ÜBER DIE GALOISMODULSTRUKTUR UND DIE ABSOLUTE GALOISGRUPPE $\mathfrak{p}$-ADISCHER ZAHLKÖRPER

Dissertation
zur Erlangung des Doktorgrades
des Fachbereichs Mathematik
der Universität Hamburg

vorgelegt von
U w e J a n n s e n
aus Meddewade

HAMBURG 1980

Genehmigt vom Fachbereich Mathematik der Universität Hamburg
auf Antrag von Prof. Dr. H. Brückner

Hamburg, den 9.7.1980

Prof. Dr. C. Geiger
Sprecher des Fachbereichs

Inhalt

Einleitung

Ist K/k eine endliche galoissche Erweiterung $\mathfrak{p}$-adischer Zahlkörper über $\mathbb{Q}_p$, so operiert die Galoisgruppe G auf der multiplikativen Gruppe K^*. Die G-Modul-Struktur von K^* hängt nach der lokalen Klassenkörpertheorie mit der Struktur der absoluten Galoisgruppe G_k von k zusammen und ist noch nicht vollständig bekannt.

Ausführlich wurden bisher zahm-verzweigte Erweiterungen [14], [25] und p-Erweiterungen [2], [3], [5], [8], [17], [30] untersucht. Für andere Erweiterungen liegen derzeit nur Einzelergebnisse vor; diese beschränken sich auf Fälle mit zyklischer Verzweigungsgruppe, siehe z.B. [4] und [31].

In der vorliegenden Arbeit werden nun Erweiterungen mit beliebiger Galoisgruppe G behandelt. Es erweist sich dabei als sinnvoll, die pro-endliche Vervollständigung und insbesondere die pro-p-Vervollständigung A(K) von K^* zu betrachten, die ein Modul über dem Gruppenring $\mathbb{Z}_p[G]$ ist. Wir erhalten in §3 das folgende allgemeine Resultat:

Satz: Ist $n = [k:\mathbb{Q}_p]$ und $1 \longrightarrow R_{n+3} \longrightarrow F_{n+3} \longrightarrow G \longrightarrow 1$ eine Darstellung der Gruppe G durch eine freie Gruppe F_{n+3} mit n+3 freien Erzeugenden - eine solche existiert, da G durch n+3 Elemente erzeugt werden kann -, so gibt es eine exakte Sequenz

$$0 \longrightarrow \mathbb{Z}_p[G]^2 \longrightarrow (R_{n+3}{}^{ab})_p \longrightarrow A(K) \longrightarrow 0$$

mit dem $\mathbb{Z}_p[G]$-Modul $(R_{n+3}{}^{ab})_p = \mathbb{Z}_p \otimes R_{n+3}{}^{ab}$.

Dies verallgemeinert einen entsprechenden Satz für p-Gruppen aus der Arbeit [17] von K. Wingberg und dem Autor, vgl. auch [5].

Ist K regulär, d.h., enthält K keine primitive p-te Einheitswurzel, so läßt sich G durch n+2 Elemente erzeugen, und wir erhalten aus dem obigen Satz die Isomorphie

$$A(K) \oplus \mathbb{Z}_p[G] \cong (R_{n+2}{}^{ab})_p,$$

bzw. $A(K) \cong (R_{n+1}{}^{ab})_p$, wenn G durch n+1 Elemente erzeugt wird, und damit eine vollständige Lösung des Problems. Das ist ebenfalls eine direkte Verallgemeinerung eines analogen Satzes für p-Gruppen, s. Borevič [3] und Wingberg [30]. Die sogenannten Relationenmoduln $R_{n+2}{}^{ab}$ bzw. $R_{n+1}{}^{ab}$ werden wieder aus freien Darstellungen $1 \longrightarrow R_m \longrightarrow F_m \longrightarrow G \longrightarrow 1$ für $m = n+2$ bzw. $m = n+1$ gewonnen, wobei die $\mathbb{Z}_p[G]$-Struktur der Lokalisierung $(R_m{}^{ab})_p = \mathbb{Z}_p \otimes R_m{}^{ab}$ nur von m und nicht von der speziellen Wahl der freien Darstellung abhängt.

Die betrachtete Galoismodulstruktur ist durch die lokale Klassenkörpertheorie eng verknüpft mit dem galoistheoretischen Aufbau der Erweiterungen von k. Man gewinnt aus ihr nicht nur mittels der Kohomologietheorie das lokale Reziprozitätsgesetz und damit die Kenntnis der abelschen Erweiterungen von k, sondern mit dem Satz von Weil-Šafarevič,[1] XV Th. 6, auch Informationen über nicht-abelsche Erweiterungen, vgl. a. [18].

Iwasawa [14] benutzte als erster die Galoismodulstruktur zahmverzweigter Erweiterungen, um daraus Aussagen über die absolute Galoisgruppe $\mathfrak{p}$-adischer Zahlkörper abzuleiten. Trotz umfangreicher weiterer Untersuchungen von Koch [20] und Jakovlev [15] gelang es jedoch nicht, die absolute Galoisgruppe vollständig zu bestimmen; das entsprechende Theorem von Jakovlev enthält einen Fehler, vgl. die Korrektur in [16]. Wir beschreiten den Weg von Iwasawa, um hier einige neue Ergebnisse zu erhalten.

Dazu bestimmen wir in §2 ebenfalls die $\mathbb{Z}_p[G]$-Struktur der Einseinheitengruppe U_K^1 einer zahm-verzweigten Erweiterung K/k, allerdings mit anderen Methoden. Die etwas komplizierten und speziell auf die Einseinheitengruppe zugeschnittenen Betrachtungen von Iwasawa werden ersetzt durch die Beobachtung, daß U_K^1 als $\mathbb{Z}_p[G]$-Modul dadurch charakterisiert wird, daß er kohomologisch trivial ist und $\mathbb{Q}_p \otimes U_K^1 \cong \mathbb{Q}_p[G]^n$ mit $n = [k:\mathbb{Q}_p]$ gilt. Das motiviert die folgende

Definition: Sei G eine endliche Gruppe. Ein endlich erzeugter $\mathbb{Z}_p[G]$-Modul M heißt quasifrei, wenn M kohomologisch trivial ist und die Isomorphie $\mathbb{Q}_p \otimes M \cong \mathbb{Q}_p[G]^m$ für ein $m \in \mathbb{N}$ gilt.

Die Untersuchung quasifreier $\mathbb{Z}_p[G]$-Moduln in §1 zeigt, daß deren Struktur sehr einfach ist und gut beschrieben werden kann. Insbesondere ergibt sich die $\mathbb{Z}_p[G]$-Struktur von U_K^1 ganz kanonisch aus der G-Struktur der Gruppe μ_K der in U_K^1 enthaltenen Einheitswurzeln. Dies bietet aber nicht nur einen technischen Vorteil. Die Beschreibung von U_K^1 durch n $\mathbb{Z}_p[G]$-Erzeugende, ein $\mathbb{Z}_p$-Erzeugendes, eine $\mathbb{Z}_p$- und zwei $\mathbb{Z}_p[G]$-Relationen in [14] u. [25] wird ersetzt durch die Angabe von n+1 $\mathbb{Z}_p[G]$-Erzeugenden und einer $\mathbb{Z}_p[G]$-Relation, die zudem eine sehr einfache Gestalt hat. Das hat zwei wesentliche Konsequenzen:

Erstens bereitet der Übergang zum projektiven Limes, durch den wir mittels der Klassenkörpertheorie die Operation der Galoisgruppe $\mathcal{G}$ der maximalen zahm-verzweigten Erweiterung von k auf der Faktorkommutatorgruppe V_k^{ab} der Verzweigungsgruppe V_k von G_k bestimmen, keine Schwierigkeiten wie bei Iwasawa [14] und Koch [20], und wir erhalten eine einfache Beschreibung der Gruppe $G_k/[V_k, V_k]$.

Zweitens folgern wir in §4, daß zur Beschreibung der ganzen Gruppe G_k neben der bekannten Relation für $\mathfrak{g}$ nur noch eine weitere Relation nötig ist, während die bisherigen Arbeiten immer von zwei weiteren Relationen ausgehen. Wir erhalten das Aussehen dieser einen Relation bis auf Kommutatoren aus V_k und können unser Ergebnis folgendermaßen formulieren:

Satz: Sei k ein $\mathfrak{p}$-adischer Zahlkörper vom Grad n und Restklassengrad f über $\mathbb{Q}_p$, $\tilde{k}$ ein algebraischer Abschluß von k, V der Verzweigungskörper von $\tilde{k}/k$ und μ_V die Gruppe der in V enthaltenen Einheitswurzeln von p-Potenzordnung. Dann ist die absolute Galoisgruppe $G_k = \mathrm{Gal}(\tilde{k}/k)$ von k eine pro-endliche Gruppe mit n+3 Erzeugenden und 2 Relationen. Es gibt Erzeugende $y_o, \ldots, y_n$, σ und τ derart, daß die Relationen die Gestalt

$$\sigma\,\tau\,\sigma^{-1} = \tau^{p^f}$$

und $$[\sigma, y_o]\, y_o^{1-g} [\tau, y_1]\, y_1^{1-h(1+p^s)} \cdot r' = 1 \quad \text{mit } r' \in [V_k, V_k]$$

besitzen. Dabei ist $[a,b] = aba^{-1}b^{-1}$ der Kommutator von a und b, $p^s = (\mu_V : 1)$, g eine ganzrationale Zahl und h eine (p-1)-te Einheitswurzel aus $\mathbb{Z}_p$ derart, daß für eine primitive p^s-te Einheitswurzel ζ aus μ_V die Beziehung $\sigma(\zeta) = \zeta^g$ bzw. $\tau(\zeta) = \zeta^h$ gilt.

Alle oben genannten Resultate ergeben sich mit Hilfe der lokalen Klassenkörpertheorie und der Galoiskohomologie aus zwei klassischen Arbeiten von Gilbarg [9] und Swan [29]. Daher ist die folgende Darstellung in sich abgeschlossen in dem Sinne, daß keine der anderen Arbeiten über die Galoismodulstruktur der multiplikativen Gruppe K^* oder über die Struktur der absoluten Galoisgruppe G_k zu ihrem Verständnis benötigt wird.

§1 Quasifreie $\mathbb{Z}_p[G]$-Moduln.

Bezeichnungen:

p ist eine Primzahl,

$\mathbb{Q}_p$ der Körper der p-adischen Zahlen und

$\mathbb{Z}_p$ der darin enthaltene Ring der ganzen p-adischen Zahlen.

$\mathbb{Z}_p[G]$ ist für eine endliche Gruppe G der Gruppenring mit Koeffizienten in $\mathbb{Z}_p$. Für zwei $\mathbb{Z}_p[G]$-Moduln A und B wird

$\mathrm{Hom}(A,B) := \mathrm{Hom}_{\mathbb{Z}_p}(A,B)$ zu einem $\mathbb{Z}_p[G]$-Modul durch die Definition

$$(sf)(a) := sf(s^{-1}a) \quad \text{für } f \in \mathrm{Hom}(A,B),\ s \in G \text{ und } a \in A,$$

$A \otimes B := A \otimes_{\mathbb{Z}_p} B$ zu einem $\mathbb{Z}_p[G]$-Modul durch die Definition

$$s(a \otimes b) := (sa) \otimes (sb) \quad \text{für } s \in G,\ a \in A \text{ und } b \in B.$$

$\mathbb{Z}_p$, $\mathbb{Q}_p$ und $\mathbb{Q}_p/\mathbb{Z}_p$ werden als $\mathbb{Z}_p[G]$-Moduln immer mit der trivialen G-Operation versehen. $\mathbb{Q}_p \otimes A$ liefert dann die übliche Skalarerweiterung von $\mathbb{Z}_p$ nach $\mathbb{Q}_p$ bzw. von $\mathbb{Z}_p[G]$ nach $\mathbb{Q}_p[G]$, dem Gruppenring mit Koeffizienten in $\mathbb{Q}_p$.

$A^D := \mathrm{Hom}(A, \mathbb{Q}_p/\mathbb{Z}_p)$ ist das Pontrjagindual eines endlich erzeugten $\mathbb{Z}_p[G]$-Moduls A; bekanntlich gilt in kanonischer Weise die Isomorphie $(A^D)^D \cong A$.

$\mathrm{Tor}(A)$ bezeichnet den Torsionsmodul von A.

$\mathrm{Rg}\, A := \dim_{\mathbb{Q}_p} \mathbb{Q}_p \otimes A$ ist der $\mathbb{Z}_p$-Rang eines $\mathbb{Z}_p$-Moduls A.

Ist R ein beliebiger Ring und A ein R-Modul, so werden für eine natürliche Zahl n die R-Moduln ${}_nA$ und A_n durch die exakte Sequenz

$$0 \longrightarrow {}_nA \longrightarrow A \xrightarrow{\cdot n} A \longrightarrow A_n \longrightarrow 0$$

definiert, die durch die Multiplikation mit n in A entsteht. Es ist also ${}_nA = \{a \in A;\ na = 0\}$ und $A_n = A/nA$.

Wir setzen im folgenden die Begriffe und Sätze der Kohomologie von pro-endlichen Gruppen und der lokalen Klassenkörpertheorie voraus, wie sie etwa in [1] oder [26] - [28] zu finden sind. Für eine pro-endliche Gruppe G und einen G-Modul A bezeichne dabei $H^0(G,A)$ die gewöhnliche (nicht reduzierte) nullte Kohomologiegruppe, es ist also $H^0(G,A) = A^G = \{a \in A;\ \sigma a = a \ \forall \sigma \in G\}$ der Fixmodul von A unter G.

