangle/\langle\pi_0\rangle^{p^r}, \\ \pi_0^a &\mapsto \left(\pi_0^{a \bmod p^r\mathbb{Z}_p}\right)_r. \end{aligned}$$

Ziel ist es, zu zeigen, dass φ ein Isomorphismus ist. Zunächst ist festzustellen, dass diese Abbildung wohldefiniert ist, denn für $r \geq s$ gilt $\pi_0^{a_0+\ldots+a_{r-1}p^{r-1}} \equiv \pi_0^{a_0+\ldots+a_{s-1}p^{s-1}} \mod \pi_0^{p^s}$, d.h. $\varphi(\pi_0^a)$ ist ein Element des projektiven Limes $\lim_r \langle\pi_0\rangle/\langle\pi_0\rangle^{p^r}$. Außerdem ist φ injektiv, denn es gilt

$$\begin{aligned} \varphi(\pi_0^a) = 1 \quad &\Longrightarrow \quad \pi_0^a \equiv 1 \mod \pi_0^{p^r} \text{ für alle } r \geq 1, \\ &\Longrightarrow \quad a \equiv 0 \mod p^r \text{ für alle } r \geq 1 \implies a = 0 \implies \pi_0^a = 1. \end{aligned}$$

Zum Beweis der Surjektivität sei $(\pi_0^{a_r})_r$ vorerst ein beliebiges Element des direkten Produkts $\prod_{r\geq 1}\langle\pi_0\rangle/\langle\pi_0\rangle^{p^r}$. Damit dies ein Element des projektiven Limes ist, muss für $r \geq s$

$$\pi_0^{a_r} \equiv \pi_0^{a_s} \mod \pi_0^{p^s}$$

gelten, d.h. $a_r \equiv a_s \mod p^s\mathbb{Z}_p$. Das Tupel $(a_r)_r$ definiert somit ein Element a des projektiven Limes $\mathbb{Z}_p$ und π_0^a ist das Urbild von $(\pi_0^{a_r})_r$. Damit ist die erste Identität nachgewiesen.

Um $(1+\mathfrak{m}_0)' = \lim_r (1+\mathfrak{m}_0)'/(1+\mathfrak{m}_0)'^{p^r}$ zu zeigen, wird auf der Gruppe $(1+\mathfrak{m}_0)$ neben der Bewertungstopologie $\mathcal{T}$ eine weitere Topologie $\mathcal{T}'$ eingeführt, die mit den Potenzen $(1+\mathfrak{m}_0)^{p^r}$ korrespondiert. Aus der Äquivalenz beider Topologien, die im Anschluss bewiesen wird, kann man Aussagen über die Komplettierung von $(1+\mathfrak{m}_0)'$ bezüglich der Topologie $\mathcal{T}'$ folgern. Die Topologien sind durch ihre Umgebungsbasen gegeben,

$$\begin{aligned} \mathcal{T}: \quad &\text{Umgebungsbasis der 1:} \quad \{V_\rho(1),\ \rho \in (p-1)\mathbb{N}\} \\ &\qquad\qquad\qquad\qquad\quad V_\rho(1) = \{x \in (1+\mathfrak{m}_0) : \nu_0(x-1) > \rho\}, \\ \mathcal{T}': \quad &\text{Umgebungsbasis der 1:} \quad \{(1+\mathfrak{m}_0)^{p^r},\ r \geq 0\}. \end{aligned}$$

Für die Elemente der Umgebungsbasis der 1 der Topologie $\mathcal{T}$ gilt $V_\rho(1) = 1+\mathfrak{m}_0^{\rho+1}$.

Lemma 6.12 *Auf $(1 + \mathfrak{m}_0)$ sind die Topologien $\mathcal{T}$ und $\mathcal{T}'$ äquivalent.*

Beweis: Es ist zu zeigen, dass jedes Element der Umgebungsbasis der 1 der einen Topologie in einem Element der Umgebungsbasis der 1 der anderen Topologie enthalten ist. Nach Lemma 4.2 gilt

$$(1 + \mathfrak{m}_0)^{p^r} \subseteq 1 + p^r\mathfrak{m}_0 = 1 + \mathfrak{m}_0^{r(p-1)+1} = V_{r(p-1)}(1).$$

Für $r=0$ gilt hier sogar Gleichheit. Nun ist $1+\mathfrak{m}_0^{r(p-1)+1} = V_{r(p-1)}(1) \subseteq (1 + \mathfrak{m}_0)^{p^{r-1}}$ für $r \geq 1$ zu zeigen. Wegen $r(p-1)+1 > 1$ für $r \geq 1$ kann Lemma 4.1 angewandt werden. Mit $r(p-1)+1 \geq (r-1)(p-1)+2$ folgt

$$\log V_{r(p-1)}(1) = \mathfrak{m}_0^{r(p-1)+1} \subseteq \mathfrak{m}_0^{(r-1)(p-1)+2}.$$

Andererseits gilt

$$\log(1 + \mathfrak{m}_0)^{p^{r-1}} = p^{r-1}\log(1 + \mathfrak{m}_0) = p^{r-1}\log(1 + \mathfrak{m}_0^2) = p^{r-1}\mathfrak{m}_0^2 = \mathfrak{m}_0^{(r-1)(p-1)+2}.$$

An dieser Stelle wurde die Gleichheit $\log(1 + \mathfrak{m}_0) = \log(1 + \mathfrak{m}_0^2)$ verwendet. Die Gültigkeit dieser Gleichheit kann mit derselben Argumentation wie im Beweis zu Satz 5.6 begründet werden. Zusammenfassend ergibt sich

$$\log V_{r(p-1)}(1) \subseteq \log(1 + \mathfrak{m}_0)^{p^{r-1}}.$$

Die Anwendung der Exponentialabbildung, die in diesem Fall ein Isomorphismus ist, liefert

$$V_{r(p-1)}(1) \subseteq (1 + \mathfrak{m}_0)^{p^{r-1}},$$

womit der Beweis der Äquivalenz der beiden Topologien abgeschlossen ist.

QED

Satz 6.13 *Die Gruppe $(1+\mathfrak{m}_0)'$ ist vollständig bezüglich der Topologie $\mathcal{T}$ bzw. $\mathcal{T}'$. Somit ist die Vervollständigung $\lim_r (1 + \mathfrak{m}_0)'/(1 + \mathfrak{m}_0)'^{p^r}$ von $(1 + \mathfrak{m}_0)'$ bezüglich $\mathcal{T}'$ gerade $(1 + \mathfrak{m}_0)'$, d.h.*

$$(1 + \mathfrak{m}_0)' = \varprojlim_r (1 + \mathfrak{m}_0)'/(1 + \mathfrak{m}_0)'^{p^r}.$$

Beweis: Die Gruppe $(1 + \mathfrak{m}_0)'$ läßt sich als

$$(1 + \mathfrak{m}_0)' = N_0^{-1}(\{1\}) \cap (1 + \mathfrak{m}_0)$$

darstellen. Dabei bezeichnet $N_0^{-1}(\{1\})$ das Urbild der 1 unter der Normabbildung $N_0 : (1 + \mathfrak{m}_0) \to \mathbb{Z}_p$. Um von dieser Darstellung auf die Vollständigkeit von

$(1+\mathfrak{m}_0)'$ schließen zu können, müssen die Stetigkeit von N_0 und die Vollständigkeit von $(1+\mathfrak{m}_0)$, jeweils bezüglich der Topologie $\mathcal{T}$ oder $\mathcal{T}'$, gezeigt werden. In diesem Fall gilt dann, dass $(1+\mathfrak{m}_0)'$ als Durchschnitt zweier abgeschlossener Mengen selbst abgeschlossen und als abgeschlossene Teilmenge eines vollständigen Raumes auch vollständig ist.

Wegen $\nu_0\big(\sigma(x-1)\big) = \nu_0(x-1)$ für $x \in (1+\mathfrak{m}_0)$ und $\sigma \in G(K_0/\mathbb{Q}_p)$ sind die Automorphismen $\sigma \in G(K_0/\mathbb{Q}_p)$ stetig. Somit ist auch die Normabbildung als Produkt der stetigen Abbildungen $\sigma \in G(K_0/\mathbb{Q}_p)$ stetig.

Nun ist noch die Vollständigkeit von $(1+\mathfrak{m}_0)$ zu begründen. Sei $\{z_j,\ j \in \mathbb{N}\}$ eine Folge in $(1+\mathfrak{m}_0)$, die gegen z konvergiert. Dann ist zu zeigen, dass $z \in (1+\mathfrak{m}_0)$. Aus der Konvergenz $z_j \to z$ folgt die Konvergenz $z_j - 1 \to z - 1$, d.h. es gilt $\nu_0(z_j-1) = \nu_0(z-1)$ für $j \geq j_0$. Wegen $\nu_0(z_j-1) \geq 1$ für alle $j \in \mathbb{N}$ folgt daraus $\nu_0(z-1) \geq 1$, d.h. $z \in (1+\mathfrak{m}_0)$.

QED

Damit ist auch der Beweis von Satz 6.11 abgeschlossen.

QED

Nach Konstruktion ist jedes Element $x \in X_0,\ x \neq 0$, als $x = \pi_0^a y^b$ mit $a, b \in \mathbb{Z}_p$ und $y \in (1+\mathfrak{m}_0)'$ darstellbar. Für ein derartiges x gilt $\psi_0(x) = a\psi_0(\pi_0) + b\psi_0(y)$. Damit kann ψ_0 nun als Abbildung

$$\psi_0 : X_0 \to \mathfrak{X}_0/p\,\mathfrak{X}_0$$

betrachtet werden.
Wie bereits in Satz 6.11 bemerkt, enthält X_0, im Gegensatz zu K_0', nicht mehr die $(p-1)$-ten Einheitswurzeln. Dass dies keinen Informationsverlust bedeutet, zeigt das folgende Lemma.

Lemma 6.14 *Für eine $(p-1)$-te Einheitswurzel ξ gilt $\psi_0(\xi) = 0$.*

Beweis: Sei $m \geq 1$. Dann gilt $N_{m0}(\xi) = \xi^{p^m} = \xi$, denn wie schon im Beweis zu Satz 6.11 begründet, gilt $p^m \equiv 1 \mod (p-1)$. Somit ist ξ ein Normurbild von ξ und man erhält

$$\psi_0(\xi) = -\frac{1}{p^m}\, S_{m0}\big(\delta_0(\xi)\big).$$

Die Potenzreihe $f(T) \in \mathbb{Z}_p[[T]],\ f(T) = \xi$, ist eine Potenzreihe für ξ. Mit Hilfe dieser Potenzreihe berechnet man

$$\delta_0(\xi) = \frac{\zeta_0}{\xi} f'(\pi_0) = 0.$$

Damit ist auch $\psi_0(\xi) = 0$. QED

Nachdem nun K_0' derart zu X_0 vervollständigt worden ist, dass die Projektoren $\widetilde{P}_\chi$ auf Elemente aus X_0 angewandt werden können, kann die Zerlegung von X_0 in Eigenräume angegeben werden. Die sich anschließenden Betrachtungen erfolgen unter Verwendung von [Was], Chap. 13, § 13.7 und § 13.8.

Satz 6.15 *Für die Eigenräume von X_0 gilt* $\operatorname{rk}_{\mathbb{Z}_p} X_0(\chi) = 1$.

Beweis: Sei $\chi \in G^\times$. Unter Verwendung von Lemma 6.3 gilt

$$\begin{aligned}
\nu_0\big(\widetilde{P}_\chi(\pi_0)\big) &= \nu_0\left(\Big(\prod_{\sigma\in G}\big(\sigma^{-1}(\pi_0)\big)^{\chi(\sigma)}\Big)^{\frac{1}{p-1}}\right)\\
&= \frac{1}{p-1}\sum_{\sigma\in G}\chi(\sigma)\nu_0\big(\sigma^{-1}(\pi_0)\big)\\
&= \frac{1}{p-1}\sum_{\sigma\in G}\chi(\sigma)\nu_0(\pi_0)\\
&= \begin{cases} 1, & \text{für } \chi = 1,\\ 0, & \text{für } \chi \neq 1. \end{cases}
\end{aligned} \tag{6.6}$$

Der Projektor $\widetilde{P}_1$ ist somit der einzige Projektor, der in die Untergruppe $\langle\langle\pi_0\rangle\rangle$ projiziert. Betrachtet werde die exakte Sequenz

$$1 \to (1+\mathfrak{m}_0)' \to X_0 \to X_0/(1+\mathfrak{m}_0)' \to 1.$$

Die Faktorgruppe $X_0/(1+\mathfrak{m}_0)'$ ist als $\mathbb{Z}_p$-Modul isomorph zu $\langle\langle\pi_0\rangle\rangle$, hat also $\mathbb{Z}_p$-Rang 1.