Wir stellen zunächst fünf Lemmata bereit, die sich im folgenden als äußerst nützlich erweisen werden:

Lemma 1.1.: Sei R ein beliebiger Ring; eine exakte Sequenz

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

von R-Moduln induziert kanonisch eine exakte Sequenz

$$0 \longrightarrow {}_nA \xrightarrow{f} {}_nB \xrightarrow{g} {}_nC \longrightarrow A_n \xrightarrow{\bar{f}} B_n \xrightarrow{\bar{g}} C_n \longrightarrow 0$$

Beweis: Anwendung des Schlangenlemmas auf das Diagramm

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle \cdot n} & & \uparrow{\scriptstyle \cdot n} & & \uparrow{\scriptstyle \cdot n} & & \\ 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0. \end{array}$$

Lemma 1.2. (Lemma von Schanuel): Sei R ein Ring und seien

$$0 \longrightarrow A \longrightarrow P \longrightarrow C \longrightarrow 0$$

$$0 \longrightarrow A' \longrightarrow P' \longrightarrow C' \longrightarrow 0$$

exakte Sequenzen von R-Moduln mit projektiven Moduln P und P'. Gilt dann $C \cong C'$, so folgt $A \oplus P' \cong A' \oplus P$.

Beweis: Dies folgt leicht aus einem Pullback-Diagramm, vergl. Gruenberg [10] §8.10 Lemma 11.

Lemma 1.3. (Lemma von Swan): Sind P und P' projektive, endlich erzeugte $\mathbb{Z}_p[G]$-Moduln, dann gilt:

$$\mathbb{Q}_p \otimes P \cong \mathbb{Q}_p \otimes P' \quad \Rightarrow \quad P \cong P'.$$

Beweis: Dieses Ergebnis bildet, in etwas allgemeinerer Form, das Kernstück der grundlegenden Arbeit von Swan [29], siehe dort Th. 6.1. bzw. Cor. 6.4..

Lemma 1.4.: Ein endlich erzeugter $\mathbb{Z}_p[G]$-Modul ist genau dann projektiv, wenn er torsionsfrei und kohomologisch trivial ist.

Beweis: Dies folgt aus Sätzen von Nakayama, siehe etwa [10], §10.7 Theorem 3.

Lemma 1.5. (semi-lokaler Kürzungssatz): Ist R ein kommutativer, semi-lokaler Ring und sind A und B endlich erzeugte Moduln über dem Gruppenring $R[G]$, so gilt:

$$A \oplus R[G] \cong B \oplus R[G] \quad \Rightarrow \quad A \cong B.$$

Beweis: Siehe etwa Gruenberg [10], §10.6 Th. 1.

Wir wollen uns in diesem Paragraphen mit Moduln beschäftigen, die sich nicht allzusehr von freien Moduln unterscheiden; dazu definieren wir:

Definition 1.6.: Ein endlich erzeugter $\mathbb{Z}_p[G]$-Modul A heißt quasifrei, wenn er kohomologisch trivial und $\mathbb{Q}_p \otimes A$ ein freier $\mathbb{Q}_p[G]$-Modul ist.

Bemerkungen 1.7.:

a.) Aus der Definition folgt, daß der $\mathbb{Z}_p$-Rang eines quasifreien Moduls A immer ein Vielfaches der Gruppenordnung ist; wir nennen im folgenden A einen quasifreien Modul vom Rang m, wenn $\mathbb{Q}_p \otimes A \cong \mathbb{Q}_p[G]^m$ gilt; der $\mathbb{Z}_p$-Rang von A ist dann m(G:1).

b.) Ein torsionsfreier quasifreier Modul ist $\mathbb{Z}_p[G]$-frei. Dies folgt aus Lemma 1.4. und Lemma 1.3..

Definition 1.8.: Seien A und B endlich erzeugte $\mathbb{Z}_p[G]$-Moduln. A heißt quasiisomorph zu B, wenn es einen $\mathbb{Z}_p[G]$-Homomorphismus $f: A \longrightarrow B$ mit endlichem Kern und Cokern gibt. Wir schreiben dafür $A \sim B$ und nennen f einen Quasiisomorphismus.

Satz 1.9.: Für endlich erzeugte $\mathbb{Z}_p[G]$-Moduln A und B gilt:

$$A \sim B \iff \mathbb{Q}_p \otimes A \cong \mathbb{Q}_p \otimes B \quad \text{(als } \mathbb{Q}_p[G]\text{-Moduln)}.$$

Beweis: Aus einer exakten Sequenz

$$0 \longrightarrow M \longrightarrow A \longrightarrow B \longrightarrow N \longrightarrow 0$$

mit endlichen Moduln M und N folgt die Isomorphie $\mathbb{Q}_p \otimes A \cong \mathbb{Q}_p \otimes B$, da das Tensorieren mit $\mathbb{Q}_p$ exakt und $\mathbb{Q}_p \otimes N = \mathbb{Q}_p \otimes M = 0$ ist.

Sei umgekehrt $h: \mathbb{Q}_p \otimes A \longrightarrow \mathbb{Q}_p \otimes B$ ein $\mathbb{Q}_p[G]$-Isomorphismus. Die kanonischen Homomorphismen $A \xrightarrow{i} \mathbb{Q}_p \otimes A$ und $B \xrightarrow{j} \mathbb{Q}_p \otimes B$ haben die Kerne Tor(A) bzw. Tor(B); für ein $m \in \mathbb{N}$ mit $p^m \mathrm{Tor}(B) = 0$ können wir daher $p^m B$ vermöge j als Untermodul von $\mathbb{Q}_p \otimes B$ auffassen. A ist endlich erzeugt, etwa von $x_1, \ldots, x_r$; da $\mathbb{Q}_p \otimes B$ von $p^m B$ über $\mathbb{Q}_p$ erzeugt wird, gilt für geignetes $n \in \mathbb{N}$ $p^n h(i(x_i)) \in p^m B$ für alle i. Der Homomorphismus

$$p^n A \xrightarrow{i} \mathbb{Q}_p \otimes A \xrightarrow{h} \mathbb{Q}_p \otimes B$$

liefert daher einen Homomorphismus $g: p^nA \longrightarrow p^mB$, dessen Kern in Tor(A) enthalten ist. Der Kern der Abbildung

$$f: A \xrightarrow{p^n} p^nA \xrightarrow{g} p^mB \longrightarrow B$$

ist dann ebenfalls in Tor(A) enthalten und damit endlich. Da $Rg\ A = \dim \mathbb{Q}_p \otimes A = \dim \mathbb{Q}_p \otimes B = Rg\ B$ gilt, hat der Cokern von f den Rang Null; da er endlich erzeugt ist, ist er endlich. Insgesamt ergibt sich, daß f ein Quasiisomorphismus ist. q.e.d.

Corollar 1.10.: Quasiisomorphie ist eine Äquivalenzrelation.

Satz 1.11.: Sei A ein endlich erzeugter $\mathbb{Z}_p[G]$-Modul, dann sind folgende Aussagen äquivalent:

a.) A ist quasifrei.

b.) A ist kohomologisch trivial und es gilt $A \sim \mathbb{Z}_p[G]^m$ für ein $m \in \mathbb{N}$.

c.) A ist kohomologisch trivial und enthält einen freien $\mathbb{Z}_p[G]$-Modul von endlichem Index in A.

d.) Es gibt eine exakte Sequenz

$$0 \longrightarrow \mathbb{Z}_p[G]^k \longrightarrow \mathbb{Z}_p[G]^l \longrightarrow A \longrightarrow 0.$$

Beweis: a.) $\Rightarrow$ b.): Aus der Isomorphie $\mathbb{Q}_p \otimes A \cong \mathbb{Q}_p[G]^m \cong \mathbb{Q}_p \otimes \mathbb{Z}_p[G]^m$ folgt mit Satz 1.9. $A \sim \mathbb{Z}_p[G]^m$.

b.) $\Rightarrow$ c.): Aus $A \sim \mathbb{Z}_p[G]^m$ folgt mit Corollar 1.10. $\mathbb{Z}_p[G]^m \sim A$; es gibt also einen $\mathbb{Z}_p[G]$-Homomorphismus $f: \mathbb{Z}_p[G]^m \longrightarrow A$ mit endlichem Kern und Cokern. Als torsionsfreier Modul muß der Kern dann Null sein; dies zeigt c.).

c.) $\Rightarrow$ a.): Aus einer exakten Sequenz $0 \longrightarrow \mathbb{Z}_p[G]^m \longrightarrow A \longrightarrow M \longrightarrow 0$ mit endlichem M folgt $\mathbb{Q}_p[G]^m \cong \mathbb{Q}_p \otimes A$ durch Tensorieren mit $\mathbb{Q}_p$.

a.) $\Leftrightarrow$ d.): Sei $0 \longrightarrow B \longrightarrow \mathbb{Z}_p[G]^l \longrightarrow A \longrightarrow 0$ eine Darstellung von A durch einen freien $\mathbb{Z}_p[G]$-Modul, dann ist B genau dann kohomologisch trivial, wenn dies für A gilt. Weiter folgt mit dem Satz von Maschke die Isomorphie

$$\mathbb{Q}_p[G]^l \cong \mathbb{Q}_p \otimes B \oplus \mathbb{Q}_p \otimes A.$$

Wegen der Gültigkeit des Krull-Schmidt-Theorems für $\mathbb{Q}_p[G]$-Moduln ist daher A genau dann quasifrei, wenn B quasifrei ist. Wegen der Torsionsfreiheit von B ist dies genau dann der Fall, wenn B $\mathbb{Z}_p[G]$-frei ist, vergl. Bem. 1.7. b.). q.e.d.

Corollar 1.12.: Ist G eine p-Gruppe, so ist jeder endlich erzeugte, kohomologisch triviale $\mathbb{Z}_p[G]$-Modul quasifrei.

Beweis: Ist $0 \longrightarrow B \longrightarrow \mathbb{Z}_p[G]^l \longrightarrow A \longrightarrow 0$ eine Darstellung des kohomologisch trivialen Moduls A, so ist B nach Lemma 1.4. projektiv. Da für eine p-Gruppe G der Gruppenring $\mathbb{Z}_p[G]$ ein lokaler Ring ist, siehe [10], §10.5 Prop. 10, ist B sogar frei, siehe z.B. [11] Prop. 3.16.. Mit Satz 1.11. folgt dann die Behauptung.

Wir werden nun die quasifreien Moduln in drei Schritten klassifizieren:

Satz 1.13.: Ein quasifreier $\mathbb{Z}_p[G]$-Modul ist eindeutig durch seinen Rang und seinen Torsionsmodul bestimmt.

Beweis: Seien M und M' quasifrei, dann gibt es nach Satz 1.11.

exakte Sequenzen

$$0 \longrightarrow \mathbb{Z}_p[G]^k \longrightarrow \mathbb{Z}_p[G]^l \longrightarrow M \longrightarrow 0$$

$$0 \longrightarrow \mathbb{Z}_p[G]^{k'} \longrightarrow \mathbb{Z}_p[G]^{l'} \longrightarrow M' \longrightarrow 0.$$

Sie induzieren für $n = p^r \in \mathbb{N}$ nach Lemma 1.1. exakte Sequenzen

$$0 \longrightarrow {}_n\mathrm{Tor}(M) \longrightarrow \mathbb{Z}/n\mathbb{Z}[G]^k \longrightarrow \mathbb{Z}/n\mathbb{Z}[G]^l \longrightarrow M_n \longrightarrow 0$$

$$0 \longrightarrow {}_n\mathrm{Tor}(M') \longrightarrow \mathbb{Z}/n\mathbb{Z}[G]^{k'} \longrightarrow \mathbb{Z}/n\mathbb{Z}[G]^{l'} \longrightarrow M'_n \longrightarrow 0.$$

Durch Dualisieren, d.h., die Anwendung des exakten Funktors $M \rightsquigarrow M^D$, erhalten wir die exakten Sequenzen

$$0 \longrightarrow M_n{}^D \longrightarrow \mathbb{Z}/n\mathbb{Z}[G]^l \longrightarrow \mathbb{Z}/n\mathbb{Z}[G]^k \longrightarrow {}_n\mathrm{Tor}(M)^D \longrightarrow 0$$

$$0 \longrightarrow M'_n{}^D \longrightarrow \mathbb{Z}/n\mathbb{Z}[G]^{l'} \longrightarrow \mathbb{Z}/n\mathbb{Z}[G]^{k'} \longrightarrow {}_n\mathrm{Tor}(M')^D \longrightarrow 0.$$

Gilt nun $\mathrm{Tor}(M) \cong \mathrm{Tor}(M')$, so folgt mit dem Lemma von Schanuel (zweimalige Anwendung, vergl. auch [10], p. 163):

$$M_n{}^D \oplus \mathbb{Z}/n\mathbb{Z}[G]^{k+l'} = M'_n{}^D \oplus \mathbb{Z}/n\mathbb{Z}[G]^{k'+l}.$$

Gilt weiter $(l-k)(G:1) = \mathrm{Rg}\ M = \mathrm{Rg}\ M' = (l'-k')(G:1)$, also $k'+l = k+l'$, so folgt $M_n{}^D \cong M'_n{}^D$ und damit

$$M/nM \cong M'/nM' \quad \text{für alle} \quad n = p^r \in \mathbb{N}.$$

Daraus folgt aber $M \cong M'$, wie man folgendermaßen einsehen kann: Die Mengen $\mathrm{Isom}(M/nM, M'/nM')$ der Isomorphismen von M/nM nach M'/nM' bilden ein projektives System nicht-leerer, endlicher Mengen. Nach einem allgemeinen Satz (Bourbaki, Top. Gén., Chap. I, 3ème ed., Append. th. 1) ist daher der projektive Limes nicht leer. Ein Element des projektiven Limes vermittelt aber gerade einen Isomorphismus zwischen M und M', da M (bzw. M') der projektive Limes der M/nM (bzw. M'/nM') für $n = p^r \in \mathbb{N}$ ist.