Die Gruppe $(1+\mathfrak{m}_0)'$ ist ein G-Modul, denn für $\sigma \in G$ und $x \in (1+\mathfrak{m}_0)'$ gilt $N_0\big(\sigma(x)\big) = N_0(x) = 1$ und $\nu_0\big(\sigma(x)-1\big) = \nu_0\big(\sigma(x-1)\big) = \nu_0(x-1) \geq 1$, also $\sigma(x) \in (1+\mathfrak{m}_0)'$. Somit kann man, ähnlich wie im Beweis zu Lemma 6.6, sehen, dass $X_0/(1+\mathfrak{m}_0)'$, im Gegensatz zu $\langle\langle\pi_0\rangle\rangle$, ein G-Modul ist. Aus diesem Grund kann die Wirkung von $\widetilde{P}_\chi$ auf $X_0/(1+\mathfrak{m}_0)'$ untersucht werden. Mit einer zu Lemma 6.8 analogen Rechnung sieht man, dass $\widetilde{P}_\chi\big(X_0/(1+\mathfrak{m}_0)'\big) = \widetilde{P}_\chi(X_0)/\widetilde{P}_\chi(1+\mathfrak{m}_0)'$. Daher geht die obige exakte Sequenz bei Anwendung von $\widetilde{P}_\chi$ in die exakte Sequenz

$$1 \to \widetilde{P}_\chi(1+\mathfrak{m}_0)' \to \widetilde{P}_\chi(X_0) \to \widetilde{P}_\chi\big(X_0/(1+\mathfrak{m}_0)'\big) \to 1 \tag{6.7}$$

über. Hier hat die Gruppe $\widetilde{P}_\chi\big(X_0/(1+\mathfrak{m}_0)'\big)$ entweder den $\mathbb{Z}_p$-Rang 0 oder 1.

Sei nun $\chi = 1$ der 1-Charakter. Dann gilt $\widetilde{P}_1(1+\mathfrak{m}_0)' = 1$, denn für $x \in (1+\mathfrak{m}_0)'$ gilt $\widetilde{P}_1(x) = \big(N_0(x)\big)^{\frac{1}{p-1}} = \sqrt[p-1]{1} = 1$, da $(1+\mathfrak{m}_0)'$ keine $(p-1)$-ten Einheitswurzeln außer 1 enthält. Somit erhält man aus der Sequenz (6.7) die Sequenz

$$1 \to 1 \to \widetilde{P}_1(X_0) \xrightarrow{\cong} \widetilde{P}_1\big(X_0/(1+\mathfrak{m}_0)'\big) \to 1.$$

Die mittlere Abbildung ist ein Isomorphismus, so dass $\widetilde{P}_1(X_0)$ denselben $\mathbb{Z}_p$-Rang hat wie $\widetilde{P}_1\big(X_0/(1+\mathfrak{m}_0)'\big)$. Dieser ist aufgrund der Gleichung (6.6) gleich 1, also

$$\mathrm{rk}_{\mathbb{Z}_p} X_0(1) = \mathrm{rk}_{\mathbb{Z}_p}\big(X_0/(1+\mathfrak{m}_0)'\big)(1) = 1.$$

Sei nun $\chi \neq 1$. Da die Projektoren $\widetilde{P}_\chi$ für $\chi \neq 1$ nicht auf die Untergruppe $\langle\langle \pi_0 \rangle\rangle$ projizieren, gilt $\widetilde{P}_\chi\big(X_0/(1+\mathfrak{m}_0)'\big) = 1$. Aus (6.7) erhält man deshalb die Sequenz

$$1 \to \widetilde{P}_\chi(1+\mathfrak{m}_0)' \xrightarrow{\cong} \widetilde{P}_\chi(X_0) \to 1 \to 1,$$

wobei die mittlere Abbildung wiederum ein Isomorphismus ist. Nach Theorem 13.54 und der dem Theorem vorangegangenen Bemerkung in [Was], Chap. 13, § 13.8, gilt $\widetilde{P}_\chi(1+\mathfrak{m}_0)' = \widetilde{P}_\chi(1+\mathfrak{m}_0)$ und $\mathrm{rk}_{\mathbb{Z}_p}(1+\mathfrak{m}_0)(\chi) = 1$ für $\chi \neq 1$. Somit haben alle Eigenräume $\widetilde{P}_\chi(1+\mathfrak{m}_0)'$ für $\chi \neq 1$ den $\mathbb{Z}_p$-Rang 1,

$$\mathrm{rk}_{\mathbb{Z}_p} X_0(\chi) = \mathrm{rk}_{\mathbb{Z}_p}(1+\mathfrak{m}_0)'(\chi) = 1.$$

QED

Da X_0 in $p-1$ Eigenräume vom $\mathbb{Z}_p$-Rang 1 zerlegt wurde, gilt

$$\mathrm{rk}_{\mathbb{Z}_p}(X_0) = \sum_{\chi \in G^\times} \mathrm{rk}_{\mathbb{Z}_p}\big(X_0(\chi)\big) = p-1.$$

Zusätzlich erhält man das Resultat $\mathrm{rk}_{\mathbb{Z}_p}(1+\mathfrak{m}_0)' = p-2$.

Nach dem Beweis zu Lemma 13.36 in [Was], Chap. 13, § 13.7, lassen sich die Eigenräume $\widetilde{P}_\chi(1+\mathfrak{m}_0)'$ folgendermaßen durch die Angabe erzeugender Elemente charakterisieren.

Lemma 6.16 *Sei $\chi = \omega^k,\ k = 1, \ldots, p-2$.*

(i) *Für $k \neq 1$ wird $\widetilde{P}_{\omega^k}(1+\mathfrak{m}_0)'$ von dem Element $\widetilde{P}_{\omega^k}(1-\pi_0^k)$ erzeugt.*

(ii) *$\widetilde{P}_\omega(1+\mathfrak{m}_0)'$ wird von $\widetilde{P}_\omega(1-\pi_0) = \widetilde{P}_\omega(\zeta_0)$ und $\widetilde{P}_\omega(1-\pi_0^p)$ erzeugt.*

Nach Lemma 4.7 gilt $\zeta_0 \in (1+\mathfrak{m}_0)'$. Die anderen Elemente $1-\pi_0^k,\ k = 2, \ldots, p-2, p$ liegen nicht unbedingt in $(1+\mathfrak{m}_0)'$, sind aber Elemente von $(1+\mathfrak{m}_0)$. Da nach der Bemerkung vor Theorem 13.54 in [Was], Chap. 13, § 13.8, für $\chi \neq 1$ die Identität $\widetilde{P}_\chi(1+\mathfrak{m}_0) = \widetilde{P}_\chi(1+\mathfrak{m}_0)'$ gilt, sind $\widetilde{P}_{\omega^k}(1-\pi_0^k),\ k = 1, \ldots, p-2, p$, auch tatsächlich Elemente von $\widetilde{P}_{\omega^k}(1+\mathfrak{m}_0)'$.

Sei $\sigma_a \in G$ der Automorphismus, der durch $\sigma_a(\zeta_0) = \zeta_0^a$ gekennzeichnet ist. Dann gilt

$$\widetilde{P}_\omega(\zeta_0) = \Bigg(\prod_{a=1}^{p-1} \big(\sigma_a^{-1}(\zeta_0)\big)^{\omega(a)}\Bigg)^{\frac{1}{p-1}} = \Bigg(\prod_{a=1}^{p-1} \zeta_0^{\frac{\omega(a)}{a}}\Bigg)^{\frac{1}{p-1}} = \zeta_0,$$

da es im Exponenten von ζ_0 nur auf den Wert modulo p ankommt und $\omega(a) \equiv a \mod p$ gilt. Somit kann man $\widetilde{P}_\omega(1+\mathfrak{m}_0)'$ auch als

$$\widetilde{P}_\omega(1+\mathfrak{m}_0)' = \langle\zeta_0\rangle \times \langle \widetilde{P}_\omega(1-\pi_0^p)\rangle$$

schreiben, wobei $\langle\zeta_0\rangle = \{\zeta_0^j,\ j = 0,\dots,p-1\}$ die endliche Untergruppe der p-ten Einheitswurzeln und $\langle \widetilde{P}_\omega(1-\pi_0^p)\rangle$ der von $\widetilde{P}_\omega(1-\pi_0^p)$ erzeugte $\mathbb{Z}_p$-Modul ist.

Da nun die Eigenräume $X_0(\chi),\ \chi \neq 1$, explizit durch Angabe ihrer Erzeugenden charakterisiert sind, ist es von Interesse, die Abbildung ψ_0 auf den Erzeugenden anzugeben. Aus diesem Grund werden zunächst zwei vorbereitende Lemmata formuliert.

Lemma 6.17 *Das folgende Diagramm ist kommutativ.*

$$\begin{array}{ccc} X_0 & \xrightarrow{\psi_0} & \mathfrak{X}_0/p\,\mathfrak{X}_0 \\ \Big\downarrow{\scriptstyle \widetilde{P}_\chi} & & \Big\downarrow{\scriptstyle P_{\chi\omega^{-1}}} \\ X_0(\chi) & \xrightarrow[\psi_0(\chi)]{} & \mathfrak{X}_0/p\,\mathfrak{X}_0(\chi\omega^{-1}) \end{array}$$

Beweis: Sei $x \in X_0$. Dann gilt unter Verwendung von Lemma 5.27

$$\begin{aligned} \psi_0\big(\widetilde{P}_\chi(x)\big) &= \psi_0\left(\Big(\prod_{\sigma\in G}\big(\sigma^{-1}(x)\big)^{\chi(\sigma)}\Big)^{\frac{1}{p-1}}\right) \\ &= \frac{1}{p-1}\sum_{\sigma\in G}\chi(\sigma)\psi_0\big(\sigma^{-1}(x)\big) \\ &= \frac{1}{p-1}\sum_{\sigma\in G}\chi(\sigma)\kappa(\sigma^{-1})\sigma^{-1}\big(\psi_0(x)\big). \end{aligned}$$

Die Abbildung $\sigma \mapsto \kappa(\sigma)$, wobei $\kappa(\sigma)$ die eindeutig bestimmte p-adische Einheit aus Lemma 5.10 ist, ist ein Charakter auf $G(K/\mathbb{Q}_p),\ K = \bigcup_{n\geq 0} K_n$. Dieser werde mit κ bezeichnet. Schränkt man κ auf $G = G(K_0/\mathbb{Q}_p)$ ein, und ist σ_a der Automorphismus aus G, der durch $\sigma_a(\zeta_0) = \zeta_0^a,\ a \in (\mathbb{Z}/p\,\mathbb{Z})^*$, bestimmt ist, so ist $\kappa(\sigma_a) \equiv a \mod p$, d.h. es gilt $\kappa_{|_G} = \omega$. Damit kann man weiter argumentieren

$$\begin{aligned} \psi_0\big(\widetilde{P}_\chi(x)\big) &= \frac{1}{p-1}\sum_{\sigma\in G}\chi(\sigma)\kappa(\sigma^{-1})\sigma^{-1}\big(\psi_0(x)\big) \\ &= \frac{1}{p-1}\sum_{\sigma\in G}\chi(\sigma)\omega^{-1}(\sigma)\sigma^{-1}\big(\psi_0(x)\big) \\ &= \frac{1}{p-1}\sum_{\sigma\in G}\chi\omega^{-1}(\sigma)\sigma^{-1}\big(\psi_0(x)\big) \\ &= P_{\chi\omega^{-1}}\big(\psi_0(x)\big), \end{aligned}$$

womit $\psi_0 \circ \widetilde{P}_\chi = P_{\chi\omega^{-1}} \circ \psi_0$ gezeigt ist.

QED

Ein schwieriger Teil bei der Berechnung der Bilder $\psi_0(x)$ ist das Finden von Normurbildern $x_m \in K'_m,\ N_{m0}(x_m) = x$. In dem hier betrachteten Spezialfall $n = 0$ ist es jedoch möglich, für ψ_0 eine vereinfachte Bildungsvorschrift anzugeben, bei der die Suche nach Normurbildern entfällt.

Lemma 6.18 *Es gilt* $\psi_0 = -\dfrac{1}{p}\,\delta_0$.

BEWEIS: Nach Satz 5.12 erhält man für $m \geq n$ und $y \in K_m^*$ die Gleichung

$$\delta_n\big(N_{mn}(y)\big) \equiv p^{-(m-n)} S_{mn}\big(\delta_m(y)\big) \mod \mathfrak{D}_n.$$

Speziell mit $n = 0,\ y = x_m$ und $N_{m0}(x_m) = x$ folgt $\delta_0(x) \equiv p^{-m} S_{m0}\big(\delta_m(x_m)\big)$ mod $\mathfrak{D}_0$. Dividiert man diese Gleichung durch p und beachtet $\mathfrak{D}_0 = p\,\mathfrak{m}_0^{-1}$, so ergibt sich

$$\psi_0(x) = -\frac{1}{p^{m+1}}\, S_{m0}\big(\delta_m(x_m)\big) \equiv -\frac{1}{p}\,\delta_0(x) \mod \mathfrak{m}_0^{-1}.$$

Um das Äquivalenzzeichen durch ein Gleichheitszeichen ersetzen zu können, ist der Nachweis von $\mathfrak{m}_0^{-1} \subseteq p\,\mathfrak{X}_0$ notwendig. Da aus Gleichung (5.18)

$$p\,\mathfrak{X}_0 = \big\{x \in K_0 : S_0\big(x \log(1+\mathfrak{m}_0)\big) \equiv 0 \mod p\big\}$$

folgt, reduziert sich der Beweis auf die Begründung von $S_0\big(\mathfrak{m}_0^{-1}\log(1+\mathfrak{m}_0)\big) \equiv 0$ mod p. So wie im Beweis zu Satz 5.6 sieht man, dass $\log(1+\mathfrak{m}_0) = \log(1+\mathfrak{m}_0^2)$. Auf $(1+\mathfrak{m}_0^2)$ ist der Logarithmus aber ein Isomorphismus (vgl. Lemma 4.1), so dass $\log(1+\mathfrak{m}_0) = \mathfrak{m}_0^2$ folgt. Es ergibt sich daher, unter Verwendung von Satz 4.9,

$$S_0\big(\mathfrak{m}_0^{-1}\log(1+\mathfrak{m}_0)\big) = S_0(\mathfrak{m}_0^{-1}\mathfrak{m}_0^2) = S_0(\mathfrak{m}_0) = p\,\mathbb{Z}_p \equiv 0 \mod p.$$

Damit ist das Lemma bewiesen.

QED

Mit Hilfe dieser vereinfachten Vorschrift ist es nun möglich, die Abbildung ψ_0 auf den Erzeugenden $\widetilde{P}_1(\pi_0),\ \zeta_0$ und $\widetilde{P}_{\omega^k}(1-\pi_0^k),\ k = 2\ldots p-2, p$ anzugeben.

Satz 6.19 *Für den Erzeuger* $\widetilde{P}_1(\pi_0)$ *von* $X_0(1)$ *und* ζ_0 *als Erzeuger des endlichen Anteils von* $X_0(\omega)$ *gilt*

$$\psi_0\big(\widetilde{P}_1(\pi_0)\big) = -P_{\omega^{-1}}(\mu_0) \quad \textit{und} \quad \psi_0(\zeta_0) = \frac{1}{p}.$$

Für die Erzeuger $\widetilde{P}_{\omega^k}(1-\pi_0^k)$ der Eigenräume $X_0(\omega^k)$, $k = 2, \ldots, p-2, p$, gilt

$$\psi_0\big(\widetilde{P}_{\omega^k}(1-\pi_0^k)\big) = \frac{k}{(p-1)p} \sum_{\sigma\in G} \omega^{k-1}(\sigma)\sigma^{-1}(\zeta_0)\frac{\sigma^{-1}(\pi_0)^{k-1}}{1-\sigma^{-1}(\pi_0)^k}.$$

Beweis: Die Einheitswurzel ζ_0 erzeugt nach Lemma 6.16 den endlichen Anteil des Eigenraumes $(1+\mathfrak{m}_0)'(\omega)$. Es gilt, unter Verwendung von $\delta_0(\zeta_0) = -1$ (vgl. Gleichung (5.7) auf Seite 53),

$$\psi_0(\zeta_0) = \frac{1}{p}.$$

Sei nun $k \in \{2, \ldots, p-2, p\}$ fest. Um $\psi_0\big(\widetilde{P}_{\omega^k}(1-\pi_0^k)\big)$ berechnen zu können, ist zunächst eine Potenzreihe für

$$\widetilde{P}_{\omega^k}(1-\pi_0^k) = \Big(\prod_{\sigma\in G}\big(\sigma^{-1}(1-\pi_0^k)\big)^{\omega^k(\sigma)}\Big)^{\frac{1}{p-1}}$$

anzugeben. Es ist $f(T) := 1-T^k$ eine Potenzreihe von $1-\pi_0^k$.
Mit $u_{\sigma^{-1}}(T) := 1-(1-T)^{\kappa(\sigma^{-1})}$ ist

$$f\big(u_{\sigma^{-1}}(T)\big) = 1-u_{\sigma^{-1}}(T)^k = 1-\big(1-(1-T)^{\kappa(\sigma^{-1})}\big)^k$$

eine Potenzreihe für $\sigma^{-1}(1-\pi_0^k)$ (vgl. Beweis zu Satz 5.11). Wählt man

$$f_{\sigma^{-1}}(T) := f\big(u_{\sigma^{-1}}(T)\big)^{\frac{\omega^k(\sigma)}{p-1}}$$

als Potenzreihe für $\sigma^{-1}(1-\pi_0^k)^{\frac{\omega^k(\sigma)}{p-1}}$, so erhält man

$$g(T) := \prod_{\sigma\in G} f_{\sigma^{-1}}(T)$$

als Potenzreihe für $\widetilde{P}_{\omega^k}(1-\pi_0^k)$. Damit gilt nun

$$\delta_0\big(\widetilde{P}_{\omega^k}(1-\pi_0^k)\big) = \zeta_0\,\frac{g'(T)}{g(T)}\Big|_{T=\pi_0}.$$

Zur Berechnung von $\frac{g'(T)}{g(T)} = \sum_{\sigma\in G}\frac{f'_{\sigma^{-1}}(T)}{f_{\sigma^{-1}}(T)}$ betrachtet man

$$\begin{aligned}
f'_{\sigma^{-1}}(T) &= \frac{\omega^k(\sigma)}{p-1}\, f\big(u_{\sigma^{-1}}(T)\big)^{\frac{\omega^k(\sigma)}{p-1}-1}\, f'\big(u_{\sigma^{-1}}(T)\big)\\
&= \frac{\omega^k(\sigma)}{p-1}\, f\big(u_{\sigma^{-1}}(T)\big)^{\frac{\omega^k(\sigma)}{p-1}-1}\big(-ku_{\sigma^{-1}}(T)^{k-1}\big)u'_{\sigma^{-1}}(T)\\
&= \frac{\omega^k(\sigma)}{p-1}\, f\big(u_{\sigma^{-1}}(T)\big)^{\frac{\omega^k(\sigma)}{p-1}-1}\big(-ku_{\sigma^{-1}}(T)^{k-1}\big)\kappa(\sigma^{-1})(1-T)^{\kappa(\sigma^{-1})-1},
\end{aligned}$$

so dass

$$\frac{f'_{\sigma^{-1}}(T)}{f_{\sigma^{-1}}(T)} = -\frac{\omega^k(\sigma)\kappa(\sigma^{-1})}{p-1}\frac{1}{f\big(u_{\sigma^{-1}}(T)\big)}\,k\,u_{\sigma^{-1}}(T)^{k-1}(1-T)^{\kappa(\sigma^{-1})-1}.$$

Wegen $\sigma \in G = G(K_0/\mathbb{Q}_p)$ gilt $\kappa(\sigma) = \omega(\sigma)$ und somit

$$\begin{aligned}\frac{f'_{\sigma^{-1}}(T)}{f_{\sigma^{-1}}(T)}\Big|_{T=\pi_0} &= -\frac{\omega^{k-1}(\sigma)}{p-1}\frac{1}{f\big(u_{\sigma^{-1}}(T)\big)}\,k\,u_{\sigma^{-1}}(T)^{k-1}(1-T)^{\omega^{-1}(\sigma)-1}\Big|_{T=\pi_0}\\ &= -\frac{\omega^{k-1}(\sigma)}{p-1}\,\frac{k\sigma^{-1}(\pi_0)^{k-1}}{1-\sigma^{-1}(\pi_0)^k}\,\frac{\sigma^{-1}(\zeta_0)}{\zeta_0}.\end{aligned}$$

Schließlich ergibt sich

$$\begin{aligned}\psi_0\big(\widetilde{P}_{\omega^k}(1-\pi_0^k)\big) &= -\frac{\zeta_0}{p}\,\frac{g'(T)}{g(T)}\Big|_{T=\pi_0}\\ &= \frac{\zeta_0}{p}\sum_{\sigma\in G}\frac{\omega^{k-1}(\sigma)}{p-1}\frac{k\sigma^{-1}(\pi_0)^{k-1}}{1-\sigma^{-1}(\pi_0)^k}\frac{\sigma^{-1}(\zeta_0)}{\zeta_0}\\ &= \frac{k}{(p-1)p}\sum_{\sigma\in G}\omega^{k-1}(\sigma)\sigma^{-1}(\zeta_0)\frac{\sigma^{-1}(\pi_0)^{k-1}}{1-\sigma^{-1}(\pi_0)^k}.\end{aligned}$$

Abschließend ist noch die Formel für $\psi_0\big(\widetilde{P}_1(\pi_0)\big)$ zu berechnen. Da π_0 ein Erzeuger von $\langle\langle\pi_0\rangle\rangle$ ist, ist für $\chi = 1$ das Element $\widetilde{P}_1(\pi_0)$ ein Erzeuger von $\big(X_0/(1+\mathfrak{m}_0)'\big)(1) \cong X_0(1)$ (vgl. Satz 6.15). Für das Bild dieses Erzeugers unter ψ_0 ergibt sich mit dem Diagramm aus Lemma 6.17 und Gleichung (5.8) von Seite 53

$$\psi_0\big(\widetilde{P}_1(\pi_0)\big) = P_{\omega^{-1}}\big(\psi_0(\pi_0)\big) = -\frac{1}{p}P_{\omega^{-1}}\big(\delta_0(\pi_0)\big) = -\frac{1}{p}P_{\omega^{-1}}\left(\frac{\zeta_0}{\pi_0}\right) = -P_{\omega^{-1}}(\mu_0).$$

Damit ist das Bild von ψ_0 auf allen Erzeugern der Eigenräume von X_0 angegeben.

QED

Es sei angemerkt, dass sich beim Beweis des letzten Satzes für die Berechnung von $\psi_0\big(\widetilde{P}_{\omega^k}(1-\pi_0^k)\big)$ nicht die Kommutativität des Diagramms aus Lemma 6.17 ausnutzen ließ. Die Abbildung ψ_0 darf nicht auf die Elemente $1-\pi_0^k$ angewendet werden, da diese nicht in X_0 liegen.

Zum Abschluss dieses Abschnitts sei noch eine allgemeine Formel für $\psi_0\big(\widetilde{P}_\chi(x)\big) = P_{\chi\omega^{-1}}\big(\psi_0(x)\big)$ angegeben. Damit diese leichter auf den Fall $n > 0$ übertragen werden kann, wird nun wieder mit der ursprünglichen Beschreibung von ψ_0 gearbeitet.

Mit Blick auf Satz 6.11 genügt es, die allgemeine Gleichung für $P_{\chi\omega^{-1}}\big(\psi_0(x)\big)$ für $x \in (1+\mathfrak{m}_0)'$ zu bestimmen.

Für $n \geq 0$ sei $(1+\mathfrak{m}_n)' := \big\{x \in (1+\mathfrak{m}_n) : N_n(x) = 1\big\}$. Da die universellen Normen K_n' nach Lemma 5.23 ein projektives System bezüglich der Normabbildungen N_{mn} bilden, bilden auch die $(1+\mathfrak{m}_n)'$ als direkte Faktoren der K_n' (vgl. Lemma 5.29) ein projektives System bezüglich der Abbildungen N_{mn}. Sei

$$U := \varprojlim_n (1+\mathfrak{m}_n)'. \tag{6.8}$$

Für ein beliebiges $x \in (1+\mathfrak{m}_0)'$ findet man ein $x_1 \in (1+\mathfrak{m}_1)'$ mit $N_{10}(x_1) = x$. Für dieses x_1 findet man wiederum ein $x_2 \in (1+\mathfrak{m}_2)'$ mit $N_{21}(x_2) = x_1$, und so fort. Dann ist das Element $u := (\ldots, x_2, x_1, x)$ ein Element des projektiven Limes U. Nach [Was], Chap. 13, § 13.7, Theorem 13.38, gibt es zu diesem u eine eindeutig bestimmte Potenzreihe $f_u \in \mathbb{Z}_p[[T]]$ mit $f(\pi_n) = x_n$ für alle $n \geq 1$ bzw. $f(\pi_0) = x$. Mit Hilfe dieser Potenzreihe wird der folgende Satz formuliert.

Satz 6.20 *Seien $m \geq 1$, $x \in (1+\mathfrak{m}_0)'$, $u \in U$ ein zu x gehörendes Element des projektiven Limes und f_u die für u eindeutig bestimmte Potenzreihe aus $\mathbb{Z}_p[[T]]$. Dann gilt*

$$P_{\chi\omega^{-1}}\big(\psi_0(x)\big) = -\frac{1}{(p-1)p^{m+1}} \sum_{\rho \in G(K_m/\mathbb{Q}_p)} \chi\omega^{-1}(\rho) \left((1-T)\frac{f_u'(T)}{f_u(T)}\right)\Bigg|_{T=\rho^{-1}(\pi_m)}.$$

Dabei ist $\chi\omega^{-1}(\rho)$ definiert als $\chi\omega^{-1}(\rho')$ mit $\rho' \in G = G(K_0/\mathbb{Q}_p)$ und $\rho \equiv \rho'$ mod $G(K_m/K_0)$.