Definition 1.14.: Für einen endlich erzeugten $\mathbb{Z}_p[G]$-Modul N definieren wir den Erzeugendenrang $d_G(N)$ als die minimale Anzahl von $\mathbb{Z}_p[G]$-Erzeugenden von N und den Relationenrang $r_G(N)$ wie folgt: Ist $0 \longrightarrow B \longrightarrow \mathbb{Z}_p[G]^n \longrightarrow N \longrightarrow 0$ eine beliebige Darstellung von N durch einen freien $\mathbb{Z}_p[G]$-Modul, so sei $r_G(N) = d_G(B) - n + d_G(N)$.

Bemerkungen 1.15.: a.) $r_G(N)$ ist wohldefiniert, denn sei

$$0 \longrightarrow B' \longrightarrow \mathbb{Z}_p[G]^{n'} \longrightarrow N \longrightarrow 0$$

eine andere freie Darstellung von N, so folgt mit dem Lemma von Schanuel

$$B \oplus \mathbb{Z}_p[G]^{n'} \cong B' \oplus \mathbb{Z}_p[G]^{n}$$

und daraus wiederum $d_G(B) + n' = d_G(B') + n$, siehe Gruenberg [11], Lemma 5.8., da $\mathbb{Z}_p[G]$ ein semi-lokaler Ring ist.

b.) $r_G(N)$ kann auch definiert werden als der Erzeugendenrang $d_G(B)$ in einer minimalen Darstellung

$$0 \longrightarrow B \longrightarrow \mathbb{Z}_p[G]^{d_G(N)} \longrightarrow N \longrightarrow 0.$$

c.) Es gilt immer $r_G(N) \geq 0$, wie aus b.) folgt.

d.) Ist N endlich, so gilt $r_G(N) \geq d_G(N)$, denn nach b.) gibt es eine exakte Sequenz

$$\mathbb{Z}_p[G]^r \longrightarrow \mathbb{Z}_p[G]^d \longrightarrow N \longrightarrow 0$$

mit $r = r_G(N)$ und $d = d_G(N)$, die für $\mathbb{Q}_p \otimes N = 0$ eine Surjektion $\mathbb{Q}_p[G]^r \twoheadrightarrow \mathbb{Q}_p[G]^d$ induziert. Gilt $r = d$, so ist die erste Abbildung in der obigen Sequenz notwendig injektiv und daher N kohomologisch trivial. Ist umgekehrt N endlich und kohomologisch trivial, so ist N quasifrei und mit den gleichen Schlüssen wie in Satz 1.11. folgt $r_G(N) = d_G(N)$.

Satz 1.16.: Ist M ein quasifreier $\mathbb{Z}_p[G]$-Modul und

$$(*) \qquad 0 \longrightarrow \mathbb{Z}_p[G]^k \longrightarrow \mathbb{Z}_p[G]^l \xrightarrow{\pi} M \longrightarrow 0$$

exakt, so gilt mit $N = \mathrm{Tor}(M)$:

$$k \geq d_G(N^D), \quad l \geq r_G(N^D) \quad \text{und} \quad l - k \geq r_G(N^D) - d_G(N^D).$$

Beweis: Aus der Sequenz $(*)$ folgt die exakte Sequenz

$$\mathrm{Hom}(M,\mathbb{Z}_p) \longrightarrow \mathrm{Hom}(\mathbb{Z}_p[G]^l,\mathbb{Z}_p) \longrightarrow \mathrm{Hom}(\mathbb{Z}_p[G]^k,\mathbb{Z}_p) \xrightarrow{\varphi} \mathrm{Tor}(M)^D \longrightarrow 0$$

wegen $\mathrm{Ext}^1_{\mathbb{Z}_p}(\mathbb{Z}_p[G]^l,\mathbb{Z}_p) = 0$ und den kanonischen Isomorphismen

$$\mathrm{Ext}^1_{\mathbb{Z}_p}(M,\mathbb{Z}_p) = \mathrm{Ext}^1_{\mathbb{Z}_p}(M,\mathbb{Q}_p/\mathbb{Z}_p)^D \cong \mathrm{Tor}_1^{\mathbb{Z}_p}(M,\mathbb{Q}_p/\mathbb{Z}_p)^D \cong \mathrm{Tor}(M)^D,$$

siehe Cartan-Eilenberg [7], Chap. VI Prop. 5.3.; explizit setze etwa $\varphi(f)(x) = f(p^m y)/p^m + \mathbb{Z}_p$, wenn $\pi(y) = x$ und $p^m x = 0$ ist. Da für $n \in \mathbb{N}$ $\mathrm{Hom}(\mathbb{Z}_p[G]^n,\mathbb{Z}_p)$ wieder ein freier $\mathbb{Z}_p[G]$-Modul vom Rang n ist, erhalten wir eine exakte Sequenz

$$\mathbb{Z}_p[G]^l \longrightarrow \mathbb{Z}_p[G]^k \xrightarrow{\varphi} N^D \longrightarrow 0.$$

Daraus folgt sofort $k \geq d_G(N^D)$, sowie $l \geq d_G(\mathrm{Ker}\,\varphi) =$ $= r_G(N^D) + k - d_G(N^D)$ nach Definition des Relationenranges, also $l - k \geq r_G(N^D) - d_G(N^D)$. Aus beiden Ungleichungen folgt schließlich auch $l \geq r_G(N^D)$. q.e.d.

Aus dem obigen Satz folgt insbesondere, daß die Ränge der quasifreien Moduln mit Torsionsmodul N nach unten durch die Konstante $r_G(N^D) - d_G(N^D)$ beschränkt sind. Es existiert auch immer ein quasifreier Modul mit diesem minimalen Rang. Dies ergibt sich aus dem nächsten Satz, der zeigt, wie man einen quasifreien Modul aus seinem Torsionsmodul konstruieren kann:

Satz 1.17.: Sei N ein endlicher $\mathbb{Z}_p[G]$-Modul und

$$P \xrightarrow{f} Q \longrightarrow N^D \longrightarrow 0$$

exakt mit $P \cong \mathbb{Z}_p[G]^l$ und $Q \cong \mathbb{Z}_p[G]^k$. Ist

$$f^*: \mathrm{Hom}(Q,\mathbb{Z}_p) \longrightarrow \mathrm{Hom}(P,\mathbb{Z}_p)$$

die von f induzierte Abbildung, so ist f^* injektiv und der Cokern von f^* der quasifreie $\mathbb{Z}_p[G]$-Modul vom Rang k-l mit Torsionsmodul N.

Beweis: Die Injektivität von f^* folgt wegen $\mathrm{Hom}(N^D,\mathbb{Z}_p) = 0$ aus der Linksexaktheit des Hom-Funktors. $M = \mathrm{Cok}\, f^*$ ist quasifrei, da $\mathrm{Hom}(P,\mathbb{Z}_p)$ und $\mathrm{Hom}(Q,\mathbb{Z}_p)$ freie $\mathbb{Z}_p[G]$-Moduln sind, vergl. Satz 1.11. d.). Es ist noch $\mathrm{Tor}(M) \cong N$ zu zeigen. Durch erneute Anwendung des Hom-Funktors erhalten wir die exakte Sequenz

$$\mathrm{Hom}(\mathrm{Hom}(P,\mathbb{Z}_p),\mathbb{Z}_p) \xrightarrow{f^{**}} \mathrm{Hom}(\mathrm{Hom}(Q,\mathbb{Z}_p),\mathbb{Z}_p) \longrightarrow \mathrm{Tor}(M)^D \longrightarrow 0,$$

wieder wegen $\mathrm{Ext}^1_{\mathbb{Z}_p}(M,\mathbb{Z}_p) \cong \mathrm{Tor}(M)^D$. Eine kurze Überlegung zeigt, daß die Abbildungen

$$\varphi_P: P \xrightarrow{\sim} \mathrm{Hom}(\mathrm{Hom}(P,\mathbb{Z}_p),\mathbb{Z}_p) \quad \text{mit} \quad \varphi_P(x)(g) = g(x)$$

eine Äquivalenz von Funktoren auf der Kategorie der endlich erzeugten, torsionsfreien $\mathbb{Z}_p[G]$-Moduln vermitteln (diese Moduln sind reflexive $\mathbb{Z}_p$-Moduln). Aus dem kommutativen Diagramm

$$\begin{array}{ccc} P & \xrightarrow{\quad f \quad} & Q \\ \downarrow{\scriptstyle \varphi_P} & & \downarrow{\scriptstyle \varphi_Q} \\ \mathrm{Hom}(\mathrm{Hom}(P,\mathbb{Z}_p),\mathbb{Z}_p) & \xrightarrow{f^{**}} & \mathrm{Hom}(\mathrm{Hom}(Q,\mathbb{Z}_p),\mathbb{Z}_p) \end{array}$$

folgt daher $N^D = \mathrm{Cok}\, f \cong \mathrm{Cok}\, f^{**} = \mathrm{Tor}(M)^D$, also $\mathrm{Tor}(M) \cong N$. q.e.d.

Corollar 1.18.: Sei N ein endlicher $\mathbb{Z}_p[G]$-Modul, $d = d_G(N^D)$ und $r = r_G(N^D)$, dann existiert ein quasifreier $\mathbb{Z}_p[G]$-Modul M_o mit Torsionsmodul N vom minimalen Rang r-d, der nach Satz 1.17. aus einer exakten Sequenz

$$\mathbb{Z}_p[G]^r \longrightarrow \mathbb{Z}_p[G]^d \longrightarrow N^D \longrightarrow 0$$

konstruiert werden kann. Für ihn gibt es eine exakte Sequenz

$$0 \longrightarrow \mathbb{Z}_p[G]^d \longrightarrow \mathbb{Z}_p[G]^r \longrightarrow M_o \longrightarrow 0.$$

Für jeden anderen quasifreien Modul M mit $Tor(M) \cong N$, etwa vom Rang $n = (r-d) + j$ mit $j \geq 0$, gilt die Isomorphie

$$M \cong M_o \oplus \mathbb{Z}_p[G]^j,$$

und es gibt eine exakte Sequenz

$$0 \longrightarrow \mathbb{Z}_p[G]^d \longrightarrow \mathbb{Z}_p[G]^{n+d} \longrightarrow M \longrightarrow 0.$$

Beweis: Existenz, Konstruktion und Minimalität von M_o sind nach den vorigen Sätzen klar. Da $M_o \oplus \mathbb{Z}_p[G]^j$ offenbar quasifrei vom Rang (r-d) + j ist und den Torsionsmodul N besitzt, folgt die Isomorphie $M \cong M_o \oplus \mathbb{Z}_p[G]^j$ aus Satz 1.13.. Aus der Sequenz für M_o erhalten wir trivialerweise die exakte Sequenz

$$0 \longrightarrow \mathbb{Z}_p[G]^d \longrightarrow \mathbb{Z}_p[G]^{r+j} \longrightarrow M_o \oplus \mathbb{Z}_p[G]^j \longrightarrow 0,$$

und es gilt gerade r+j = n+d. q.e.d.

§2 Zahm-verzweigte Erweiterungen $\mathfrak{p}$-adischer Zahlkörper

Als abelsche pro-p-Gruppe ist die Gruppe U_k^1 der Einseinheiten eines $\mathfrak{p}$-adischen Zahlkörpers k, dessen Restklassenkörper die Charakteristik p hat, ein $\mathbb{Z}_p$-Modul, nämlich durch die natürliche Ausdehnung des Exponentenbereichs von $\mathbb{Z}$ auf $\mathbb{Z}_p$. Es ist für $x \in U_k^1$ und $a \in \mathbb{Z}_p$ also $x^a = \lim_{n\to\infty} x^{a_n}$, wenn $a = \lim_{n\to\infty} a_n$ ist mit $a_n \in \mathbb{Z}$. Bei einer galoisschen Erweiterung K/k wird die Einseinheitengruppe U_K^1 durch die stetige Operation der Automorphismen der Galoisgruppe G zu einem $\mathbb{Z}_p[G]$-Modul. Klassisch sind die folgenden Ergebnisse:

Satz 2.1.: Sei k ein $\mathfrak{p}$-adischer Zahlkörper vom Grad n über $\mathbb{Q}_p$ und K/k eine endliche galoissche Erweiterung mit Galoisgruppe G, dann gilt:

a.) Als $\mathbb{Z}_p$-Modul ist $U_K^1 \cong \mathbb{Z}_p^{ng} \times \mathbb{Z}/p^s\mathbb{Z}$ mit $g = (G:1)$ und $s \geq 0$.

b.) U_K^1 enthält einen freien $\mathbb{Z}_p[G]$-Modul vom Rang n und von endlichem Index in U_K^1.

c.) Ist K/k zahm-verzweigt, so ist U_K^1 kohomologisch trivial.

Beweis: a.) geht bereits auf Hensel zurück und ist Innalt des Einseinheitensatzes von Hasse [12], §15, wegen $ng = [K:\mathbb{Q}_p]$.
b.) ist aus der lokalen Klassenkörpertheorie bekannt, wo es zur Berechnung des Herbrandkoeffizienten benutzt werden kann, und wurde in dieser Form zuerst von Gilbarg [9] bewiesen.
c.) Sei K/k zahm-verzweigt und T der Trägheitskörper von K/k. Da die Trägheitsgruppe $G_o = \mathrm{Gal}(K/T)$ zu p prime Ordnung hat,

ist die p-Gruppe U_K^1 kohomologisch trivial unter G_o. Aus der Hochschild-Serre-Spektralsequenz folgt daher die Isomorphie

$$H^r(G,U_K^1) \xleftarrow[\sim]{Inf} H^r(Gal(T/k),U_T^1) \quad \text{für} \quad r \in \mathbb{N}.$$

Die letztere Gruppe ist aber Null, da U_T^1 für die unverzweigte Erweiterung T/k kohomologisch trivial ist, s. [26] Chap. XII §3. Dasselbe gilt für alle Untergruppen.