Beweis: Sei $x_m = f_u(\pi_m)$. Dann gilt

$$\delta_m(x_m) = \frac{\zeta_m}{x_m} f_u'(\pi_m) = \zeta_m \frac{f_u'(\pi_m)}{f(\pi_m)} = (1-\pi_m)\frac{f_u'(\pi_m)}{f(\pi_m)} = \left((1-T)\frac{f_u'(T)}{f_u(T)}\right)\Bigg|_{T=\pi_m}.$$

Zur Berechnung von $P_{\chi\omega^{-1}}\big(\psi_0(x)\big)$ wird zunächst die kurze exakte Sequenz

$$\begin{array}{ccccccccc} 1 \to & G(K_m/K_0) & \overset{\iota}{\hookrightarrow} & G(K_m/\mathbb{Q}_p) & \overset{\pi}{\twoheadrightarrow} & G(K_0/\mathbb{Q}_p) & \to 1, \\ & \sigma & \mapsto & \sigma;\ \tau' & \mapsto & \tau & \end{array}$$

betrachtet. Sei H die Untergruppe der Elemente von $G(K_m/\mathbb{Q}_p)$, deren Ordnung ein Teiler von $p-1$ ist. Dann gibt es einen Isomorphismus $\pi|_H : H \cong G(K_0/\mathbb{Q}_p)$. In obiger Sequenz seien die τ' als Elemente von H aufgefasst. In der folgenden Rechnung werden σ, τ und τ' immer als Elemente derjenigen Galoisgruppe verstanden, wie es in obiger Sequenz angezeigt ist. Für einen beliebigen Charakter

$\chi \in G(K_0/\mathbb{Q}_p)^\times$ und ein beliebiges $y \in K_m$ gilt

$$\begin{aligned} P_\chi\big(S_{m0}(y)\big) &= P_\chi\Big(\sum_\sigma \sigma(y)\Big) \\ &= \frac{1}{p-1}\sum_\tau \chi(\tau)\sum_\sigma \tau'^{-1}\sigma(y) = \frac{1}{p-1}\sum_{\tau',\sigma}\chi(\tau')\tau'^{-1}\sigma(y), \end{aligned}$$

wobei $\chi(\tau')$ mit $\chi(\tau)$ identifiziert wird, wenn sich τ' und τ unter dem Isomorphismus $\pi|_H$ entsprechen. Wenn τ und σ in obiger Summe unabhängig voneinander die Gruppen $G(K_0/\mathbb{Q}_p)$ und $G(K_m/K_0)$ durchlaufen, so durchläuft $\rho^{-1} := \tau'^{-1}\sigma$ die ganze Gruppe $G(K_m/\mathbb{Q}_p)$. Vereinbart man noch $\chi(\rho) := \chi\big(\pi(\rho)\big)$ für $\rho \in G(K_m/\mathbb{Q}_p)$, so folgt

$$P_\chi\big(S_{m0}(y)\big) = \frac{1}{p-1}\sum_{\rho\in G(K_m/\mathbb{Q}_p)} \chi(\rho)\rho^{-1}(y).$$

Angewandt auf $P_{\chi\omega^{-1}}\big(\psi_0(x)\big)$ ergibt dies

$$\begin{aligned} P_{\chi\omega^{-1}}\big(\psi_0(x)\big) &= -\frac{1}{p^{m+1}}P_{\chi\omega^{-1}}\Big(S_{m0}\Big(\Big((1-T)\frac{f_u'(T)}{f_u(T)}\Big)\Big|_{T=\pi_m}\Big)\Big) \\ &= -\frac{1}{(p-1)p^{m+1}}\sum_{\rho\in G(K_m/\mathbb{Q}_p)}\chi\omega^{-1}(\rho)\Big((1-T)\frac{f_u'(T)}{f_u(T)}\Big)\Big|_{T=\rho^{-1}(\pi_m)}. \end{aligned}$$

QED

6.3 Ausblick auf den Fall $n > 0$

Nachdem im Abschnitt 6.2 die Zerlegung der Abbildung ψ_0 unter den Charakteren der Gruppe $G(K_0/\mathbb{Q}_p)$ angegeben worden ist, sollen die Resultate in diesem Abschnitt auf die Abbildung

$$\psi_n : K_n' \to \mathfrak{X}_n/p^{n+1}\mathfrak{X}_n, \quad x \mapsto -\frac{1}{p^{m+1}}S_{mn}(\delta_m(x_m)),\ m \geq 2n+1,$$

übertragen werden. Dabei sind

$$K_n' = \langle\pi_n\rangle \times \mu_{p-1} \times (1+\mathfrak{m}_n)'$$

mit $(1+\mathfrak{m}_n)' = \big\{x \in (1+\mathfrak{m}_n) : N_n(x) = 1\big\}$ und

$$\mathfrak{X}_n = \left\{\sum_\sigma c_\sigma\sigma(\mu_n) + \sum_\sigma d_\sigma\sigma(\theta_n),\ \sigma \in G(K_n/\mathbb{Q}_p),\ c_\sigma, d_\sigma \in \mathbb{Z}_p,\ \sum_\sigma d_\sigma = 0\right\}$$

mit $\mu_n := \frac{1}{p^{n+1}}\frac{\zeta_n}{\pi_n}$ und $\theta_n := \frac{1}{p^{n+1}}\sum_{j=0}^n \zeta_j^{-1}$. Eine Verallgemeinerung ist in zwei Richtungen denkbar.

Zum einen kann man die Zerlegung von ψ_n unter den Charakteren der Galoisgruppe $G(K_n/\mathbb{Q}_p)$ betrachten. Analog wie in den Beweisen zu Lemma 6.6 und Lemma 6.7 erkennt man, dass $\mathfrak{X}_n$ und K_n' $G(K_n/\mathbb{Q}_p)$-Moduln sind. Auf beiden Gruppen betrachtet man für $\chi \in G(K_n/\mathbb{Q}_p)^\times$ die Projektoren

$$P_\chi = \frac{1}{(p-1)p^n} \sum_{\sigma \in G(K_n/\mathbb{Q}_p)} \chi(\sigma)\sigma^{-1} \quad \text{und} \quad \widetilde{P}_\chi = \prod_{\sigma \in G(K_n/\mathbb{Q}_p)} (\sigma^{-1})^{\frac{\chi(\sigma)}{(p-1)p^n}}.$$

Diese sind nun aber nicht mehr Elemente von $\mathbb{Z}_p[G(K_n/\mathbb{Q}_p)]$, sondern von $\mathbb{Q}_p[G(K_n/\mathbb{Q}_p)]$, denn es ist $\mathbb{Z}_p[\frac{1}{p^n}] = \mathbb{Z}_p[\frac{1}{p}] = \mathbb{Q}_p$. Die Gruppen $\mathfrak{X}_n$ und K_n' müssen also in der Weise erweitert werden, dass in $\mathfrak{X}_n$ die Multiplikation und in K_n' die Potenzierung mit Elementen $a \in \mathbb{Q}_p$ erklärt ist. Während letzteres ein schwieriges Problem darstellt, kann man ersteres bewerkstelligen, indem man

$$\mathfrak{X}_n := \Big\{ \sum_\sigma c_\sigma \sigma(\mu_n) + \sum_\sigma d_\sigma \sigma(\theta_n),\ \sigma \in G(K_n/\mathbb{Q}_p),\ c_\sigma, d_\sigma \in \mathbb{Q}_p,\ \sum_\sigma d_\sigma = 0 \Big\}$$

definiert. Allerdings kann nun nicht mehr der Faktor $\mathfrak{X}_n/p^{n+1}\mathfrak{X}_n$ betrachtet werden.

Die andere Möglichkeit der Verallgemeinerung besteht darin, dass man $\mathfrak{X}_n$ und K_n' als $G(K_0/\mathbb{Q}_p)$-Moduln auffasst. Dies erreicht man, wenn man $G = G(K_0/\mathbb{Q}_p)$ mit der Untergruppe $H \subseteq G(K_n/\mathbb{Q}_p)$ aller Elemente σ mit $\sigma^{p-1} = id$ identifiziert. Dann gilt das folgende Lemma.

Lemma 6.21 *Sei $G = G(K_0/\mathbb{Q}_p)$. Die Gruppen $\mathfrak{X}_n$ und K_n' sind G-Moduln. Die Projektoren haben die Gestalt*

$$P_\chi = \frac{1}{p-1} \sum_{\sigma \in G} \chi(\sigma)\sigma^{-1} \quad \textit{und} \quad \widetilde{P}_\chi = \Big(\prod_{\sigma \in G} (\sigma^{-1})^{\chi(\sigma)} \Big)^{\frac{1}{p-1}}.$$

Die Anwendung von P_χ auf Elemente $x \in \mathfrak{X}_n$ ist wohldefiniert, im Gegensatz zur Anwendung von $\widetilde{P}_\chi$ auf Elemente $x \in K_n'$, da in K_n' die Potenzierung mit Elementen $a \in \mathbb{Z}_p$ nicht definiert ist. Geht man jedoch zur Komplettierung

$$X_n := \varprojlim_r K_n'/(K_n')^{p^r} = \langle\langle \pi_n \rangle\rangle \times (1 + \mathfrak{m}_n)'$$

über, so kann $\widetilde{P}_\chi$ auf $x \in X_n$ angewandt werden. Da für eine $(p-1)$-te Einheitswurzel $\xi \in \mu_{p-1}$ die Gleichheit $\psi_n(\xi) = 0$ gilt, stellt der Übergang von K_n' zum projektiven Limes X_n, der μ_{p-1} nicht mehr als direkten Faktor enthält, keinen Informationsverlust dar.

Die Aussagen des Lemmas folgen aus den Beweisen der dazu analogen Aussagen im Fall $n = 0$ in Lemma 6.6, Lemma 6.7, Satz 6.11 und Lemma 6.14.

Wie im Fall $n = 0$, so genügt es auch hier zunächst, die Eigenräume von $\mathfrak{X}_n$ zu bestimmen (vgl. Lemma 6.8). Als Voraussetzung dazu ist das nachstehende Lemma notwendig (vgl. Lemma 6.9).

Lemma 6.22 *In $\mathfrak{X}_n$ besteht zwischen μ_n und θ_n die Beziehung*

$$\mu_n = \frac{1}{p^{n+1}} \sum_{\substack{a=0 \\ (a,p)=1}}^{p^{n+1}-1} \Big(a - \frac{p^{n+1}-p}{2}\Big)\sigma_a(\theta_n),$$

wobei mit σ_a der Automorphismus aus $G(K_n/\mathbb{Q}_p)$ gemeint ist, für den $\sigma_a(\zeta_n) = \zeta_n^a$ gilt.

Beweis: Es ist die Gleichheit

$$\frac{\zeta_n}{\pi_n} = \sum_{\substack{a=0 \\ (a,p)=1}}^{p^{n+1}-1} a\sigma_a(\theta_n) - \frac{p^{n+1}-p}{2} \sum_{\substack{a=0 \\ (a,p)=1}}^{p^{n+1}-1} \sigma_a(\theta_n) \tag{6.9}$$

zu zeigen. Dazu werden die beiden Summen auf der rechten Seite einzeln ausgewertet. Zuvor wird jedoch die Gleichheit

$$\frac{1}{p^{n+1}} \sum_{a=0}^{p^{n+1}-1} a\zeta_n^{-a} = \frac{1}{p^{n+1}} \sum_{a=1}^{p^{n+1}-1} a\zeta_n^{-a} = \frac{\zeta_n}{\pi_n} \tag{6.10}$$

bewiesen. Es gilt

$$\pi_n \sum_{a=1}^{p^{n+1}-1} a\zeta_n^{-a} = \sum_{a=1}^{p^{n+1}-1} a(1-\zeta_n)\zeta_n^{-a} = \sum_{a=1}^{p^{n+1}-1} a\zeta_n^{-a} - \sum_{a=1}^{p^{n+1}-1} a\zeta_n^{1-a}.$$

In der zweiten Summe auf der rechten Seite werde die Variablensubstitution $-b := 1 - a$ vorgenommen, so dass

$$\begin{aligned}
\pi_n \sum_{a=1}^{p^{n+1}-1} a\zeta_n^{-a} &= \sum_{a=1}^{p^{n+1}-1} a\zeta_n^{-a} - \sum_{b=0}^{p^{n+1}-2} (b+1)\zeta_n^{-b} \\
&= \sum_{a=1}^{p^{n+1}-2} a\zeta_n^{-a} + (p^{n+1}-1)\zeta_n^{-(p^{n+1}-1)} - 1 - \sum_{b=1}^{p^{n+1}-2} (b+1)\zeta_n^{-b} \\
&= (p^{n+1}-1)\zeta_n - 1 - \sum_{b=1}^{p^{n+1}-1} \zeta_n^{-b} + \zeta_n^{-(p^{n+1}-1)} \\
&= p^{n+1}\zeta_n - 1 - \sum_{b=1}^{p^{n+1}-1} \zeta_n^{-b}.
\end{aligned}$$

Für die Summe in der letzten Zeile ergibt sich

$$\sum_{b=1}^{p^{n+1}-1} \zeta_n^{-b} = \sum_{k=0}^{n} \sum_{\substack{b=1 \\ v_p(b)=k}}^{p^{n+1}-1} \zeta_n^{-b}.$$

Es ist $\{1 \le b \le p^{n+1}-1, v_p(b) = k\} = \{b'p^k, (b',p) = 1, 1 \le b' \le p^{n-k+1}-1\}$. Damit folgt

$$\sum_{k=0}^{n} \sum_{\substack{b=1 \\ v_p(b)=k}}^{p^{n+1}-1} \zeta_n^{-b} = \sum_{k=0}^{n} \sum_{\substack{b'=1 \\ (b',p)=1}}^{p^{n-k+1}-1} \zeta_n^{-b'p^k} = \sum_{k=0}^{n} \sum_{\substack{b'=1 \\ (b',p)=1}}^{p^{n-k+1}-1} \zeta_{n-k}^{-b'} = \sum_{k=0}^{n} S_{n-k}(\zeta_{n-k}^{-1}) = -1,$$

denn nach Lemma 4.8 sind die Summanden der letzten Summe für $k < n$ alle gleich Null. Nur für $k = n$ gilt $S_0(\zeta_0^{-1}) = -1$. Insgesamt ergibt sich somit

$$\pi_n \sum_{a=1}^{p^{n+1}-1} a\zeta_n^{-a} = p^{n+1}\zeta_n - 1 - \sum_{b=1}^{p^{n+1}-1} \zeta_n^{-b} = p^{n+1}\zeta_n$$

und Gleichung (6.10) ist bewiesen.

Mit $\sigma_a(\zeta_j) = \sigma_a(\zeta_n^{p^{n-j}}) = \zeta_n^{ap^{n-j}} = \zeta_j^a$ folgt nun für die erste Summe in Gleichung (6.9)

$$\sum_{\substack{a=0 \\ (a,p)=1}}^{p^{n+1}-1} a\sigma_a(\theta_n) = \frac{1}{p^{n+1}} \sum_{j=0}^{n} \sum_{\substack{a=0 \\ (a,p)=1}}^{p^{n+1}-1} a\zeta_j^{-a}.$$

Für festes j lässt sich jedes $a \in \{0, \dots, p^{n+1}-1\}$, $(a,p) = 1$, eindeutig als $a = b + kp^{j+1}$ mit $b \in \{0, \dots, p^{j+1}-1\}$, $(b,p) = 1$, und $k \in \{0, \dots, p^{n-j}-1\}$ darstellen. Damit folgt $\zeta_j^{-a} = \zeta_j^{-b-kp^{j+1}} = \zeta_j^{-b}$ und

$$\begin{aligned}
\sum_{\substack{a=0 \\ (a,p)=1}}^{p^{n+1}-1} a\sigma_a(\theta_n) &= \\
&= \frac{1}{p^{n+1}} \sum_{j=0}^{n} \sum_{\substack{b=0 \\ (b,p)=1}}^{p^{j+1}-1} \Bigg(\sum_{k=0}^{p^{n-j}-1} \big(b + kp^{j+1}\big) \Bigg) \zeta_j^{-b} \\
&= \frac{1}{p^{n+1}} \sum_{j=0}^{n} \sum_{\substack{b=0 \\ (b,p)=1}}^{p^{j+1}-1} p^{n-j} b\zeta_j^{-b} + \frac{1}{p^{n+1}} \sum_{j=0}^{n} \sum_{\substack{b=0 \\ (b,p)=1}}^{p^{j+1}-1} \Bigg(\sum_{k=0}^{p^{n-j}-1} k \Bigg) p^{j+1} \zeta_j^{-b} \\
&= \frac{1}{p^{n+1}} \sum_{j=0}^{n} \sum_{\substack{b=0 \\ (b,p)=1}}^{p^{j+1}-1} bp^{n-j} \zeta_j^{-bp^{n-j}} + \frac{1}{p^{n+1}} \sum_{j=0}^{n} p^{j+1} \frac{(p^{n-j}-1)p^{n-j}}{2} \sum_{\substack{b=0 \\ (b,p)=1}}^{p^{j+1}-1} \zeta_j^{-b}.
\end{aligned}$$

Für die zweite Summe im zweiten Summanden gilt $\sum_{b=0,(b,p)=1}^{p^{j+1}-1} \zeta_j^{-b} = S_j(\zeta_j^{-1})$. Nach Lemma 4.8 ist dieser Ausdruck für alle $j \neq 0$ gleich Null, für $j = 0$ gilt $S_0(\zeta_0^{-1}) = -1$. In der ersten Summe durchläuft der Ausdruck bp^{n-j} die Menge $0 \leq a \leq p^{n+1} - 1$, wenn b und j die angegebenen Mengen durchlaufen. Mit Hilfe der Beziehung (6.10) folgt daher

$$\sum_{\substack{a=0 \\ (a,p)=1}}^{p^{n+1}-1} a\sigma_a(\theta_n) = \frac{1}{p^{n+1}} \sum_{a=0}^{p^{n+1}-1} a\zeta_n^{-a} - \frac{1}{p^{n+1}} \frac{(p^n-1)p^{n+1}}{2} = \frac{\zeta_n}{\pi_n} - \frac{p^n-1}{2}.$$

Für die zweite Summe in Gleichung (6.9) erhält man

$$\sum_{\substack{a=0 \\ (a,p)=1}}^{p^{n+1}-1} \sigma_a(\theta_n) = S_n(\theta_n) = \frac{1}{p^{n+1}} \sum_{j=0}^{n} S_n(\zeta_j^{-a}) = -\frac{1}{p}.$$

Insgesamt ergibt sich daraus

$$\sum_{\substack{a=0 \\ (a,p)=1}}^{p^{n+1}-1} a\sigma_a(\theta_n) - \frac{p^{n+1}-p}{2} \sum_{\substack{a=0 \\ (a,p)=1}}^{p^{n+1}-1} \sigma_a(\theta_n) = \frac{\zeta_n}{\pi_n} - \frac{p^n-1}{2} + \frac{p^{n+1}-p}{2}\frac{1}{p} = \frac{\zeta_n}{\pi_n}.$$

QED

Nun kann man eine Aussage über die Eigenräume von $\mathfrak{X}_n$ formulieren.

Satz 6.23 *Für die Eigenräume von $\mathfrak{X}_n$ gilt*

$$\mathfrak{X}_n(\chi) = \begin{cases} \displaystyle\sum_{\rho \in G(K_n/K_0)} \frac{1}{p^{n+1}} \mathbb{Z}_p P_\chi(\rho\theta_n), & \text{für } \chi = \omega^{-1}, \\ \displaystyle\sum_{\rho \in G(K_n/K_0)} \frac{1}{p^n} \mathbb{Z}_p P_\chi(\rho\theta_n), & \text{sonst.} \end{cases}$$

Die Eigenräume haben den $\mathbb{Z}_p$-Rang p^n.

Beweis: Im folgenden wird die Gruppe $G := G(K_0/\mathbb{Q}_p)$ wieder mit der Untergruppe $H \subseteq G(K_n/\mathbb{Q}_p)$ der Elemente, deren Ordnung ein Teiler von $(p-1)$ ist, identifiziert. Seien χ ein Charakter von G und $\tau \in G(K_n/K_0)$. Dann gilt

$$\begin{aligned} P_\chi\big(\tau(\mu_n)\big) &= \frac{1}{p-1} \sum_{\sigma \in G} \chi(\sigma)\sigma^{-1}\tau(\mu_n) \\ &= \frac{1}{p-1} \sum_{\sigma \in G} \chi(\sigma^{-1})\sigma\tau(\mu_n) \;=\; \sum_{\sigma' \in G(K_n/\mathbb{Q}_p)} c_{\sigma'}\sigma'(\mu_n) \end{aligned}$$

mit $c_{\sigma'} = \frac{\chi(\sigma^{-1})}{p-1}$ falls $\sigma' = \sigma\tau$ und $\sigma \in G$ und $c_{\sigma'} = 0$ sonst. Damit erkennt man

$$P_\chi\big(\tau(\mu_n)\big) \in \mathfrak{X}_n \quad \text{für alle} \quad \chi \in G^\times.$$

Außerdem gilt

$$P_\chi\big(\tau(\theta_n)\big) = \frac{1}{p-1}\sum_{\sigma\in G}\chi(\sigma^{-1})\sigma\tau(\theta_n) = \sum_{\sigma'\in G(K_n/\mathbb{Q}_p)} d_{\sigma'}\sigma'(\theta_n)$$

mit $d_{\sigma'} = \frac{\chi(\sigma^{-1})}{p-1}$ für $\sigma' = \sigma\tau$ und $\sigma \in G$ und $d_{\sigma'} = 0$ sonst. Damit ist $\sum_{\sigma'} d_{\sigma'} = 1$ für $\chi = 1$ und $\sum_{\sigma'} d_{\sigma'} = 0$ für $\chi \neq 1$. Es folgt

$$P_\chi\big(\tau(\theta_n)\big) \in \mathfrak{X}_n \quad \text{für} \quad \chi \neq 1.$$

Jedes $\sigma \in G(K_n/\mathbb{Q}_p) = G(K_0/\mathbb{Q}_p) \times G(K_n/K_0)$ lässt sich eindeutig als $\sigma = \sigma_1\sigma_2$ mit $\sigma_1 \in G(K_0/\mathbb{Q}_p)$ und $\sigma_2 \in G(K_n/K_0)$ schreiben. Für $\sigma \in G(K_n/\mathbb{Q}_p)$ und $u \in K_n$ gilt, unter Verwendung der Variablensubstitution $\rho^{-1} := \tau^{-1}\sigma_1$,

$$\begin{aligned} P_\chi\big(\sigma(u)\big) &= \frac{1}{p-1}\sum_{\tau\in G}\chi(\tau)\tau^{-1}\big(\sigma(u)\big) = \frac{1}{p-1}\sum_{\tau\in G}\chi(\tau)\tau^{-1}\sigma_1\sigma_2(u) \\ &= \frac{1}{p-1}\sum_{\rho\in G}\chi(\sigma_1\rho)\rho^{-1}\sigma_2(u) = \chi(\sigma_1)P_\chi\big(\sigma_2(u)\big). \end{aligned} \tag{6.11}$$

Für ein beliebiges Element $\sum_\sigma c_\sigma\sigma(\mu_n) + \sum_\sigma d_\sigma\sigma(\theta_n)$, $\sigma \in G(K_n/\mathbb{Q}_p)$, aus $\mathfrak{X}_n$ kann man schlussfolgern

$$\begin{aligned} P_\chi\Big(\sum_\sigma c_\sigma\sigma(\mu_n) + \sum_\sigma d_\sigma\sigma(\theta_n)\Big) &= \\ &= \sum_\sigma c_\sigma P_\chi\big(\sigma(\mu_n)\big) + \sum_\sigma d_\sigma P_\chi\big(\sigma(\theta_n)\big) \\ &= \sum_\sigma c_\sigma\chi(\sigma_1)P_\chi\big(\sigma_2(\mu_n)\big) + \sum_\sigma d_\sigma\chi(\sigma_1)P_\chi\big(\sigma_2(\theta_n)\big). \end{aligned} \tag{6.12}$$

Zuerst wird der Fall $\chi \neq 1$ untersucht. Alle Vorfaktoren in Gleichung (6.12) sind Elemente von $\mathbb{Z}_p$. Daher gilt mit $\sigma_2 \in G(K_n/K_0)$ und den obigen Vorbemerkungen

$$\mathfrak{X}_n(\chi) \;\subseteq\; \sum_{\sigma_2}\mathbb{Z}_p P_\chi\big(\sigma_2(\mu_n)\big) + \sum_{\sigma_2}\mathbb{Z}_p P_\chi\big(\sigma_2(\theta_n)\big) \;\subseteq\; \mathfrak{X}_n.$$

Da andererseits die Anwendung eines $P_{\chi'}$ auf ein Element aus der mittleren Menge für $\chi' \neq \chi$ die Nullabbildung und für $\chi' = \chi$ die Identität ist, folgt die Gleichheit

$$\mathfrak{X}_n(\chi) \;=\; \sum_\sigma \mathbb{Z}_p P_\chi\big(\sigma(\mu_n)\big) + \sum_\sigma \mathbb{Z}_p P_\chi\big(\sigma(\theta_n)\big), \qquad \sigma \in G(K_n/K_0).$$

Mit Hilfe der Beziehung aus Lemma 6.22 wird die rechte Seite dieser Gleichung noch vereinfacht. Sei dazu $\tau \in G(K_n/K_0)$. Der Automorphismus $\sigma_a \in G(K_n/\mathbb{Q}_p)$,

der durch $\sigma_a(\zeta_n) = \zeta_n^a$ charakterisiert ist, werde in $\sigma_a = \sigma'_a\sigma''_a$ mit $\sigma'_a \in G(K_0/\mathbb{Q}_p)$ und $\sigma''_a \in G(K_n/K_0)$ zerlegt. Dann gilt

$$P_\chi\big(\tau(\mu_n)\big) = P_\chi\Bigg(\frac{1}{p^{n+1}} \sum_{\substack{a=0\\(a,p)=1}}^{p^{n+1}-1} \Big(a - \frac{p^{n+1}-p}{2}\Big)\tau\sigma'_a\sigma''_a(\theta_n)\Bigg).$$

Jedes a der durchlaufenen Menge lässt sich eindeutig als $a = b+kp$ mit $1 \le b \le p-1$ und $0 \le k \le p^n - 1$ schreiben. Mit dieser Schreibweise erhält man

$$\sigma_a(\zeta_0) = \sigma_a(\zeta_n^{p^n}) = \zeta_n^{ap^n} = \zeta_0^a = \zeta_0^{b+kp} = \zeta_0^b = \sigma'_a(\zeta_0).$$

Der Automorphismus σ'_a entspricht demnach für $a = b+kp$ dem Automorphismus $\tau_b \in G(K_0/\mathbb{Q}_p)$, der durch $\tau_b(\zeta_0) = \zeta_0^b$ charakterisiert ist. Der Anteil σ''_a von σ_a mit $a = b + kp$ werde mit $\tau_k \in G(K_n/K_0)$ bezeichnet. Mit Gleichung (6.11) folgt

$$\begin{aligned}
P_\chi\big(\tau(\mu_n)\big) &= P_\chi\Bigg(\frac{1}{p^{n+1}} \sum_{k=0}^{p^n-1}\sum_{b=1}^{p-1} \Big(b + kp - \frac{p^{n+1}-p}{2}\Big)\tau\tau_b\tau_k(\theta_n)\Bigg)\\
&= \frac{1}{p^{n+1}} \sum_{k=0}^{p^n-1}\sum_{b=1}^{p-1} \Big(b + kp - \frac{p^{n+1}-p}{2}\Big)P_\chi\big(\tau\tau_b\tau_k(\theta_n)\big)\\
&= \frac{1}{p^{n+1}} \sum_{k=0}^{p^n-1}\sum_{b=1}^{p-1} \Big(b + kp - \frac{p^{n+1}-p}{2}\Big)\chi(\tau_b)P_\chi\big(\tau\tau_k(\theta_n)\big)\\
&= \frac{1}{p^{n+1}} \sum_{k=0}^{p^n-1} P_\chi\big(\tau\tau_k(\theta_n)\big) \sum_{b=1}^{p-1} b\chi(\tau_b)\\
&\qquad + \frac{1}{p^n} \sum_{k=0}^{p^n-1} kP_\chi\big(\tau\tau_k(\theta_n)\big) \sum_{b=1}^{p-1} \chi(\tau_b)\\
&\qquad - \frac{1}{p^n}\frac{p^n-1}{2} \sum_{k=0}^{p^n-1} P_\chi\big(\tau\tau_k(\theta_n)\big) \sum_{b=1}^{p-1} \chi(\tau_b). \qquad (6.13)
\end{aligned}$$