Mit den Ergebnissen von §1 erhalten wir nun:

Satz 2.2.: Sei k ein $\mathfrak{p}$-adischer Zahlkörper vom Grad n über $\mathbb{Q}_p$, K/k eine endliche, zahm-verzweigte, galoissche Erweiterung mit Galoisgruppe G und μ_K die Gruppe der in K enthaltenen Einheitswurzeln von p-Potenzordnung, dann gilt:

a.) U_K^1 ist der (eindeutig bestimmte) quasifreie $\mathbb{Z}_p[G]$-Modul vom Rang n mit Torsionsmodul μ_K.

b.) Es gibt eine exakte Sequenz

$$0 \longrightarrow \mathbb{Z}_p[G] \longrightarrow \mathbb{Z}_p[G]^{n+1} \longrightarrow U_K^1 \longrightarrow 1.$$

c.) Es gilt $d_G(U_K^1) \leq n+1$.

d.) Ist K regulär, d.h., enthält K keine p-ten Einheitswurzeln außer der Eins, so gilt $U_K^1 \cong \mathbb{Z}_p[G]^n$ und $d_G(U_K^1) = n$.

Beweis: U_K^1 ist quasifrei nach Satz 2.1. b.) und c.), vergl. Satz 1.11. c.). Der Rang folgt aus 2.1. a.) oder b.), während $Tor(U_K^1) = \mu_K$ wohlbekannt ist.
b.) folgt mit Corollar 1.18., da mit μ_K auch μ_K^D zyklisch ist, also $d_G(\mu_K^D) = 1$ gilt; c.) folgt trivial aus b.).
Da U_K^1 genau dann torsionsfrei ist, wenn K regulär ist, folgt d.) aus Bemerkung 1.7. b.).

Wir wollen nun den $\mathbb{Z}_p[G]$-Modul U_K^1 für zahm-verzweigte Erweiterungen mit Hilfe von Satz 1.17. explizit durch $\mathbb{Z}_p[G]$-Erzeugende und -Relationen beschreiben. Nach Hasse [12] §16 gilt zunächst für die Struktur der Gruppe G:

Sei k ein $\mathfrak{p}$-adischer Zahlkörper über $\mathbb{Q}_p$ mit dem absoluten Restklassengrad f_o und K/k eine endliche, zahm-verzweigte, galoissche Erweiterung mit Verzweigungsindex e und Restklassengrad f, dann gilt notwendig $e \mid (p^{f_o f}-1)$ und die Galoisgruppe von K/k ist eine metazyklische Gruppe mit Erzeugenden σ und τ und den Relationen

$$\tau^e = 1 \qquad \sigma^f = \tau^r \qquad \sigma\tau\sigma^{-1} = \tau^{p^{f_o}}$$

mit einem gewissen $r \mid e$. τ erzeugt gerade die Trägheitsgruppe und σ ist eine Liftung des Frobeniusautomorphismus.

Sei s der Irregularitätsexponent von K, d.h., $(\mu_K : 1) = p^s$, und ζ eine primitive Einheitswurzel, also ein erzeugendes Element von μ_K. Dann ist die Wirkung von G auf μ_K offenbar durch zwei ganzrationale Zahlen g und h mit

$$\zeta^\sigma := \sigma(\zeta) = \zeta^g \qquad \zeta^\tau := \tau(\zeta) = \zeta^h$$

gegeben. Als Elemente von $\mathbb{Z}_p$ aufgefaßt müssen g und h Einheiten sein; sei $h = \eta \cdot \xi$ mit einer Einseinheit η und einer (p-1)-ten Einheitswurzel ξ. Wegen $h^e \equiv 1 \bmod p^s$ gilt dann $\xi^e = 1$ und $\eta^e \equiv 1 \bmod p^s$, und da e prim zu p ist, folgt daraus auch $\eta \equiv 1 \bmod p^s$, also $\zeta^\eta = 1$. Ohne Einschränkung kann daher $\eta = 1$ gesetzt und h als (p-1)-te Einheitswurzel in $\mathbb{Z}_p$ angenommen werden, wobei $h^e = 1$ gilt.

Satz 2.3.: Sei k ein $\mathfrak{p}$-adischer Zahlkörper vom Grad n über $\mathbb{Q}_p$, K/k eine endliche, zahm-verzweigte, galoissche Erweiterung mit Verzweigungsindex e und Galoisgruppe G mit Erzeugenden σ und τ, $\tau^e = 1$; sei $s \geq 1$ der Irregularitätsexponent von K, ζ eine primitive p^s-te Einheitswurzel sowie $g \in \mathbb{Z}_p$ und h eine (p-1)-te Einheitswurzel aus $\mathbb{Z}_p$ mit

$$\zeta^\sigma = \zeta^g \qquad \zeta^\tau = \zeta^h.$$

Dann gilt die $\mathbb{Z}_p[G]$-Isomorphie $U_K^1 \cong M_1 \oplus \mathbb{Z}_p[G]^{n-1}$, wobei M_1 durch die exakte Sequenz

$$0 \longrightarrow \mathbb{Z}_p[G]b \longrightarrow \mathbb{Z}_p[G]b_0 \oplus \mathbb{Z}_p[G]b_1 \longrightarrow M_1 \longrightarrow 0$$

$$b \longmapsto (\sigma-g)b_0 + (\tau-h(1+p^s))b_1$$

gegeben ist. Anders ausgedrückt:

U_K^1 besitzt $\mathbb{Z}_p[G]$-Erzeugende $\eta_0, \ldots, \eta_n$ mit der einzigen definierenden Relation

$$\eta_0^{\sigma-g}\,\eta_1^{\tau-h(1+p^s)} = 1.$$

Beweis: Wir konstruieren M_1 als quasifreien Modul vom Rang 1 mit Torsionsmodul μ_K gemäß Satz 1.17. aus dem Anfang einer freien Auflösung von μ_K^D.

Offenbar wird $\mu_K^D = \mathrm{Hom}(\mu_K, \mathbb{Q}_p/\mathbb{Z}_p)$ von χ mit $\chi(\zeta) = 1/p^s + \mathbb{Z}_p$ erzeugt, und es gilt $\sigma^{-1}\chi = g\chi$ und $\tau^{-1}\chi = h\chi$. Betrachten wir den surjektiven $\mathbb{Z}_p[G]$-Homomorphismus

$$\varphi : \mathbb{Z}_p[G]c \twoheadrightarrow \mu_K^D \quad \text{mit} \quad \varphi(c) = \chi,$$

so liegen also $(\sigma^{-1}-g)c$, $(\tau^{-1}-h)c$ und $p^s\mathbb{Z}_p[G]c$ in $\mathrm{Ker}\,\varphi$. Wir behaupten, daß $\mathrm{Ker}\,\varphi$ von $(\sigma^{-1}-g)c$ und $(\tau^{-1}-h(1+p^s))c$ erzeugt wird. Sei dazu B der von diesen Elementen erzeugte Untermodul,

dann gilt $\sigma^{-1}c \equiv gc \bmod B$ und $\tau^{-1}c \equiv h(1+p^s)c \bmod B$, also, da σ^{-1} und τ^{-1} G erzeugen, für beliebiges $\alpha \in \mathbb{Z}_p[G]$

$$\alpha c \equiv ac \bmod B \quad \text{mit einem } a \in \mathbb{Z}_p.$$

$\mathbb{Z}_p[G]c/B$ ist daher zyklisch. Weiter gilt wegen $h^e = 1$

$$c = (\tau^{-1})^e c \equiv (1+p^s)^e c \bmod B.$$

Da e prim zu p ist, ist $(1+p^s)^e - 1 = p^s \cdot u$ mit einer Einheit $u \in \mathbb{Z}_p$; es folgt

$$p^s c = u^{-1}((1+p^s)^e - 1)c \equiv 0 \bmod B.$$

Dies zeigt, daß die kanonische Abbildung

$$\mathbb{Z}_p[G]c/B \longrightarrow\!\!\!\!\!\rightarrow \mathbb{Z}_p[G]c/\operatorname{Ker}\varphi \xrightarrow{\sim} \mu_K^D$$

ein Isomorphismus ist, d.h., $B = \operatorname{Ker}\varphi$ wie behauptet gilt.

Wir erhalten daraus eine exakte Sequenz

$$\mathbb{Z}_p[G]c_0 \oplus \mathbb{Z}_p[G]c_1 \xrightarrow{\psi} \mathbb{Z}_p[G]c \xrightarrow{\varphi}\!\!\!\!\!\rightarrow \mu_K^D \longrightarrow 1$$

mit $\psi(c_0) = (\sigma^{-1}-g)c$ und $\psi(c_1) = (\tau^{-1}-h(1+p^s))c$.

Nach Satz 1.17. induziert diese die exakte Sequenz

$$0 \longrightarrow \operatorname{Hom}(\mathbb{Z}_p[G]c, \mathbb{Z}_p) \xrightarrow{\psi^*} \operatorname{Hom}(\mathbb{Z}_p[G]c_0 \oplus \mathbb{Z}_p[G]c_1, \mathbb{Z}_p) \longrightarrow M_1 \longrightarrow 0$$

für den quasifreien Modul M_1 vom Rang 1 mit Torsionsmodul μ_K, und wegen der Eindeutigkeit gilt $U_K^1 \cong M_1 \oplus \mathbb{Z}_p[G]^{n-1}$.

Wählen wir für den freien $\mathbb{Z}_p[G]$-Modul $\operatorname{Hom}(\mathbb{Z}_p[G]c, \mathbb{Z}_p)$ (bzw. für $\operatorname{Hom}(\mathbb{Z}_p[G]c_i, \mathbb{Z}_p)$) das Basiselement b mit

$$b\Big(\sum_{\sigma\in G} a_\sigma \sigma\, c\Big) = a_1 \qquad \Big(\text{bzw. } b_i \text{ mit } b_i\Big(\sum_{\sigma\in G} a_\sigma \sigma\, c_i\Big) = a_1\Big)$$

so zeigt eine leichte Rechnung

$$\psi^*(b) = (\sigma-g)b_0 + (\tau-h(1+p^s))b_1. \qquad \text{q.e.d.}$$

§3 Die $\mathbb{Z}_p[G]$-Struktur von A(K).

Für eine pro-endliche Gruppe H sei H(p) die maximale pro-p-Faktorgruppe, $[H,H]$ die topologische Kommutatorgruppe und $H^{ab} = H/[H,H]$ die Faktorkommutatorgruppe. Eine exakte Sequenz

$$1 \longrightarrow H \longrightarrow E \longrightarrow G \longrightarrow 1$$

von pro-endlichen Gruppen induziert durch die Konjugation in E eine kanonische G-Modul-Struktur auf H^{ab}. Im Fall einer pro-p-Gruppe H wird H^{ab} dadurch zu einem $\mathbb{Z}_p[G]$-Modul.

Satz 3.1.: Sei k ein $\mathfrak{p}$-adischer Zahlkörper vom Grad n über $\mathbb{Q}_p$ und $\tilde{k}$ ein algebraischer Abschluß. Dann wird die absolute Galoisgruppe $G_k = \mathrm{Gal}(\tilde{k}/k)$ von k topologisch von n+3 Elementen erzeugt.

Beweis: Es genügt zu zeigen, daß für jede endliche galoissche Erweiterung K/k die Galoisgruppe $G = \mathrm{Gal}(K/k)$ von n+3 Elementen erzeugt wird. Denn ist für jedes derartige G die endliche Menge S(G) der (n+3)-Tupel $(s_1, \ldots, s_{n+3}) \in G^{n+3}$, die G erzeugen, nicht leer, so ist nach einem bereits zitierten Satz auch der projektive Limes $S = \varprojlim S(G)$ nicht leer. Ein Element von S ist aber ein System von n+3 topologischen Erzeugenden von G_k.

Da nach dem Burnside'schen Basissatz eine p-Gruppe H von Elementen $s_1, \ldots, s_m$ erzeugt wird, wenn deren Restklassen H^{ab} erzeugen, genügt es weiter, Erweiterungen mit abelscher Verzweigungsgruppe G_1 zu betrachten. Wird in der exakten Sequenz

$$1 \longrightarrow G_1 \longrightarrow G \longrightarrow \bar{G} \longrightarrow 1$$

G_1 als $\mathbb{Z}_p[\bar{G}]$-Modul von r Elementen und $\bar{G}$ als Gruppe von s Elementen erzeugt, so läßt sich G offenbar durch r+s Elemente erzeugen.

Es ist aber $\bar{G}$ die Galoisgruppe einer zahm-verzweigten Erweiterung und wird daher von 2 Elementen erzeugt, während G_1 nach lokaler Klassenkörpertheorie, auch als $\mathbb{Z}_p[\bar{G}]$-Modul, isomorph zu einer Faktorgruppe der Einseinheitengruppe U_V^1 des Verzweigungskörpers V von K/k ist; nach Satz 2.2. c.) gilt also $d_{\bar{G}}(G_1) \leq n+1$.

q.e.d.

Sei k ein $\mathfrak{p}$-adischer Zahlkörper über $\mathbb{Q}_p$ und K/k eine beliebige endliche Erweiterung. Es ist für die folgenden Untersuchungen zweckmäßig, nicht die multiplikative Gruppe K^* selbst, sondern deren totale pro-endliche Vervollständigung

$$\widehat{K^*} = \varprojlim_m K^*/K^{*m}$$

zu betrachten. Anschaulich geht $\widehat{K^*}$ aus K^* hervor, indem man bei einem fest gewählten Primelement auch Exponenten aus $\hat{\mathbb{Z}}$, der totalen pro-endlichen Vervollständigung von $\mathbb{Z}$, zuläßt. Genauer ist $\widehat{K^*}$ durch das kommutative Diagramm

$$\begin{array}{ccccccccc} 1 & \longrightarrow & U_K & \longrightarrow & K^* & \xrightarrow{v} & \mathbb{Z} & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & U_K & \longrightarrow & \widehat{K^*} & \xrightarrow{\hat{v}} & \hat{\mathbb{Z}} & \longrightarrow & 0 \end{array}$$

bestimmt, in dem U_K die Einheitengruppe und v die additive Bewertungsfunktion von K ist. Insbesondere betrachten wir den p-primären Anteil A(K) von $\widehat{K^*}$; es ist

$$A(K) = \varprojlim_r K^*/K^{*p^r}$$

die pro-p-Vervollständigung von K^* und wir haben die exakte Sequenz

$$1 \longrightarrow U_K^1 \longrightarrow A(K) \xrightarrow{\hat{v}} \mathbb{Z}_p \longrightarrow 0.$$

Nach der lokalen Klassenkörpertheorie liefert das universelle Normrestsymbol ω_K eine topologische Isomorphie

$$\hat{K}^* \xrightarrow{\omega_K} G_K^{ab}$$

zwischen $\hat{K}^*$ und der Galoisgruppe der maximalen abelschen Erweiterung von K. Ist K/k galoissch mit Galoisgruppe G, so ist ω_K auch ein G-Isomorphismus, wenn G auf G_K^{ab} vermöge der exakten Sequenz

$$1 \longrightarrow G_K \longrightarrow G_k \longrightarrow G \longrightarrow 1$$

operiert. Insbesondere liefert ω_K einen $\mathbb{Z}_p[G]$-Isomorphismus

$$A(K) \xrightarrow{\omega_K} G_K^{ab}(p) \cong G_K(p)^{ab}$$

zwischen A(K) und der Galoisgruppe der maximalen abelschen p-Erweiterung von K.

Wählen wir nach Satz 3.1. mit $n = [k:\mathbb{Q}_p]$ eine Surjektion

$$\hat{F}_{n+3} \twoheadrightarrow G_k$$

von der freien pro-endlichen Gruppe $\hat{F}_{n+3}$ mit n+3 freien Erzeugenden auf G_k, so induziert die kanonische Projektion von G_k auf G ein kommutatives Diagramm

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \hat{R}_{n+3} & \longrightarrow & \hat{F}_{n+3} & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & G_K & \longrightarrow & G_k & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

mit exakten Zeilen. Die daraus entstehende Abbildung

$$\varphi: \hat{R}_{n+3}^{ab} \twoheadrightarrow G_K^{ab}$$

ist ein surjektiver G-Homomorphismus; sei $Y := \operatorname{Ker} \varphi$.

Satz 3.2.: Y ist kohomologisch trivial.

Der Beweis dieses Satzes beruht auf der Tatsache, daß sowohl $\hat{F}_{n+3}$ als auch G_k sogenannte "malleable groups" sind. Dieses kohomologische Konzept stammt von Kawada [19], die Benennung von Brumer [6]. Im folgenden wird malleable mit formierbar übersetzt, da "malleable" etwa "formbar, schmiedbar, schmiegsam" bedeutet und eine solche Gruppe eine kanonische Klassenformation liefert.

Definition 3.3.: Eine pro-endliche Gruppe H heißt formierbar (engl. malleable), wenn für alle offenen Untergruppen $V \subseteq U$ von H, für die V normal in U ist, gilt:

a.) $H^1(U/V, V^{ab}) = 0$,

b.) $H^2(U/V, V^{ab}) \cong \mathbb{Z}/(U:V)\mathbb{Z}$,

c.) $H^2(U/V, V^{ab})$ wird von der Kohomologieklasse $\varkappa$ erzeugt, die der Gruppenerweiterung $1 \longrightarrow V^{ab} \longrightarrow U/[V,V] \longrightarrow U/V \longrightarrow 1$ zugeordnet ist.

Aus dem Satz von Tate und Nakayama, siehe [26] Chap. IX §8, folgt:

Lemma 3.4.: Die Aussagen a.) - c.) sind äquivalent dazu, daß das Cupprodukt mit $\varkappa$ einen Isomorphismus

$$\varkappa \cup \; : \; H^r(U/V, \mathbb{Z}) \xrightarrow{\sim} H^{r+2}(U/V, V^{ab})$$

der Tate'schen Kohomologiegruppen für alle $r \in \mathbb{Z}$ vermittelt.

Satz 3.5.: Eine freie pro-endliche Gruppe $\hat{F}$ und die absolute Galoisgruppe G_k eines $\mathfrak{p}$-adischen Zahlkörpers k sind formierbar.

Beweis: Für G_k folgt dies aus der Proposition von Weil-Šafarevič, s. [1] Chap. XV Th. 6, und für freie Gruppen ist dies ein Ergebnis von Tate, s. Kawada [19] Th. A. Vergleiche für beides auch Brumer [6] Th. 6.1., 6.4. und Cor. 6.6..

Beweis von Satz 3.2.:

Nach Satz 3.5. und Lemma 3.4. gilt für eine Untergruppe g von G

$$H^1(g,G_K^{ab}) = 0 \quad \text{und} \quad H^3(g,\hat{R}_{n+3}^{ab}) \cong H^1(g,\mathbb{Z}) = 0.$$

Aus der exakten Sequenz

$$0 \longrightarrow Y \longrightarrow \hat{R}_{n+3}^{ab} \xrightarrow{\varphi} G_K^{ab} \longrightarrow 0$$

von G-Moduln folgt daher die lange exakte Kohomologiesequenz

$$0 \longrightarrow H^2(g,Y) \longrightarrow H^2(g,\hat{R}_{n+3}^{ab}) \xrightarrow{\varphi^*} H^2(g,G_K^{ab}) \longrightarrow H^3(g,Y) \longrightarrow 0.$$

Sind U bzw. G_L die Urbilder von g in $\hat{F}_{n+3}$ bzw. G_k bei den jeweiligen Projektionen auf G, und ist in dem kommutativen Diagramm

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \hat{R}_{n+3}^{ab} & \longrightarrow & U/[\hat{R}_{n+3},\hat{R}_{n+3}] & \longrightarrow & g & \longrightarrow & 1 \\ & & \varphi\downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & G_K^{ab} & \longrightarrow & G_L/[G_K,G_K] & \longrightarrow & g & \longrightarrow & 1 \end{array}$$

$\chi_1 \in H^2(g,\hat{R}_{n+3}^{ab})$ der oberen und $\chi_2 \in H^2(g,G_K^{ab})$ der unteren Gruppenerweiterung zugeordnet, so gilt gerade $\varphi^*(\chi_1) = \chi_2$. Da $\hat{F}_{n+3}$ und G_k formierbar sind, erzeugen beide Elemente gerade die jeweiligen Kohomologiegruppen, die von der gleichen Ordnung (g:1) sind. Daher ist φ^* ein Isomorphismus, und es gilt

$$H^2(g,Y) = H^3(g,Y) = 0.$$

Da dies für alle Untergruppen von G gilt, erhalten wir mit einem bekannten Satz von Tate die kohomologische Trivialität von Y. q.e.d.

Wir wollen nun die Struktur der G-Moduln in der exakten Sequenz

$$0 \longrightarrow Y \longrightarrow \hat{R}_{n+3}^{ab} \longrightarrow \hat{K}^* \longrightarrow 1$$

für $\hat{K}^* \cong G_K^{ab}$ weiter untersuchen. Die Struktur von $\hat{R}_{n+3}^{ab}$ hängt nur von G und n ab und läßt sich aus einer diskreten freien Darstellung von G gewinnen:

Satz 3.6.: Sind

$$1 \longrightarrow R_m \longrightarrow F_m \longrightarrow G \longrightarrow 1$$

bzw. $$1 \longrightarrow \hat{R}_m \longrightarrow \hat{F}_m \longrightarrow G \longrightarrow 1$$

zwei beliebige Darstellungen der endlichen Gruppe G durch eine freie diskrete Gruppe F_m bzw. eine freie pro-endliche Gruppe $\hat{F}_m$, mit m freien Erzeugenden, so gilt die $\hat{\mathbb{Z}}[G]$-Isomorphie

$$\hat{R}_m^{ab} \cong \hat{\mathbb{Z}} \otimes R_m^{ab}.$$

Beweis: Induziert die obere Sequenz durch pro-endliche Vervollständigung gerade die untere, so folgt die Aussage unmittelbar, siehe auch den Anhang über pro-endliche Vervollständigungen. Ist aber

$$1 \longrightarrow R_m' \longrightarrow F_m' \longrightarrow G \longrightarrow 1$$

eine weitere Darstellung von G durch eine freie diskrete Gruppe mit m freien Erzeugenden, so folgt für jede Primzahl q die Isomorphie

$$\mathbb{Z}_q \otimes R_m'^{ab} \cong \mathbb{Z}_q \otimes R_m^{ab}$$

und wegen $\hat{\mathbb{Z}} = \prod_q \mathbb{Z}_q$ damit auch die Isomorphie $\hat{\mathbb{Z}} \otimes R_m'^{ab} \cong \hat{\mathbb{Z}} \otimes R_m^{ab}$ aus den folgenden beiden Lemmata:

Lemma 3.7.: Sei $1 \longrightarrow R_m \longrightarrow F_m \longrightarrow G \longrightarrow 1$ eine Darstellung der endlichen Gruppe G durch eine freie diskrete Gruppe F_m mit m freien Erzeugenden. Dann gibt es eine exakte Sequenz von $\mathbb{Z}[G]$-Moduln

$$0 \longrightarrow R_m^{ab} \longrightarrow \mathbb{Z}[G]^m \longrightarrow I_G \longrightarrow 0,$$

wobei $I_G = \left\{ \sum_{s \in G} a_s s \in \mathbb{Z}[G];\ \sum_{s \in G} a_s = 0 \right\}$ das Augmentationsideal von $\mathbb{Z}[G]$ ist.

Beweis: Dies folgt z.B. aus der Gruenberg-Auflösung von $\mathbb{Z}$, [10] Chap. 3 Th. 2 und die Bem. auf p.37, oder aus Ergebnissen von Lyndon [22] §4.

Lemma 3.8.: Sind $1 \longrightarrow R_m \longrightarrow F_m \longrightarrow G \longrightarrow 1$

und $1 \longrightarrow R_k \longrightarrow F_k \longrightarrow G \longrightarrow 1$

Darstellungen der endlichen Gruppe G durch freie diskrete Gruppen mit m bzw. k Erzeugenden, etwa $k \geq m$, so gilt für eine Primzahl q die $\mathbb{Z}_q[G]$-Isomorphie

$$\mathbb{Z}_q \otimes R_k^{ab} \cong \mathbb{Z}_q \otimes R_m^{ab} \oplus \mathbb{Z}_q[G]^{k-m}.$$

Beweis: Aus Lemma 3.7. folgt mit dem Lemma von Schanuel

$$R_k^{ab} \oplus \mathbb{Z}[G]^m \cong R_m^{ab} \oplus \mathbb{Z}[G]^k,$$

durch Tensorieren mit $\mathbb{Z}_q$ also

$$\mathbb{Z}_q \otimes R_k^{ab} \oplus \mathbb{Z}_q[G]^m \cong \mathbb{Z}_q \otimes R_m^{ab} \oplus \mathbb{Z}_q[G]^k.$$

Der semi-lokale Kürzungssatz 1.5. liefert dann die Behauptung.

Wir setzen im folgenden für eine Primzahl q $(R_m^{ab})_q := \mathbb{Z}_q \otimes R_m^{ab}$.

Bemerkung 3.9.: Über den sogenannten Relationenmodul R_m^{ab} gibt es umfangreiche Literatur; seine G-Struktur ist mit interessanten gruppen- und darstellungstheoretischen Problemen verknüpft, s. Gruenberg [11] . Während nach den obigen Lemmata die $\mathbb{Z}_q[G]$-Struktur von $(R_m^{ab})_q$ nicht von der Wahl der freien Darstellung

$$1 \longrightarrow R_m \longrightarrow F_m \longrightarrow G \longrightarrow 1$$

abhängt, weiß man nicht, ob dies allgemein auch für die $\mathbb{Z}[G]$-Struktur von R_m^{ab} gilt, vergl. [11] Lect. 5.

Aus der exakten Sequenz von G-Moduln

$$1 \longrightarrow U_K \longrightarrow \hat{K}^* \xrightarrow{\hat{v}} \hat{\mathbb{Z}} \longrightarrow 0$$

erhalten wir für eine Primzahl $q \neq p$ die exakte Sequenz der q-primären Anteile

$$1 \longrightarrow \mu_K^q \longrightarrow \hat{K}^*(q) \longrightarrow \mathbb{Z}_q \longrightarrow 0,$$

wobei μ_K^q die Gruppe der in K enthaltenen Einheitswurzeln von q-Potenzordnung bezeichnet. Diese Sequenz zerfällt im allgemeinen nicht, aber die Struktur von $\hat{K}^*(q)$ kann auf andere Weise leicht angegeben werden: $\hat{K}^*(q)$ ist isomorph zur pro-q-Vervollständigung von K^*, und da U_K^1 eine pro-p-Gruppe ist, ist die pro-q-Vervollständigung von K^* gleich der von K^*/U_K^1. Da K^*/U_K^1 ein endlich erzeugter $\mathbb{Z}$-Modul ist, folgt die $\mathbb{Z}_q[G]$-Isomorphie

$$\hat{K}^*(q) \quad \cong \quad \mathbb{Z}_q \otimes (K^*/U_K^1),$$

vgl. den Anhang. Die G-Struktur von K^*/U_K^1 ist aber einfach: Die Verzweigungsgruppe G_1 von G operiert trivial auf diesem Modul, und für die Operation der zahm-verzweigten Gruppe G/G_1 siehe Hasse [12] §16. Unser Interesse gilt daher dem p-primären Anteil A(K) von $\hat{K}^*$. Für ihn erhalten wir nun als Hauptergebnis dieses Paragraphen:

Satz 3.10.: Sei k ein $\mathfrak{p}$-adischer Zahlkörper vom Grad n über $\mathbb{Q}_p$, K/k eine endliche galoissche Erweiterung mit Galoisgruppe G und

$$1 \longrightarrow R_{n+3} \longrightarrow F_{n+3} \longrightarrow G \longrightarrow 1$$

eine Darstellung von G durch eine freie diskrete Gruppe F_{n+3} mit n+3 freien Erzeugenden. Dann gibt es eine exakte Sequenz

$$0 \longrightarrow \mathbb{Z}_p[G]^2 \longrightarrow (R_{n+3}{}^{ab})_p \longrightarrow A(K) \longrightarrow 0.$$