Nun wird für χ eine Fallunterscheidung vorgenommen. Im Fall $\chi = \omega^{-1}$ gilt wie im Beweis zu Satz 6.10 die Relation $\sum_{b=1}^{p-1} b\chi(\tau_b) \in \mathbb{Z}_p$, und nach Lemma 6.1 ist $\sum_{b=1}^{p-1} \chi(\tau_b) = 0$. Für $\chi \ne 1, \omega^{-1}$ gilt $\sum_{b=1}^{p-1} b\chi(\tau_b) \in p\,\mathbb{Z}_p$ und $\sum_{b=1}^{p-1} \chi(\tau_b) \in \mathbb{Z}_p$. Insgesamt ergibt sich mit $\rho := \tau\tau_k \in G(K_n/K_0)$

$$P_\chi\big(\tau(\mu_n)\big) \in \begin{cases} \displaystyle\sum_\rho \frac{1}{p^{n+1}}\,\mathbb{Z}_p P_{\omega^{-1}}\big(\rho(\theta_n)\big), & \text{für } \chi = \omega^{-1},\\[2ex] \displaystyle\sum_\rho \frac{1}{p^n}\,\mathbb{Z}_p P_\chi\big(\rho(\theta_n)\big), & \text{für } \chi \ne 1, \omega^{-1}. \end{cases}$$

Somit erhält man mit $\rho,\ \tau \in G(K_n/K_0)$ für die Eigenräume

$$\begin{aligned}
\mathfrak{X}_n(\chi) &= \sum_\tau \mathbb{Z}_p P_\chi\big(\tau(\mu_n)\big) + \sum_\rho \mathbb{Z}_p P_\chi\big(\rho(\theta_n)\big) \\
&= \begin{cases} \displaystyle\sum_\tau \mathbb{Z}_p \sum_\rho \frac{1}{p^{n+1}} \mathbb{Z}_p P_{\omega^{-1}}\big(\rho(\theta_n)\big) + \sum_\rho \mathbb{Z}_p P_{\omega^{-1}}\big(\rho(\theta_n)\big), & \text{für } \chi = \omega^{-1}, \\ \displaystyle\sum_\tau \mathbb{Z}_p \sum_\rho \frac{1}{p^{n}} \mathbb{Z}_p P_{\chi}\big(\rho(\theta_n)\big) + \sum_\rho \mathbb{Z}_p P_{\chi}\big(\rho(\theta_n)\big), & \text{für } \chi \neq 1, \omega^{-1}, \end{cases} \\
&= \begin{cases} \displaystyle\sum_\rho \Big(\Big(\sum_\tau \mathbb{Z}_p \Big) \frac{1}{p^{n+1}} \mathbb{Z}_p + \mathbb{Z}_p \Big) P_{\omega^{-1}}\big(\rho(\theta_n)\big), & \text{für } \chi = \omega^{-1}, \\ \displaystyle\sum_\rho \Big(\Big(\sum_\tau \mathbb{Z}_p \Big) \frac{1}{p^{n}} \mathbb{Z}_p + \mathbb{Z}_p \Big) P_{\chi}\big(\rho(\theta_n)\big), & \text{für } \chi \neq 1, \omega^{-1}, \end{cases}
\end{aligned}$$

und schließlich

$$\mathfrak{X}_n(\chi) = \begin{cases} \displaystyle\sum_\rho \frac{1}{p^{n+1}} \mathbb{Z}_p P_{\omega^{-1}}\big(\rho(\theta_n)\big), & \text{für } \chi = \omega^{-1}, \\ \displaystyle\sum_\rho \frac{1}{p^{n}} \mathbb{Z}_p P_{\chi}\big(\rho(\theta_n)\big), & \text{für } \chi \neq 1, \omega^{-1}. \end{cases}$$

Nun wird der Fall $\chi = 1$ behandelt. Sei wie oben $x = \sum_\sigma c_\sigma \sigma(\mu_n) + \sum_\sigma d_\sigma \sigma(\theta_n)$ ein beliebiges Element aus $\mathfrak{X}_n$. Dann gilt mit $\sigma = \sigma_1\sigma_2 \in G \times G(K_n/K_0)$

$$\begin{aligned}
P_1(x) &= \sum_\sigma c_\sigma P_1\big(\sigma_2(\mu_n)\big) + \sum_\sigma d_\sigma P_1\big(\sigma_2(\theta_n)\big) \\
&= \sum_{\sigma_2} \Big(\sum_{\sigma_1} c_{\sigma_1\sigma_2} \Big) P_1\big(\sigma_2(\mu_n)\big) + \sum_{\sigma_2} \Big(\sum_{\sigma_1} d_{\sigma_1\sigma_2} \Big) P_1\big(\sigma_2(\theta_n)\big) \\
&= \sum_{\sigma_2} {c'}_{\sigma_2} P_1\big(\sigma_2(\mu_n)\big) + \sum_{\sigma_2} {d'}_{\sigma_2} P_1\big(\sigma_2(\theta_n)\big) \\
&\in \Big\{ \sum_\tau {c'}_\tau P_1\big(\tau(\mu_n)\big) + \sum_\tau {d'}_\tau P_1\big(\tau(\theta_n)\big),\ \tau \in G(K_n/K_0),\ \sum_\tau {d'}_\tau = 0 \Big\}
\end{aligned}$$

Jedes Element der Menge in der letzten Zeile läßt sich als $P_1(y)$ schreiben mit

$$y = \sum_{\tau \in G(K_n/K_0)} c_\tau \tau(\mu_n) + \sum_{\tau \in G(K_n/K_0)} d_\tau \tau(\theta_n), \quad c_\tau, d_\tau \in \mathbb{Z}_p, \quad \sum_\tau d_\tau = 0.$$

Somit erhält man

$$\mathfrak{X}_n(1) = \Big\{ \sum_\tau c_\tau P_1\big(\tau(\mu_n)\big) + \sum_\tau d_\tau P_1\big(\tau(\theta_n)\big),\ \tau \in G(K_n/K_0),\ \sum_\tau d_\tau = 0 \Big\}.$$

Sei nun $y = \sum_\tau c_\tau \tau(\mu_n) + \sum_\tau d_\tau \tau(\theta_n)$ ein Element der oben beschriebenen Gestalt aus $\mathfrak{X}_n$. Wertet man Formel 6.13, welche auch im Fall $\chi = 1$ gilt, im Fall $\chi = 1$

aus, so erhält man

$$\begin{aligned} P_1\big(\tau(\mu_n)\big) &= \frac{1}{p^{n+1}} \sum_{k=0}^{p^n-1} P_1\big(\tau\tau_k(\theta_n)\big) \cdot \frac{p(p-1)}{2} \\ &\quad + \frac{1}{p^n} \sum_{k=0}^{p^n-1} k P_1\big(\tau\tau_k(\theta_n)\big)(p-1) \\ &\quad - \frac{1}{p^n}\frac{p^n-1}{2} \sum_{k=0}^{p^n-1} P_1\big(\tau\tau_k(\theta_n)\big)(p-1) \\ &= \frac{1}{p^n} \sum_{k=0}^{p^n-1} (p-1)\Big(k+1-\frac{p^n}{2}\Big) P_1\big(\tau\tau_k(\theta_n)\big) \\ &= \frac{1}{p^n} \sum_{\rho\in G(K_n/K_0)} c_{\rho,\tau} P_1\big(\rho(\theta_n)\big) \end{aligned}$$

mit $c_{\rho,\tau} = (p-1)\big(k+1-\frac{p^n}{2}\big)$ falls $\tau^{-1}\rho : \zeta_n \mapsto \zeta_n^{1+kp}$. Wendet man P_1 auf obiges y an und verwendet das Ergebnis der letzten Rechnung, so ergibt sich

$$\begin{aligned} P_1(y) &= \sum_\tau c_\tau P_1\big(\tau(\mu_n)\big) + \sum_\tau d_\tau P_1\big(\tau(\theta_n)\big) \\ &= \sum_\tau c_\tau \cdot \frac{1}{p^n} \sum_\rho c_{\rho,\tau} P_1\big(\rho(\theta_n)\big) + \sum_\rho d_\rho P_1\big(\rho(\theta_n)\big) \\ &= \sum_\rho \bigg(\frac{1}{p^n}\Big(\sum_\tau c_{\rho,\tau}c_\tau\Big) + d_\rho\bigg) P_1\big(\rho(\theta_n)\big) \\ &= \frac{1}{p^n} \sum_\rho \bigg(\Big(\sum_\tau c_{\rho,\tau}c_\tau\Big) + p^n d_\rho\bigg) P_1\big(\rho(\theta_n)\big) \\ &\in \frac{1}{p^n} \sum_\rho \mathbb{Z}_p P_1\big(\rho(\theta_n)\big). \end{aligned}$$

Daraus folgt

$$P_1(\mathfrak{X}_n) \subseteq \frac{1}{p^n} \sum_{\rho\in G(K_n/K_0)} \mathbb{Z}_p P_1\big(\rho(\theta_n)\big).$$

Sei nun $z = \frac{1}{p^n}\sum_\rho \bar{c}_\rho P_1\big(\rho(\theta_n)\big)$ ein beliebiges Element aus der rechten Menge. Es soll gezeigt werden, dass es ein Element $y \in \mathfrak{X}_n$ gibt mit $z = P_1(y)$. Hat y wie oben die Gestalt $y = \sum_\tau c_\tau\tau(\mu_n) + \sum_\tau d_\tau\tau(\theta_n),\ \tau \in G(K_n/K_0)$, so muss für jedes $\rho \in G(K_n/K_0)$ die Gleichung

$$\bar{c}_\rho = \sum_\tau c_{\rho,\tau}c_\tau + p^n d_\rho$$

erfüllt sein. Allgemein läßt sich das Problem so formulieren: Seien eine $m \times m$-Matrix A und ein m-komponentiger Vektor b gegeben. Gesucht sind Vektoren c und d, so dass

$$b = Ac + d.$$

Diese Gleichung ist äquivalent zu der Gleichung

$$b = (A|E)\,u,\ E = m \times m \text{ - Einheitsmatrix, } u = \binom{c}{d}.$$

Diese Gleichung hat eine Lösung, denn die Matrix $(A|E)$ hat vollen Rang. In unserem Fall muss der Vektor d aber noch die zusätzliche Bedingung erfüllen, dass die Summe seiner Einträge gleich Null ist. Dazu wird die Matrix $(A|E)$ um eine unterste Zeile $(0,\ldots,0,1,\ldots,1)$ aus m Nullen und m Einsen und der Vektor b um den letzten Eintrag Null ergänzt. Die Frage ist nun, ob die neue Gleichung

$$\begin{pmatrix} A & E \\ 0..0 & 1..1 \end{pmatrix} \binom{c}{d} = \binom{b}{0}$$

eine Lösung hat, ob also die Matrix $\begin{pmatrix} A & E \\ 0..0 & 1..1 \end{pmatrix}$ vollen Rang hat. In der rechten Hälfte dieser Matrix gilt, dass die Summe der oberen m Zeilen die unterste Zeile ergibt. Die Matrix hat vollen Rang, wenn diese Bedingung in der linken Hälfte verletzt ist. Dazu ist es notwendig, die genaue Struktur der Einträge der Matrix A im konkreten Fall zu ermitteln.