Beweis: Aus der exakten Sequenz von G-Moduln

$$0 \longrightarrow Y \longrightarrow \hat{R}_{n+3}{}^{ab} \longrightarrow \hat{K}^* \longrightarrow 0$$

erhalten wir mit X := Y(p) die exakte Sequenz

$$0 \longrightarrow X \longrightarrow (R_{n+3}{}^{ab})_p \longrightarrow A(K) \longrightarrow 0$$

der p-primären Anteile. X ist torsionsfrei als Untermodul von $(R_{n+3}{}^{ab})_p$ und nach Satz 3.2. kohomologisch trivial, nach Lemma 1.4. also projektiv. Um zu zeigen, daß $X \cong \mathbb{Z}_p[G]^2$ ist, genügt es daher nach dem Lemma von Swan, zu zeigen, daß $\mathbb{Q}_p \otimes X \cong \mathbb{Q}_p[G]^2$ ist. Aus Lemma 3.7. und der kanonischen exakten Sequenz

$$0 \longrightarrow I_G \longrightarrow \mathbb{Z}[G] \xrightarrow{\text{Aug}} \mathbb{Z} \longrightarrow 0$$

folgt durch Tensorieren mit $\mathbb{Q}_p$ leicht

$$\mathbb{Q}_p \otimes (R_{n+3}{}^{ab})_p \cong \mathbb{Q}_p \otimes_{\mathbb{Z}} R_{n+3}{}^{ab} \cong \mathbb{Q}_p[G]^{n+2} \oplus \mathbb{Q}_p.$$

Dies ist ein klassisches Resultat von Gaschütz, vergl. [11] Th. 2.7.. Andererseits folgt aus der exakten Sequenz

$$1 \longrightarrow U_K^1 \longrightarrow A(K) \longrightarrow \mathbb{Z}_p \longrightarrow 0$$

und Satz 2.1. b.) die Isomorphie

$$\mathbb{Q}_p \otimes A(K) \cong \mathbb{Q}_p \otimes U_K^1 \oplus \mathbb{Q}_p \cong \mathbb{Q}_p[G]^n \oplus \mathbb{Q}_p.$$

Aus der Isomorphie $\mathbb{Q}_p \otimes X \oplus \mathbb{Q}_p \otimes A(K) = \mathbb{Q}_p \otimes (R_{n+3}{}^{ab})_p$ folgt daher in der Tat $\mathbb{Q}_p \otimes X \cong \mathbb{Q}_p[G]^2$. q.e.d.

Für reguläre Körper K erhalten wir aus diesem Satz die vollständige Beschreibung der $\mathbb{Z}_p[G]$-Struktur von A(K); insbesondere zeigt es sich, daß diese nur von n und G abhängt:

Satz 3.11.: Sei K/k eine endliche galoissche Erweiterung regulärer $\mathfrak{p}$-adischer Zahlkörper über $\mathbb{Q}_p$ und $n = [k:\mathbb{Q}_p]$, dann gilt:

a.) $G = \mathrm{Gal}(K/k)$ kann durch n+2 Elemente erzeugt werden.

b.) Ist $1 \longrightarrow R_{n+2} \longrightarrow F_{n+2} \longrightarrow G \longrightarrow 1$ eine Darstellung von G durch eine freie diskrete Gruppe F_{n+2} mit n+2 freien Erzeugenden, so gilt die $\mathbb{Z}_p[G]$-Isomorphie

$$A(K) \oplus \mathbb{Z}_p[G] \cong (R_{n+2}{}^{ab})_p.$$

c.) Wird G von n+1 Elementen erzeugt und ist

$$1 \longrightarrow R_{n+1} \longrightarrow F_{n+1} \longrightarrow G \longrightarrow 1$$

eine Darstellung mit einer freien Gruppe F_{n+1} mit n+1 freien Erzeugenden, so gilt die $\mathbb{Z}_p[G]$-Isomorphie

$$A(K) \cong (R_{n+1}{}^{ab})_p.$$

Beweis: a.) folgt mit den gleichen Schlüssen wie im Beweis von Satz 3.1., wenn man beachtet, daß für reguläres K nach Satz 2.2. d.) $d_{\bar{G}}(U_V^1) = n$ für die Einseinheitengruppe des Verzweigungskörpers V von K/k gilt, wobei $\bar{G} = \mathrm{Gal}(V/k)$ ist.

Für das weitere ist entscheidend, daß bei regulärem K der Modul A(K) torsionsfrei ist; daher gilt $\mathrm{Ext}^1_{\mathbb{Z}_p[G]}(A(K), \mathbb{Z}_p[G]^2) = 0$, vergl. Gruenberg [10] §10.1 Prop. 3, d.h., die Sequenz aus Satz 3.10. zerfällt, und wir erhalten

$$A(K) \oplus \mathbb{Z}_p[G]^2 \cong (R_{n+3}{}^{ab})_p.$$

Alles weitere folgt aus Lemma 3.8. und dem semi-lokalen Kürzungssatz.

Der Vollständigkeit halber soll noch erwähnt werden, daß sich das Ergebnis von Lesev [31] noch verschärfen läßt:

Satz 3.12.: Sei K/k eine endliche galoissche Erweiterung regulärer $\mathfrak{p}$-adischer Zahlkörper über $\mathbb{Q}_p$, $G = \mathrm{Gal}(K/k)$ und $n = [k:\mathbb{Q}_p]$, dann sind die folgenden Aussagen äquivalent:

a.) $A(K) \cong \mathbb{Z}_p \oplus \mathbb{Z}_p[G]^n$.

b.) G besitzt eine zyklische p-Sylowgruppe G_p und die Verzweigungsgruppe G_1 liegt im Zentrum von G.

Beweis: Sei G_p eine p-Sylowgruppe von G, dann folgt mit der lokalen Klassenkörpertheorie aus a.):

$$G_p^{ab} \cong \hat{H}^0(G_p,K^*) \cong \hat{H}^0(G_p,A(K)) \cong \mathbb{Z}/(G_p:1)\mathbb{Z}.$$

Dies kann nur sein, wenn G_p zyklisch ist. Weiter folgt aus dem kommutativen Diagramm

$$\begin{array}{ccc} \hat{H}^0(G_p,A(K)) & \xrightarrow[\sim]{\mathrm{Cor}} & \hat{H}^0(G,A(K)) \\ \downarrow\wr & & \| \\ & & \hat{H}^0(G,K^*)(p) \\ G_p & \longrightarrow & G^{ab}(p) \quad \| \wr \end{array}$$

daß die untere, von der Inklusion $G_p \subseteq G$ induzierte Abbildung ein Isomorphismus ist. Aus der Injektivität folgt $G_p \cap [G,G] = 1$, also auch $[G_1,G] = 1$, denn da G_1 Normalteiler und p-Gruppe ist, gilt $[G_1,G] \subseteq G_1 \subseteq G_p$; dies bedeutet aber gerade, daß G_1 im Zentrum von G liegt.

Ist umgekehrt b.) erfüllt und G_0 die Trägheitsgruppe von G, so folgt zunächst $G_0 = G_1 \times G_0/G_1$, und dies ist eine Zerlegung in G/G_0-Moduln. Da G_p und G/G_0 zyklisch sind und die Ordnung von G_0/G_1 prim zu p ist, erhält man weiter leicht, daß die von der Inklusion induzierte Abbildung $G_p \longrightarrow G^{ab}(p)$ ein Isomorphis-

mus ist, insbesondere gilt

$$\hat{H}^0(G,A(K)) \cong G^{ab}(p) \cong \mathbb{Z}/(G_p:1)\mathbb{Z}.$$

Sei $z \in A(K)^G$ derart gewählt, daß die Restklasse von z die Gruppe $\hat{H}^0(G,A(K))$ erzeugt. Ist Z der von z erzeugte Untermodul und $C = A(K)/Z$, so gilt $Z \cong \mathbb{Z}_p$, und C ist torsionsfrei, da A(K) torsionsfrei und z keine p-Potenz ist. Wegen $H^{-1}(G_p,A(K)) \cong H^1(G_p,A(K)) = 0 = H^1(G,Z)$ erhalten wir die exakte Sequenz

$$0 \longrightarrow H^{-1}(G_p,C) \longrightarrow \hat{H}^0(G_p,Z) \xrightarrow{i^*}_{\sim} \hat{H}^0(G_p,A(K)) \longrightarrow \hat{H}^0(G_p,C) \longrightarrow 0,$$

in der die Abbildung i^* nach Wahl von z ein Isomorphismus ist. Daraus folgt $H^{-1}(G_p,C) = \hat{H}^0(G_p,C) = 0$ und also die kohomologische Trivialität von C unter G, da C p-primär ist. Weiter folgt aus der exakter Sequenz

$$(*) \qquad 0 \longrightarrow Z \longrightarrow A(K) \longrightarrow C \longrightarrow 0$$

durch Tensorieren mit $\mathbb{Q}_p$ die Isomorphie $\mathbb{Q}_p \otimes C \cong \mathbb{Q}_p[G]^n$. Daraus folgt mit Bemerkung 1.7. b.) $C \cong \mathbb{Z}_p[G]^n$, weiter zerfällt die Sequenz (*), und wir erhalten a.). q.e.d.

§4 Die absolute Galoisgruppe $\mathfrak{p}$-adischer Zahlkörper.

Sei in diesem Paragraphen k ein $\mathfrak{p}$-adischer Zahlkörper vom Grad n und Restklassengrad f über $\mathbb{Q}_p$, $\tilde{k}$ ein algebraischer Abschluß von k und $G_k = \mathrm{Gal}(\tilde{k}/k)$ die absolute Galoisgruppe von k. Sei ferner V der Verzweigungskörper von $\tilde{k}/k$, also das Kompositum aller endlichen zahm-verzweigten Erweiterungen von k in $\tilde{k}$ und $V_k = \mathrm{Gal}(\tilde{k}/V)$ die Verzweigungsgruppe von G_k.

Nach Iwasawa [14] ist $\mathcal{G} = \mathrm{Gal}(V/k)$ eine pro-endliche Gruppe mit zwei Erzeugenden σ und τ und der definierenden Relation

$$\sigma \tau \sigma^{-1} = \tau^{p^f}$$

d.h., die totale pro-endliche Vervollständigung einer diskreten Gruppe mit diesen Eigenschaften. Dies folgt, da $\mathcal{G}$ der projektive Limes der Galoisgruppen aller endlichen zahm-verzweigten Erweiterungen von k ist, leicht aus den Resultaten von Hasse [12] §16.

Die von τ erzeugte abgeschlossene zyklische Untergruppe $\mathcal{G}_0$ ist ein Normalteiler, und es gilt

$$\mathcal{G}_0 \cong \prod_{q \neq p} \mathbb{Z}_q .$$

Die Faktorgruppe $\mathcal{G}/\mathcal{G}_0$ ist als Galoisgruppe der maximalen unverzweigten Erweiterung von k isomorph zu $\hat{\mathbb{Z}}$.

Satz 4.1.: Es gilt $\mathrm{cd}_p(\mathcal{G}) = 1$.

Beweis: Aus der exakten Sequenz $1 \longrightarrow \mathcal{G}_0 \longrightarrow \mathcal{G} \longrightarrow \hat{\mathbb{Z}} \longrightarrow 0$ folgt mit Serre [27] I 3.3. Prop. 15:

$$\mathrm{cd}_p(\mathcal{G}) \leq \mathrm{cd}_p(\mathcal{G}_0) + \mathrm{cd}_p(\hat{\mathbb{Z}}) = 0 + 1 = 1,$$

da die p-Sylowgruppe von $\mathcal{G}_0$ trivial und $\hat{\mathbb{Z}}$ eine freie pro-p-Gruppe ist; $\mathrm{cd}_p(\mathcal{G}) = 0$ ist offenbar nicht möglich.

Satz 4.2. (Iwasawa): V_k ist eine freie pro-p-Gruppe und die exakte Sequenz $1 \longrightarrow V_k \longrightarrow G_k \longrightarrow \mathcal{G} \longrightarrow 1$ zerfällt.

Beweis: Wir verkürzen den ursprünglichen Beweis von Iwasawa [14], indem wir Ergebnisse aus der Galoiskohomologie benutzen.

Als projektiver Limes der Verzweigungsgruppen endlicher Erweiterungen ist V_k offenbar eine pro-p-Gruppe. Da der Restklassenkörper von V algebraisch abgeschlossen ist, ist die Brauergruppe von V gleich Null, s. [26] Chap.XII §3 Prop. 3; und da dies auch für alle endlichen Erweiterungen von V gilt, ist $cd_p(V_k) \leq 1$, s. Serre [27] Chap. II Prop. 5. daraus folgt wiederum, daß V_k eine freie pro-p-Gruppe ist, s. [27] Chap. I 4.2. Cor. 2.

Die Sequenz zerfällt wegen $cd_p(\mathcal{G}) = 1$, s. [27] Chap. I Prop. 16.

Dieser Satz liefert natürlich noch nicht die Struktur von G_k; dazu müßte man noch die Wirkung der inneren Automorphismen von G_k auf V_k kennen. Immerhin weiß man, wie $\mathcal{G}$ auf V_k^{ab} operiert, indem man die Ergebnisse aus §2 benutzt:

Sei $\mathcal{H}$ eine offene Untergruppe von $\mathcal{G}$ und $K = V^{\mathcal{H}}$ die entsprechende zahm-verzweigte Erweiterung von k mit Galoisgruppe $G = \mathcal{G}/\mathcal{H}$, dann ist das Bild der Einseinheitengruppe U_K^1 unter dem universellen Normrestsymbol ω_K die Verzweigungsgruppe von G_K^{ab}, siehe Serre [26] Chap. XV Th. 2. Diese ist aber nach dem Lemma von Herbrand das Bild der Verzweigungsgruppe von G_K in G_K^{ab}, die Verzweigungsgruppe von G_K ist aber ebenfalls V_k wegen $K \subseteq V$. Wir erhalten daher einen $\mathbb{Z}_p[G]$-Isomorphismus

$$U_K^1 \xrightarrow[\sim]{\omega_K} V_k[G_K, G_K]/[G_K, G_K].$$

Für einen Oberkörper $V \supset L \supset K$ erhalten wir nach der Klassenkörpertheorie ein kommutatives Diagramm

$$\begin{array}{ccc} U_L^1 & \longrightarrow & V_k[G_L, G_L]/[G_L, G_L] \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle \text{kan.}} \\ U_K^1 & \longrightarrow & V_k[G_K, G_K]/[G_K, G_K]. \end{array}$$

Der projektive Limes der rechten Gruppen ist V_k^{ab}; dies folgt wegen $\varprojlim_{\mathfrak{p}} \mathfrak{p}^{ab} = 1$ und der Exaktheit des projektiven Limes für profendliche Gruppen aus den exakten Sequenzen

$$1 \longrightarrow V_k[G_K, G_K]/[G_K, G_K] \longrightarrow G_K^{ab} \longrightarrow \mathfrak{p}^{ab} \longrightarrow 1$$

und der Tatsache, daß für ein projektives System $(H_\alpha)_{\alpha \in A}$ von profendlichen Gruppen $\varprojlim H_\alpha^{ab} = (\varprojlim H_\alpha)^{ab}$ gilt; dies ist dual zur Eigenschaft $\varinjlim H^1(H_\alpha, \mathbb{Q}/\mathbb{Z}) = H^1(\varprojlim H_\alpha, \mathbb{Q}/\mathbb{Z})$.

Wir erhalten also einen topologischen Isomorphismus

$$V_k^{ab} \cong \varprojlim_{\substack{K/k \text{ endl.} \\ \text{zahm-verzweigt}}} U_K^1$$

wobei der projektive Limes über die Normen zu bilden ist.

V_k^{ab} ist ein Modul über dem komplettierten Gruppenring

$$\mathbb{Z}_p[\![\mathcal{G}]\!] = \varprojlim \mathbb{Z}_p[\mathcal{G}/\mathfrak{p}]$$

wobei die Abbildungen des projektiven Systems von den kanonischen Projektionen der Gruppen induziert werden, vergl. Brumer [6]. Fassen wir auch die Einseinheitengruppen U_K^1 in natürlicher Weise als $\mathbb{Z}_p[\![\mathcal{G}]\!]$-Moduln auf, durch die Projektion von $\mathbb{Z}_p[\![\mathcal{G}]\!]$ auf $\mathbb{Z}_p[G]$, so ist der obige Isomorphismus ein $\mathbb{Z}_p[\![\mathcal{G}]\!]$-Isomorphismus.

Aus Satz 2.3. folgt nun:

Satz 4.3.: Es gibt eine exakte Sequenz von $\mathbb{Z}_p[\![G]\!]$-Moduln

$$0 \longrightarrow \mathbb{Z}_p[\![G]\!] \longrightarrow \mathbb{Z}_p[\![G]\!]^{n+1} \longrightarrow V_k^{ab} \longrightarrow 0.$$

Ist ζ eine primitive Einheitswurzel von maximaler p-Potenzordnung in V und $g \in \mathbb{Z}_p$ sowie h eine (p-1)-te Einheitswurzel aus $\mathbb{Z}_p$ mit

$$\sigma(\zeta) = \zeta^g \qquad \tau(\zeta) = \zeta^h ,$$

so gibt es genauer eine exakte Sequenz

$$0 \longrightarrow \mathbb{Z}_p[\![G]\!]\, b \longrightarrow \bigoplus_{i=0}^{n} \mathbb{Z}_p[\![G]\!]\, b_i \longrightarrow V_k^{ab} \longrightarrow 0$$

$$b \longmapsto (\sigma-g)b_0 + (\tau-h(1+p^s))b_1 ,$$

d.h., V_k^{ab} besitzt $\mathbb{Z}_p[\![G]\!]$-Erzeugende $\bar{y}_0, \ldots, \bar{y}_n$ mit der einzigen definierenden Relation

$$\bar{y}_0^{\sigma-g}\, \bar{y}_1^{\tau-h(1+p^s)} = 1.$$

Beweis: Zunächst ist die Gruppe μ_V der in V enthaltenen Einheitswurzeln von p-Potenzordnung endlich, da die Erweiterung $\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p$, die durch Adjunktion aller Einheitswurzeln von p-Potenzordnung entsteht, rein-verzweigt ist. Wählen wir in Satz 2.3. für alle zahm-verzweigten Erweiterungen K/k, die μ_V enthalten, die Darstellung von U_K^1 mit den oben beschriebenen g und h, so folgt die Aussage des Satzes durch Übergang zum projektiven Limes, da diese U_K^1 ein cofinales System bilden und für Körper $K' \supseteq K$ mit $G' = \mathrm{Gal}(K'/k)$ und $G = \mathrm{Gal}(K/k)$ die entstehenden Diagramme

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathbb{Z}_p[G'] & \longrightarrow & \mathbb{Z}_p[G']^{n+1} & \longrightarrow & U_{K'}^1 \longrightarrow 1 \\ & & \downarrow \mathrm{pr} & & \downarrow \mathrm{pr} & & \downarrow N_{K'/K} \\ 0 & \longrightarrow & \mathbb{Z}_p[G] & \longrightarrow & \mathbb{Z}_p[G]^{n+1} & \longrightarrow & U_K^1 \longrightarrow 1 \end{array}$$

mit den kanonischen Projektionen pr kommutativ sind.

Corollar 4.4.: V_k wird als Normalteiler von G_k von $n+1$ Elementen erzeugt.

Dies folgt sofort aus Satz 4.3. und dem folgenden

Lemma 4.5.: Sei $1 \longrightarrow H \longrightarrow E \longrightarrow G \longrightarrow 1$ eine exakte Sequenz von pro-endlichen Gruppen mit einer pro-p-Gruppe H, dann sind die folgenden Aussagen äquivalent:

a.) H wird als Normalteiler in E von $y_1, \ldots, y_m$ erzeugt.

b.) H^{ab} wird als $\mathbb{Z}_p[\![G]\!]$-Modul von den Restklassen $\bar{y}_1, \ldots, \bar{y}_m$ der y_i erzeugt.

Beweis: Sei H' der von $y_1, \ldots, y_m$ (topologisch) erzeugte Normalteiler. Nach dem Burnside'schen Basissatz, vergl. [27] Chap. I Prop. 23, ist die Inklusion $i: H' \hookrightarrow H$ genau dann surjektiv, wenn die induzierte Abbildung $\bar{i} : H'^{ab} \longrightarrow H^{ab}$ surjektiv ist. Da H' alle Konjugierten der y_i enthält und abgeschlossen ist, ist Im $\bar{i}$ gerade der von den $\bar{y}_i$ erzeugte $\mathbb{Z}_p[\![G]\!]$-Untermodul.q.e.d.

Zur weiteren Untersuchung der Galoisgruppe G_k konstruieren wir nun eine Gruppe $P_\mathcal{G}$, die G_k besser angepaßt ist als eine freie Gruppe, aber noch gewisse universelle Eigenschaften besitzt:

Freie Produkte pro-endlicher Gruppen wurden von Neukirch in [24] eingeführt. Das freie pro-endliche Produkt $G*H$ pro-endlicher Gruppen G und H ist dadurch charakterisiert, daß es G und H als Untergruppen enthält und jeder Homomorphismus

$$f: G*H \longrightarrow Z$$

in eine pro-endliche Gruppe Z eindeutig durch zwei Homomorphismen

$$g\colon G \longrightarrow Z \qquad \text{und} \qquad h\colon H \longrightarrow Z$$

bestimmt ist, nämlich durch die Restriktionen von f auf G bzw. auf H. Wir schreiben dafür im folgenden

$$f = (g,h).$$

Sei $\hat{F}_{n+1}$ eine freie pro-endliche Gruppe mit n+1 freien Erzeugenden $z_0, \ldots, z_n$. Das freie Produkt

$$\hat{F}_{n+1} * \mathcal{G}$$

von $\hat{F}_{n+1}$ und $\mathcal{G}$ kann auch als die totale Vervollständigung der diskreten Gruppe mit Erzeugenden $r_0, \ldots, r_n$, s und t und der definierenden Relation $sts^{-1} = t^{p^f}$ aufgefaßt werden, s.d. Anh..

Sei Z der Kern der kanonischen Projektion

$$pr_2 = (1,id)\colon \hat{F}_{n+1} * \mathcal{G} \longrightarrow \mathcal{G},$$

dann wird Z als Normalteiler in $\hat{F}_{n+1} * \mathcal{G}$ von $z_0, \ldots, z_n$ erzeugt, s. Neukirch [24] Satz 1.2.. Sei I der Normalteiler von Z, für den $Z/I = Z(p)$ die maximale pro-p-Faktorgruppe ist, so ist I auch Normalteiler in $\hat{F}_{n+1} * \mathcal{G}$, und wir erhalten aus der exakten Sequenz

$$1 \longrightarrow Z \longrightarrow \hat{F}_{n+1} * \mathcal{G} \longrightarrow \mathcal{G} \longrightarrow 1$$

mit $P := Z(p) = Z/I$ und $P_{\mathcal{G}} := \hat{F}_{n+1} * \mathcal{G} / I$ die induzierte Sequenz

$$1 \longrightarrow P \longrightarrow P_{\mathcal{G}} \longrightarrow \mathcal{G} \longrightarrow 1.$$

Sind $x_0, \ldots, x_n$ die Bilder von $z_0, \ldots, z_n$ in P, so wird offenbar P als Normalteiler in $P_{\mathcal{G}}$ von den x_i erzeugt. Wir wollen nun die Gruppe $P_{\mathcal{G}}$ untersuchen und charakterisieren:

Satz 4.6.: Es gilt:

a.) $cd_p(P_{\mathcal{G}}) = 1$.

b.) P ist eine freie pro-p-Gruppe.

c.) P^{ab} ist ein freier $\mathbb{Z}_p[\![\mathcal{G}]\!]$-Modul mit Basis $\bar{x}_0, \ldots, \bar{x}_n$, wobei $\bar{x}_i = x_i[P,P]$ das Bild von x_i in P^{ab} bezeichnet.

d.) In der Kategorie der Gruppenerweiterungen E von $\mathcal{G}$ mit einer pro-p-Gruppe H, in der die Morpnismen kommutative Diagramme

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \longrightarrow & E & \longrightarrow & \mathcal{G} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & H' & \longrightarrow & E' & \longrightarrow & \mathcal{G} & \longrightarrow & 1 \end{array}$$

sind, ist $1 \longrightarrow P \longrightarrow P_{\mathcal{G}} \longrightarrow \mathcal{G} \longrightarrow 1$ freies Objekt, und zwar frei auf $x_0, \ldots, x_n$. Dies bedeutet, daß P von $x_0, \ldots, x_n$ als Normalteiler in $P_{\mathcal{G}}$ erzeugt wird und daß es zu jeder Gruppenerweiterung $1 \longrightarrow H \longrightarrow E \longrightarrow \mathcal{G} \longrightarrow 1$ und jedem Tupel $(t_0, \ldots, t_n)$ mit $t_i \in H$ einen Morphismus

$$\begin{array}{ccccccccc} 1 & \longrightarrow & P & \longrightarrow & P_{\mathcal{G}} & \longrightarrow & \mathcal{G} & \longrightarrow & 1 \\ & & f \downarrow & & f \downarrow & & \| & & \\ 1 & \longrightarrow & H & \longrightarrow & E & \longrightarrow & \mathcal{G} & \longrightarrow & 1 \end{array}$$

mit $f(x_i) = t_i$ gibt.

e.) Die Gruppenerweiterung $1 \longrightarrow P \longrightarrow P_{\mathcal{G}} \longrightarrow \mathcal{G} \longrightarrow 1$ (und daher auch die Gruppe $P_{\mathcal{G}}$) ist durch die Eigenschaft d.) bis auf Isomorphie eindeutig bestimmt.

Beweis: Sei A ein endlicher, p-primärer $P_{\mathcal{G}}$-Modul. Operiert $\hat{F}_{n+1} * \mathcal{G}$ durch triviale Operation von 1 auf A, so gilt

$$H^2(\hat{F}_{n+1} * \mathcal{G}, A) \cong H^2(\hat{F}_{n+1}, A) \times H^2(\mathcal{G}, A) = 0,$$

vergl. Satz 4.1. und Neukirch [24], sowie

$$H^1(I, A) = \mathrm{Hom}(I, A) = 0$$

wegen $I(p) = 1$. Aus der Hochschild-Serre-Spektralsequenz

$$H^1(I, A)^{P_{\mathcal{G}}} \longrightarrow H^2(P_{\mathcal{G}}, A) \longrightarrow H^2(\hat{F}_{n+1} * \mathcal{G}, A)$$

vergl. [27] I 2.6., folgt daher $H^2(P_{\mathcal{G}}, A) = 0$. Da dies für alle

endlichen, p-primären $P_{\mathcal{G}}$-Moduln A gilt, folgt $cd_p(P_{\mathcal{G}}) \leq 1$, wegen $P \neq 1$ also a.).