Sei A die $p^n \times p^n$-Matrix mit den Einträgen $c_{\rho,\tau}$. Jedes $\sigma \in G(K_n/\mathbb{Q}_p)$ ist durch seine Wirkung $\zeta_n \mapsto \zeta_n^a$ eindeutig festgelegt, wobei a eindeutig als $a = b + kp$ mit $1 \le b \le p-1$ und $0 \le k \le p^n - 1$ geschrieben werden kann. Die Elemente von $G(K_n/K_0)$ sind durch $b = 1$ charakterisiert. Wirkt τ^{-1} auf ζ_n durch Potenzierung mit $1+ip$ und ρ durch Potenzierung mit $1+jp$, so wirkt $\tau^{-1}\rho$ durch Potenzierung mit $(1+ip)(1+jp) = 1 + (i+j+ijp)p$. Die Zahl $c_{\rho,\tau}$ hat in diesem Fall also den Wert

$$c_{\rho,\tau} = (p-1)\Big(i + j + ijp + 1 - \frac{p^n}{2}\Big) =: a_{ij}.$$

Es ist zu zeigen, dass es ein j gibt, so dass

$$\sum_{i=0}^{p^n-1} a_{ij} \neq 0.$$

Sei $j = 0$. Dann gilt

$$\begin{aligned} \sum_{i=0}^{p^n-1} a_{i0} &= (p-1) \sum_{i=0}^{p^n-1} \Big(i + 1 - \frac{p^n}{2}\Big) \\ &= (p-1)\Big(\frac{p^n(p^n-1)}{2} + p^n\Big(1 - \frac{p^n}{2}\Big)\Big) = \frac{(p-1)p^n}{2} \neq 0. \end{aligned}$$

Somit ist gezeigt, dass die Matrix $\begin{pmatrix} A & E \\ 0..0 & 1..1 \end{pmatrix}$ vollen Rang hat, dass es also zu jedem $z \in \frac{1}{p^n}\sum_\rho \mathbb{Z}_p P_1\big(\rho(\theta_n)\big)$ ein $y \in \mathfrak{X}_n$ mit $P_1(y) = z$ gibt. Daraus folgt schließlich

$$\mathfrak{X}_n(1) = \frac{1}{p^n} \sum_{\rho \in G(K_n/K_0)} \mathbb{Z}_p P_1\big(\rho(\theta_n)\big).$$

Zu guter letzt ist noch nachzuweisen, dass die Eigenräume alle den $\mathbb{Z}_p$-Rang p^n haben. Zunächst ist klar, dass der $\mathbb{Z}_p$-Rang mindestens p^n ist. Sei χ ein beliebiger Charakter von G. Nach Multiplikation mit p^n oder p^{n+1} ist zu zeigen, dass aus der Gleichung

$$\sum_{\rho\in G(K_n/K_0)} c_\rho P_\chi\big(\rho(\theta_n)\big) = 0$$

die Gleichung $c_\rho = 0$ für alle $\rho \in G(K_n/K_0)$ folgt. Schreibt man P_χ aus und multipliziert mit $p-1$, so erhält man aus obiger Gleichung

$$\sum_{\substack{\rho\in G(K_n/K_0)\\ \sigma\in G}} c_\rho\, \chi(\sigma^{-1})\, \sigma\rho(\theta^n) = 0.$$

Durchlaufen σ die Gruppe $G = G(K_0/\mathbb{Q}_p)$ und ρ die Gruppe $G(K_n/K_0)$, so durchläuft $\sigma\rho$ die gesamte Gruppe $G(K_n/\mathbb{Q}_p)$. Nach [Iwa1], § 1, Prop. 7, bilden die Elemente $\sigma'(\theta_n)$, $\sigma' \in G(K_n/\mathbb{Q}_p)$, eine Normalbasis von $K_n/\mathbb{Q}_p$. Damit folgt das Verschwinden aller $c_\rho\chi(\sigma^{-1})$ in obiger Gleichung. Da die $\chi(\sigma^{-1})$ verschieden von Null sind, folgt das Verschwinden aller c_ρ. Somit ist gezeigt, dass alle Eigenräume $\mathfrak{X}_n(\chi)$ den $\mathbb{Z}_p$-Rang p^n haben.

QED

Nachdem $\mathfrak{X}_n$ in $(p-1)$ Eigenräume vom $\mathbb{Z}_p$-Rang p^n zerlegt wurde, folgt

$$\mathrm{rk}_{\mathbb{Z}_p}\mathfrak{X}_n = (p-1)p^n.$$

Für die Eigenräume von X_n gilt der folgende Satz.

Satz 6.24 *Die Eigenräume $X_n(\chi)$ haben für $\chi \neq 1$ den $\mathbb{Z}_p$-Rang p^n. Für $\chi = 1$ gilt*

$$X_n(1) \cong X_n\big/(1+\mathfrak{m}_n)' \times (1+\mathfrak{m}_n)'(1),$$

wobei $(1+\mathfrak{m}_n)'(1) \subseteq \big\{y \in (1+\mathfrak{m}_n)' : N_{n0}(y) = 1\big\}$.

Beweis: Sei $G := G(K_0/\mathbb{Q}_p)$. Für $\chi \in G^\times$ gilt

$$\begin{aligned}\nu_n\big(\widetilde{P}_\chi(\pi_n)\big) &= \frac{1}{p-1}\sum_{\sigma\in G}\chi\sigma\nu_n\big(\sigma^{-1}(\pi_n)\big)\\ &= \frac{1}{p-1}\sum_{\sigma\in G}\chi(\sigma)\nu_n(\pi_n) = \begin{cases}1, & \text{falls } \chi = 1,\\ 0, & \text{sonst.}\end{cases}\end{aligned}$$

Somit ist $\widetilde{P}_1$ der einzige Projektor, der in die Untergruppe $\langle\langle\pi_n\rangle\rangle$ projiziert. Es werde die exakte Sequenz

$$1 \to (1+\mathfrak{m}_n)' \to X_n \to X_n\big/(1+\mathfrak{m}_n)' \to 1 \tag{6.14}$$

betrachtet. Die Faktorgruppe $X_n/(1+\mathfrak{m}_n)'$ ist als $\mathbb{Z}_p$-Modul isomorph zu $\langle\langle \pi_n \rangle\rangle$, hat also den $\mathbb{Z}_p$-Rang 1.

Durch Anwendung von $\widetilde{P}_\chi$ geht obige exakte Sequenz (6.14) in die exakte Sequenz

$$1 \to \widetilde{P}_\chi(1+\mathfrak{m}_n)' \to \widetilde{P}_\chi(X_n) \to \widetilde{P}_\chi\big(X_n/(1+\mathfrak{m}_n)'\big) \to 1 \qquad (6.15)$$

über (vgl. Beweis zu Satz 6.15). Hier hat die Gruppe $\widetilde{P}_\chi\big(X_n/(1+\mathfrak{m}_n)'\big)$ entweder den $\mathbb{Z}_p$-Rang 0 oder 1.

Sei $\chi \neq 1$. Da die Projektoren $\widetilde{P}_\chi$ nach obiger Rechnung für $\chi \neq 1$ nicht in die Komponente $X_n/(1+\mathfrak{m}_n)'$ projizieren, gilt die Beziehung $\widetilde{P}_\chi\big(X_n/(1+\mathfrak{m}_n)'\big) = 1$. Daraus erhält man $X_n(\chi) \cong (1+\mathfrak{m}_n)'(\chi)$. Nach Theorem 13.54 und der dem Theorem vorangegangenen Bemerkung in [Was], Chap. 13, § 13.8, gilt

$$\widetilde{P}_\chi(1+\mathfrak{m}_n)' = \widetilde{P}_\chi(1+\mathfrak{m}_n)$$

und $\mathrm{rk}_{\mathbb{Z}_p}(1+\mathfrak{m}_n)(\chi) = p^n$. Somit haben die Eigenräume $\widetilde{P}_\chi(1+\mathfrak{m}_n)'$ für $\chi \neq 1$ alle den $\mathbb{Z}_p$-Rang p^n,

$$\mathrm{rk}_{\mathbb{Z}_p} X_n(\chi) = \mathrm{rk}_{\mathbb{Z}_p}(1+\mathfrak{m}_n)'(\chi) = p^n.$$

Für $\chi = 1$ erhält man aus (6.15) die exakte Sequenz

$$1 \to (1+\mathfrak{m}_n)'(1) \to X_n(1) \to X_n/(1+\mathfrak{m}_n)'(1) \to 1,$$

und daraus folgt $X_n(1) \cong X_n/(1+\mathfrak{m}_n)'(1) \times (1+\mathfrak{m}_n)'(1)$. Wegen

$$\mathrm{rk}_{\mathbb{Z}_p}\big(X_n/(1+\mathfrak{m}_n)'(1)\big) = 1 = \mathrm{rk}_{\mathbb{Z}_p}\big(\langle\langle \pi_n \rangle\rangle\big) = \mathrm{rk}_{\mathbb{Z}_p}\big(X_n/(1+\mathfrak{m}_n)'\big)$$

folgt $X_n/(1+\mathfrak{m}_n)'(1) \cong X_n/(1+\mathfrak{m}_n)'$ und somit

$$X_n(1) \cong X_n/(1+\mathfrak{m}_n)' \times (1+\mathfrak{m}_n)'(1).$$

Es verbleibt, die Enthaltenseinsrelation $(1+\mathfrak{m}_n)'(1) \subseteq \{y \in (1+\mathfrak{m}_n)' \colon N_{n0}(y) = 1\}$ nachzuweisen. Zu diesem Zweck gelte in den folgenden Rechnungen immer $\sigma \in G(K_0/\mathbb{Q}_p)$ und $\tau \in G(K_n/K_0)$. Zunächst erhält man für $x \in (1+\mathfrak{m}_n)'$ die Gleichheit $\widetilde{P}_1(x) = \big(\prod_\sigma \sigma^{-1}(x)\big)^{\frac{1}{p-1}} = \big(\prod_\sigma \sigma(x)\big)^{\frac{1}{p-1}}$. Dies impliziert

$$N_{n0}\big(\widetilde{P}_1(x)\big) = N_{n0}\Big(\prod_\sigma \sigma(x)\Big)^{\frac{1}{p-1}} = \Big(\prod_\tau \Big(\prod_\sigma \sigma(x)\Big)\Big)^{\frac{1}{p-1}} = \Big(\prod_{\tau,\sigma} \tau\sigma(x)\Big)^{\frac{1}{p-1}}.$$

Durchlaufen σ und τ die angegebenen Mengen, so durchläuft das Produkt $\tau\sigma$ die Gruppe $G(K_n/\mathbb{Q}_p)$, so dass

$$N_{n0}\big(\widetilde{P}_1(x)\big) = N_n(x)^{\frac{1}{p-1}} = 1.$$

Damit sind alle Aussagen des Satzes bewiesen.

QED

Wie in Lemma 6.17 kann man zeigen, dass das Diagramm

$$\begin{array}{ccc} X_n & \xrightarrow{\psi_n} & \mathfrak{X}_n/p^{n+1}\mathfrak{X}_n \\ \Big\downarrow{\scriptstyle \widetilde{P}_\chi} & & \Big\downarrow{\scriptstyle P_{\chi\omega^{-1}}} \\ X_n(\chi) & \xrightarrow[\psi_n(\chi)]{} & \mathfrak{X}_n/p^{n+1}\mathfrak{X}_n(\chi\omega^{-1}) \end{array}$$

kommutativ ist. Mit diesem Resultat kann der nächste Satz bewiesen werden.

Satz 6.25 *Es gilt*

$$\psi_n\big(\widetilde{P}_1(\pi_n)\big) = -\frac{1}{p^{n+1}} \sum_{\tau\in G(K_n/K_0)} \Big(\sum_{b=1}^{p-1} b\omega^{-1}(\sigma_b)\Big) P_{\omega^{-1}}\big(\tau(\theta_n)\big)$$

und

$$\psi_n\big(\widetilde{P}_\chi(\zeta_n)\big) = \begin{cases} -\dfrac{1}{p^{n+1}}, & \textit{falls } \chi = \omega, \\ 0, & \textit{sonst.} \end{cases}$$

Aufgrund des Ergebnisses von Satz 6.24 ist nur von Interesse, das Bild von $\widetilde{P}_1(\pi_n)$ unter ψ_n zu kennen.

Beweis: Unter Ausnutzung der Kommutativität des obigen Diagramms folgt

$$\psi_n\big(\widetilde{P}_1(\pi_n)\big) = P_{\omega^{-1}}\big(\psi_n(\pi_n)\big) \quad \text{und} \quad \psi_n\big(\widetilde{P}_\chi(\zeta_n)\big) = P_{\chi\omega^{-1}}\big(\psi_n(\zeta_n)\big).$$

Für $m \geq 2n+1$ ist π_m ein Urbild von π_n unter der Abbildung N_{mn}, und nach Gleichung (5.8) von Seite 53 gilt $\delta_m(\pi_m) = \frac{\zeta_m}{\pi_m}$. Somit folgt unter Verwendung des Beweises von Satz 5.12

$$\psi_n(\pi_n) = -\frac{1}{p^{m+1}} S_{mn}\big(\delta_m(\pi_m)\big) = -\frac{1}{p^{m+1}} S_{mn}\Big(\frac{\zeta_m}{\pi_m}\Big) = -\frac{p^{m-n}}{p^{m+1}} \frac{\zeta_n}{\pi_n} = -\mu_n.$$

Schließlich ergibt sich daraus mit Gleichung (6.13) von Seite 102

$$\psi_n\big(\widetilde{P}_1(\pi_n)\big) = -P_{\omega^{-1}}(\mu_n) = -\frac{1}{p^{n+1}} \sum_{\tau\in G(K_n/K_0)} \Big(\sum_{b=1}^{p-1} b\omega^{-1}(\sigma_b)\Big) P_{\omega^{-1}}\big(\tau(\theta_n)\big).$$

Dies entspricht der Basisdarstellung von $-P_{\omega^{-1}}(\mu_n) \in \mathfrak{X}_n(\omega^{-1})$ (vgl. Satz 6.23 und Beweis).

Für ζ_n ist ζ_m ein Urbild unter N_{mn} und unter Verwendung von Gleichung (5.7) von Seite 53 folgt $\delta_m(\zeta_m) = -1$. Damit ist mit $G := G(K_0/\mathbb{Q}_p)$

$$\psi_n\big(\widetilde{P}_\chi(\zeta_n)\big) = P_{\chi\omega^{-1}}\Big(-\frac{1}{p^{n+1}}\Big) = -\frac{1}{p^{n+1}}\,\frac{1}{p-1}\sum_{\sigma\in G}\chi\omega^{-1}(\sigma)\sigma^{-1}(1)$$
$$= \begin{cases} -\dfrac{1}{p^{n+1}}, & \text{falls } \chi = \omega, \\ 0, & \text{sonst.} \end{cases}$$

QED

Zuletzt sei noch, analog zu Satz 6.20, eine allgemeine Formel für $P_{\chi\omega^{-1}}\big(\psi_n(x)\big)$, $x \in (1+\mathfrak{m}_n)'$, angegeben. Dazu sei an den projektiven Limes

$$U = \varprojlim_n (1+\mathfrak{m}_n)'$$

erinnert. Die Übergangsabbildungen bei der Bildung des projektiven Limes sind die Normabbildungen $N_{mn} : (1+\mathfrak{m}_m)' \to (1+\mathfrak{m}_n)'$. Für jedes Element $u = (\ldots, x_m, \ldots, x_1, x_0) \in U$ gibt es eine eindeutig bestimmte Potenzreihe $f_u \in \mathbb{Z}_p[[T]]$ mit $f_u(\pi_m) = x_m$ für alle $m \geq 0$.

Satz 6.26 *Seien $m \geq 2n+1$, $x \in (1+\mathfrak{m}_n)'$, $u \in U$ ein Element des projektiven Limes, das zu x gehört, und $f_u \in \mathbb{Z}_p[[T]]$ die eindeutig bestimmte Potenzreihe mit $f_u(\pi_n) = x$. Dann gilt*

$$P_{\chi\omega^{-1}}\big(\psi_n(x)\big) = -\frac{1}{p^{m+1}}\,\frac{1}{p-1}\sum_{\rho\in G(K_m/K_n)\times H}\chi\omega^{-1}(\rho)\left((1-T)\frac{f_u'(T)}{f_u(T)}\right)\Bigg|_{T=\rho^{-1}(\pi_m)}$$

mit $G(K_0/\mathbb{Q}_p) \cong H \subseteq G(K_m/\mathbb{Q}_p)$.

Man erkennt, dass diese Gleichung analog zu der Formel in Satz 6.20 aufgebaut ist. Allerdings erstreckt sich der Summationsbereich hier nur über eine Untergruppe von $G(K_m/\mathbb{Q}_p)$.

Beweis: Sei $x_m = f_u(\pi_m)$ ein Urbild von x unter der Abbildung N_{mn}. Dann ergibt sich die Darstellung

$$\delta_m(x_m) = \frac{\zeta_m}{x_m}f_u'(\pi_m) = \left((1-T)\frac{f_u'(T)}{f_u(T)}\right)\Bigg|_{T=\pi_m}$$

und es folgt

$$P_{\chi\omega^{-1}}\big(\psi_n(x)\big) = -\frac{1}{p^{m+1}}\,P_{\chi\omega^{-1}}\left(S_{mn}\left(\left((1-T)\frac{f_u'(T)}{f_u(T)}\right)\Bigg|_{T=\pi_m}\right)\right).$$

Über das Diagramm

$$\begin{array}{ccccccccc} & & & & 1 & & & & \\ & & & & \downarrow & & & & \\ & & & & G(K_m/K_0) & & & & \\ & & & & \downarrow & & & & \\ 1 & \longrightarrow & G(K_m/K_n) & \longrightarrow & G(K_m/\mathbb{Q}_p) & \longrightarrow & G(K_n/\mathbb{Q}_p) & \longrightarrow & 1\ , \\ & & \tau & & \downarrow & & & & \\ & & & & \sigma \in\ G(K_0/\mathbb{Q}_p) & & & & \\ & & & & \downarrow & & & & \\ & & & & 1 & & & & \end{array}$$

dessen Zeile und Spalte exakt sind, können Elemente $\tau \in G(K_m/K_n)$ und $\sigma \in G(K_0/\mathbb{Q}_p)$ als Elemente von $G(K_m/\mathbb{Q}_p)$ aufgefasst werden. Dabei wird die Gruppe $G(K_0/\mathbb{Q}_p)$ mit der Untergruppe $H \subseteq G(K_m/\mathbb{Q}_p)$ der Elemente, deren Ordnung ein Teiler von $p-1$ ist, identifiziert. Daraus ergibt sich die Enthaltenseinsrelation $G(K_m/K_n) \times G(K_0/\mathbb{Q}_p) \subseteq G(K_m/\mathbb{Q}_p)$.

Für beliebiges $y \in K_m$ gilt

$$\begin{aligned} P_{\chi\omega^{-1}}\big(S_{mn}(y)\big) &= P_{\chi\omega^{-1}}\Big(\sum_\tau \tau(y)\Big) = \frac{1}{p-1}\sum_\sigma \chi\omega^{-1}(\sigma)\sigma^{-1}\Big(\sum_\tau \tau(y)\Big) \\ &= \frac{1}{p-1}\sum_\sigma\sum_\tau \chi\omega^{-1}(\sigma)\sigma^{-1}\tau(y) = \frac{1}{p-1}\sum_\rho \chi\omega^{-1}(\rho)\rho^{-1}(y), \end{aligned}$$

wobei ρ die Untergruppe $G(K_m/K_n) \times G(K_0/\mathbb{Q}_p) = G(K_m/K_n) \times H$ durchläuft und $\chi\omega^{-1}(\rho)$ als $\chi\omega^{-1}(\sigma)$ für $\rho \equiv \sigma \mod G(K_m/K_n)$ definiert ist. Mit diesem Ergebnis kann man die obige Rechnung weiterführen

$$P_{\chi\omega^{-1}}\big(\psi_n(x)\big) = -\frac{1}{p^{m+1}}\,\frac{1}{p-1}\sum_{\rho\in G(K_m/K_n)\times H} \chi\omega^{-1}(\rho)\left((1-T)\frac{f_u'(T)}{f_u(T)}\right)\Bigg|_{T=\rho^{-1}(\pi_m)}.$$

QED

Die Resultate dieses Abschnitts haben gezeigt, dass man durch Beschränkung auf Charaktere von $G(K_0/\mathbb{Q}_p)$ das Problem der Zerlegung von ψ_n zwar vereinfacht, man dafür aber nicht mehr so "schöne" Ergebnisse bekommt wie im Fall $n = 0$. Zum Beispiel haben die erhaltenen Eigenräume nicht mehr den $\mathbb{Z}_p$-Rang 1 und man kann die Erzeugenden der Eigenräume $X_n(\chi)$ nicht so leicht angeben.

Es ist zu vermuten, dass der Eigenraum $X_n(1)$ ebenfalls, wie die anderen Eigenräume $X_n(\chi)$, den $\mathbb{Z}_p$-Rang p^n hat, so dass alle Eigenräume $X_n(\chi)$ und $\mathfrak{X}_n(\chi)$

den gleichen Rang haben und für X_n und $\mathfrak{X}_n$ gilt

$$\mathrm{rk}_{\mathbb{Z}_p} X_n = \mathrm{rk}_{\mathbb{Z}_p} \mathfrak{X}_n = (p-1)p^n.$$

Außerdem ist anzunehmen, dass sogar die Gleichheit

$$(1+\mathfrak{m}_n)'(1) = \{y \in (1+\mathfrak{m}_n)' : N_{n0}(y) = 1\}$$

gilt (vgl. Satz 6.24). Daraus würde sich ergeben, dass $\{y \in (1+\mathfrak{m}_n)' : N_{n0}(y) = 1\}$ den $\mathbb{Z}_p$-Rang $p^n - 1$ hat.

Bezeichnungen

$\mathbb{Q}$	... Körper der rationalen Zahlen
$\mathbb{Z}$	... Ring der ganzen Zahlen
$(\,.\,,\,.\,)$	... größter gemeinsamer Teiler
$\mathbb{Q}_p$	... Körper der p-adischen Zahlen
$\mathbb{Z}_p$	... Ring der ganzen p-adischen Zahlen
v_p	... p-adische Bewertung auf $\mathbb{Q}_p$
$\widehat{\mathbb{Z}}$	... projektiver Limes der Gruppen $\mathbb{Z}/n\mathbb{Z}$
$K/\mathbb{Q}_p$	... endliche Erweiterung lokaler Körper
$\nu_K : K \twoheadrightarrow \mathbb{Z}$	... normierte Bewertung auf K
$\mathcal{O}_K$	... $= \{x \in K : \nu_K(x) \geq 0\}$ Bewertungsring von K
π_K	... Primelement in $\mathcal{O}_K$, d.h. $\nu_K(\pi_K) = 1$
$\mathfrak{m}_K$	... $= \{x \in \mathcal{O}_K : \nu_K(x) > 0\} = \pi_K \mathcal{O}_K$ maximales Ideal von $\mathcal{O}_K$
$F/\mathbb{Q}$	... endliche Zahlkörper-Erweiterung
$\mathcal{O}_F$	... Ring der ganzen Zahlen von F
$\mathfrak{p}$	... ein Primideal in $\mathcal{O}_F$
$v_\mathfrak{p}$	... zu $\mathfrak{p}$ gehörige Bewertung
$F_\mathfrak{p}$	... Komplettierung von F bezüglich $v_\mathfrak{p}$
$\mathcal{O}_\mathfrak{p}$	... der Bewertungsring von $F_\mathfrak{p}$
$G(L/K)$	... Galoisgruppe einer Galoiserweiterung L/K
$N_{L/K} : L \to K$	... Normabbildung $N_{L/K}(x) = \prod_{\sigma \in G(L/K)} \sigma x$
$S_{L/K} : L \to K$	... Spurabbildung $S_{L/K}(x) = \sum_{\sigma \in G(L/K)} \sigma x$
$\mu_m,\ \mu_m(K)$	... Gruppe der m-ten Einheitswurzeln (im Körper K)

ζ_n	... primitive p^{n+1}-te Einheitswurzel
K_n	... $:= \mathbb{Q}_p(\zeta_n)$
ν_n	... normierte Bewertung auf K_n
$\mathcal{O}_n$	... Bewertungsring
π_n	... $:= 1 - \zeta_n$ Primelement in $\mathcal{O}_n$
$\mathfrak{m}_n$	... $= \pi_n \mathcal{O}_n$ maximales Ideal
$\mathfrak{D}_n$	... die Differente von $K_n/\mathbb{Q}_p$
$\eta_i^{(n)}$	... $:= 1 - \pi_n^i$
$N_n, S_n : K_n \to \mathbb{Q}_p$	... Norm- bzw. Spurabbildung
$N_{mn}, S_{mn} : K_m \to K_n$	... Norm- bzw. Spurabbildung, für $m > n$
$(\,.\,,\,.\,)_m$	... m-tes Hilbertsymbol
$(\,.\,,\,.\,)_n$	... p^{n+1}-tes Hilbertsymbol
$[\,.\,,\,.\,]_n$	... Exponent für das p^{n+1}-te Hilbertsymbol
$\langle\,.\,,\,.\,\rangle_n$	... Produkt, definiert in Definition 5.13
$G^\times$	... Charaktergruppe der Gruppe G
ω	... Teichmüller-Charakter auf der Gruppe $G(K_0/\mathbb{Q}_p)$
$P_\chi,\ \widetilde{P}_\chi$	... additiver bzw. multiplikativer Projektor zum Charakter χ
μ_n	... $:= \dfrac{1}{p^{n+1}} \dfrac{\zeta_n}{\pi_n}$
θ_n	... $:= \dfrac{1}{p^{n+1}} \displaystyle\sum_{j=0}^{n} \zeta_j^{-1}$

Literaturverzeichnis

[AHa] E. Artin, H. Hasse, *Die beiden Ergänzungssätze zum Reziprozitätsgesetz der l^n-ten Potenzreste im Körper der l^n-ten Einheitswurzeln*, Abh. Math. Sem. Univ. Hamburg 6 (1928), 146 – 162

[Ha1] H. Hasse, *Zum expliziten Reziprozitätsgesetz*, Abh. Math. Sem. Univ. Hamburg 7 (1930), 52 – 63

[Ha2] H. Hasse, *Zahlentheorie*, Akademie-Verlag Berlin, 1949

[Hal] M. Halphen, *Sur de suites de fractions, analogues à la suite de Farey*, Bull. Soc. Math. France 5 (1876/77), 170 – 175

[Iwa1] K. Iwasawa, *On some modules in the theory of cyclotomic fields*, Journ. Math. Soc. Japan 16 (1964), 42 – 82

[Iwa2] K. Iwasawa, *On explicit formulas for the norm residue symbol*, Journ. Math. Soc. Japan 20 (1968), 151 – 165

[Kudo] A. Kudo, *On Iwasawa's explicit formula for the norm residue symbol*, Mem. Fac. Sci. Kyushu Univ. Ser. A 26 (1972), 139 – 148

[Lor1] F. Lorenz, *Einführung in die Algebra I*, Hochschultaschenbuch, Spektrum Akademischer Verlag, 3. Auflage, 1996

[Lor2] F. Lorenz, *Einführung in die Algebra, Teil II*, BI-Wissenschaftsverlag, 1990

[Neu] J. Neukirch, *Algebraische Zahlentheorie*, Springer-Verlag 1992

[TTB] Teubner Taschenbuch der Mathematik, Teil I, Verlag B. G. Teubner, Leipzig, 1996

[Was] L. C. Washington, *Introduction to cyclotomic fields*, GTM 83, Springer-Verlag 1982

[Weil] A. Weil, *Basic Number Theory*, Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen, Band 144, Springer-Verlag 1967

Selbstständigkeitserklärung

Hiermit bestätige ich, dass ich diese Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Diese Arbeit wurde in dieser oder ähnlicher Form keiner anderen Prüfungsbehörde vorgelegt.