Daraus folgt für die abgeschlossene Untergruppe P $cd_p(P) \leq 1$, also b.). Wir zeigen nun zunächst d.):

Sei $1 \longrightarrow H \longrightarrow E \xrightarrow{\pi} \mathcal{G} \longrightarrow 1$ und ein Tupel $(t_0, \ldots, t_n)$ mit $t_i \in H$ gegeben, dann gibt es nach der universellen Eigenschaft freier pro-endlicher Gruppen einen Homomorphismus

$$h: \hat{F}_{n+1} \longrightarrow H \hookrightarrow E$$

mit $h(z_i) = t_i$. Weiter gibt es wegen $cd_p(\mathcal{G}) = 1$ einen Schnitt

$$s: \mathcal{G} \longrightarrow E$$

von π. Wir erhalten damit einen Homomorphismus

$$f' = (h,s): \hat{F}_{n+1} * \mathcal{G} \longrightarrow E,$$

der wegen $\pi \circ f' = (\pi \circ h, \pi \circ s) = (1, id) = pr_2$ ein kommutatives Diagramm

$$\begin{array}{ccccccccc} 1 & \longrightarrow & Z & \longrightarrow & \hat{F}_{n+1} * \mathcal{G} & \longrightarrow & \mathcal{G} & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f'} & & \| & & \\ 1 & \longrightarrow & H & \longrightarrow & E & \longrightarrow & \mathcal{G} & \longrightarrow & 1 \end{array}$$

induziert. Da H eine pro-p-Gruppe ist, faktorisiert sich f' über $P = Z(p)$ und wir erhalten den gewünschten Morphismus

$$\begin{array}{ccccccccc} 1 & \longrightarrow & P & \longrightarrow & P_{\mathcal{G}} & \longrightarrow & \mathcal{G} & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f} & & \| & & \\ 1 & \longrightarrow & H & \longrightarrow & E & \longrightarrow & \mathcal{G} & \longrightarrow & 1 \end{array}$$

mit $f(x_i) = t_i$.

c.): Da P als Normalteiler in $P_{\mathcal{G}}$ von $x_0, \ldots, x_n$ erzeugt wird, gibt es nach Lemma 4.5. einen surjektiven $\mathbb{Z}_p[\![\mathcal{G}]\!]$-Homomorphismus

$$g: \bigoplus_{i=0}^{n} \mathbb{Z}_p[\![\mathcal{G}]\!]\, b_i \longrightarrow\!\!\!\!\rightarrow P^{ab} \quad \text{mit} \quad g(b_i) = \bar{x}_i.$$

Wenden wir d.) auf die zerfallende Erweiterung

$$0 \longrightarrow \bigoplus_{i=0}^{n} \mathbb{Z}_p[\![\mathcal{G}]\!]\, b_i \longrightarrow E \longrightarrow \mathcal{G} \longrightarrow 1$$

an, so erhalten wir andererseits einen $\mathbb{Z}_p[\![\mathcal{G}]\!]$-Homomorphismus

$$\bar{f}: \; P^{ab} \longrightarrow \bigoplus_{i=0}^{n} \mathbb{Z}_p[\![\mathcal{G}]\!]\, b_i \quad \text{mit} \quad \bar{f}(\bar{x}_i) = b_i .$$

Wegen $\bar{f} \circ g = \mathrm{id}$ ist g also auch injektiv und liefert den gewünschten $\mathbb{Z}_p[\![\mathcal{G}]\!]$-Isomorphismus.

e.): Sei $1 \longrightarrow H \longrightarrow E \longrightarrow \mathcal{G} \longrightarrow 1$ eine Gruppenerweiterung, die in dem unter d.) beschriebenen Sinne frei auf $\{t_0, \ldots, t_n\} \subsetneq H$ ist, so erhalten wir zunächst einen Morphismus

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \longrightarrow & E & \longrightarrow & \mathcal{G} & \longrightarrow & 1 \\ & & \downarrow f & & \downarrow f & & \| & & \\ 1 & \longrightarrow & P & \longrightarrow & P_{\mathcal{G}} & \longrightarrow & \mathcal{G} & \longrightarrow & 1 \end{array}$$

mit $f(t_i) = x_i$. Weiter folgt wie unter c.), daß auch H^{ab} ein freier $\mathbb{Z}_p[\![\mathcal{G}]\!]$-Modul mit Basis $\bar{t}_0, \ldots, \bar{t}_n$ ist, $\bar{t}_i = t_i[H,H]$. Daher ist die induzierte Abbildung $\bar{f}: H^{ab} \longrightarrow P^{ab}$ ein Isomorphismus. Dies zeigt, daß f surjektiv ist und daß in der Spektralsequenz

$$0 \longrightarrow H^1(P, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{f^*} H^1(H, \mathbb{Z}/p\mathbb{Z}) \longrightarrow H^1(K, \mathbb{Z}/p\mathbb{Z})^P \longrightarrow H^2(P, \mathbb{Z}/p\mathbb{Z})$$

mit $K = \mathrm{Ker}\, f$ die induzierte Abbildung f^* ein Isomorphismus ist. Da wegen $\mathrm{cd}_p(P) = 1$ $H^2(P, \mathbb{Z}/p\mathbb{Z}) = 0$ ist, erhalten wir $H^1(K, \mathbb{Z}/p\mathbb{Z})^P = 0$. Da P eine pro-p-Gruppe ist, folgt hieraus $H^1(K, \mathbb{Z}/p\mathbb{Z}) = 0$, vergl. [27] I Prop. 20, also $K = 1$. q.e.d.

Bemerkung 4.7.: Man überlegt sich leicht, daß P gerade eine "freie Operatoren-p-Gruppe mit n+1 Erzeugenden und dem Operatorenbereich $\mathcal{G}$" ist, wie sie von Koch in [20] definiert wurde.

Wir betrachten nun wieder die absolute Galoisgruppe G_k von k. Seien $y_0, \ldots, y_n \in V_k$ Liftungen der $\mathbb{Z}_p[\![\mathcal{G}]\!]$-Erzeugenden $\bar{y}_0, \ldots, \bar{y}_n$ von V_k^{ab} aus Satz 4.3., dann gibt es nach Satz 4.6. d.) einen Homomorphismus $\varphi: P_{\mathcal{G}} \longrightarrow G_k$ mit $\varphi(x_i) = y_i$ derart, daß

das folgende Diagramm kommutativ ist:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & P & \longrightarrow & P_{\mathcal{G}} & \longrightarrow & \mathcal{G} & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi} & & \| & & \\ 1 & \longrightarrow & V_k & \longrightarrow & G_k & \longrightarrow & \mathcal{G} & \longrightarrow & 1. \end{array}$$

Da die induzierte Abbildung $\bar{\varphi}: P^{ab} \longrightarrow V_k{}^{ab}$ surjektiv ist, ist auch φ surjektiv. Sei $N = \operatorname{Ker} \varphi$, dann ist N offenbar in P enthalten und damit eine pro-p-Gruppe. Wir behaupten nun:

Satz 4.8.: Als Normalteiler in $P_{\mathcal{G}}$ wird N von einem Element erzeugt.

Beweis: Aus der exakten Sequenz

$$1 \longrightarrow N \longrightarrow P \xrightarrow{\varphi} V_k \longrightarrow 1$$

folgt wegen $cd_p(V_k) = 1$ die exakte Sequenz von $\mathcal{G}$-Moduln

$$0 \longrightarrow H^1(V_k, \mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow H^1(P, \mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow H^1(N, \mathbb{Q}_p/\mathbb{Z}_p)^P \longrightarrow 0$$

und dual dazu die exakte Sequenz von $\mathbb{Z}_p[\![\mathcal{G}]\!]$-Moduln

$$0 \longrightarrow N/[N,P] \longrightarrow P^{ab} \xrightarrow{\bar{\varphi}} V_k{}^{ab} \longrightarrow 0.$$

Es gilt $P^{ab} \cong \bigoplus_{i=0}^{n} \mathbb{Z}_p[\![\mathcal{G}]\!]\bar{x}_i$ und $\varphi(\bar{x}_i) = \bar{y}_i$; ein Vergleich mit der exakten Sequenz aus Satz 4.3. ergibt daher

$$N/[N,P] \cong \mathbb{Z}_p[\![\mathcal{G}]\!].$$

Ist $w \in N$ derart gewählt, daß $w[N,P]$ ein $\mathbb{Z}_p[\![\mathcal{G}]\!]$-Erzeugendes von $N/[N,P]$ ist, so erzeugt w N als Normalteiler in $P_{\mathcal{G}}$: Dafür ist nach Lemma 4.5. zu zeigen, daß der $\mathbb{Z}_p[\![G_k]\!]$-Homomorphismus

$$\psi : \mathbb{Z}_p[\![G_k]\!] \longrightarrow N^{ab} \quad \text{mit} \quad \psi(1) = \bar{w} = w[N,N]$$

surjektiv ist, oder, äquivalent dazu, daß die duale Abbildung

$$\Psi^*: \; H^1(N, \mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow \mathrm{Hom}(\mathbb{Z}_p[\![G_k]\!], \mathbb{Q}_p/\mathbb{Z}_p)$$

injektiv ist. Nach Wahl von w ist aber die Restriktion von Ψ^*:

$$\begin{array}{ccc} \Psi^{*V_k}: \; H^1(N, \mathbb{Q}_p/\mathbb{Z}_p)^{V_k} & \longrightarrow & \mathrm{Hom}(\mathbb{Z}_p[\![G_k]\!], \mathbb{Q}_p/\mathbb{Z}_p)^{V_k} \\ \| & & \| \\ \mathrm{Hom}(N/[N,P], \mathbb{Q}_p/\mathbb{Z}_p) & \xrightarrow{\sim} & \mathrm{Hom}(\mathbb{Z}_p[\![\mathcal{G}]\!], \mathbb{Q}_p/\mathbb{Z}_p) \end{array}$$

injektiv, also $(\mathrm{Ker}\,\Psi^*)^{V_k} = 0$. Da $\mathrm{Ker}\,\Psi^*$ ein p-primärer Torsionsmodul und V_k eine pro-p-Gruppe ist, folgt daraus $\mathrm{Ker}\,\Psi^* = 0$, vergl. [27] I Prop. 20. q.e.d.

Bemerkung 4.9.: Mit etwas weitergehenden Betrachtungen kann man sogar zeigen, daß das obige Ψ ein Isomorphismus ist; d.h., es gilt $N^{ab} \cong \mathbb{Z}_p[\![G_k]\!]$.

Da $P_\mathcal{G}$ im wesentlichen, d.h., bis auf die Vorgabe der pro-p-Topologie im Kern P, eine Gruppe mit n+3 Erzeugenden und einer definierenden Relation ist und G_k aus $P_\mathcal{G}$ durch eine zusätzliche Relation hervorgeht, können wir das Ergebnis dieses Paragraphen folgendermaßen aussprechen, vergl. hierzu [20] Satz 1 :

Satz 4.10.: Die absolute Galoisgruppe G_k eines $\mathcal{G}$-adischen Zahlkörpers vom Grad n über $\mathbb{Q}_p$ ist eine pro-endliche Gruppe mit n+3 Erzeugenden und zwei definierenden Relationen. Wählt man die Erzeugenden $y_0, \ldots, y_n$, σ und τ wie oben beschrieben, so erhält man die definierenden Relationen

$$\sigma \tau \sigma^{-1} = \tau^{p^f}$$

$$[y_0, \sigma] y_0^{g-1} \cdot [y_1, \tau] y_1^{h(1+p^s)-1} \cdot r' = 1$$

mit $r' \in [V_k, V_k]$ und den Konstanten g, h und s aus Satz 4.3..

Beweis: Man beachte dazu nur, daß nach Satz 4.8. und Satz 4.3. die unbekannte Relation w die Gestalt

$$w \equiv \sigma y_0 \sigma^{-1} y_0^{-g} \cdot \tau y_1 \tau^{-1} y_0^{-h(1+p^s)} \mod [V_k, V_k]$$

haben muß.

Die Bestimmung des Restterms r' ist ein äußerst schwieriges Problem; eine Lösung dieses Problems mit Methoden ähnlich denen von Koch [20] und Jakovlev [15] scheint mir jedoch nicht unmöglich zu sein. Nach ersten Untersuchungen und aus der Kenntnis der Demuškin-Relation für die maximale p-Erweiterung und der Koch'schen Relation für die maximale Erweiterung ohne zahme Verzweigung, siehe [20], möchte ich vermuten, daß die zweite Relation für gerades n die Form

$$1 = [y_0, \sigma]\, y_0^{g-1} [y_1, \tau]\, y_1^{h(1+p^s)-1} [y_1, y_2][y_3, y_4] \cdots [y_{n-1}, y_n]$$

besitzt. Für $p \neq 2$ und eine primitive p-te Einheitswurzel ζ_p wäre dann z.B. die absolute Galoisgruppe von $Q_p(\zeta_p)$ durch die Relation

$$[y_0, \sigma][y_1, \tau]\, y_1^p [y_1, y_2][y_3, y_4] \cdots [y_{n-1}, y_n] = 1$$

gegeben.

Anhang: Pro-endliche Vervollständigungen.

I. Sei G eine Gruppe, dann wird die totale pro-endliche Vervollständigung $\hat{G}$ von G definiert als der projektive Limes über alle endlichen Faktorgruppen von G:

$$\hat{G} = \varprojlim_{\substack{U \trianglelefteq G \\ (G:U)<\infty}} G/U ,$$

wobei die Homomorphismen des projektiven Systems die kanonischen Projektionen

$$G/V \longrightarrow\!\!\!\!\!\rightarrow G/U \qquad \text{für} \quad V \subseteq U$$

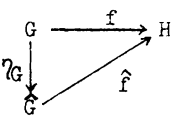
sind. $\hat{G}$ ist gerade die separierte Vervollständigung von G bezüglich der Topologie, die von den Untergruppen von endlichem Index in G erzeugt wird. Dadurch oder auch durch die universelle Eigenschaft des projektiven Limes erhält man eine von den kanonischen Projektionen $G \longrightarrow\!\!\!\!\!\rightarrow G/U$ induzierte Abbildung

$$\eta_G : \; G \longrightarrow \hat{G}.$$

Im η_G ist dicht in $\hat{G}$ und Ker η_G ist gerade der Durchschnitt aller Normalteiler von endlichem Index in G. Die pro-endliche Vervollständigung hat die folgende

Universelle Eigenschaft

Ist H eine pro-endliche Gruppe und $f: G \longrightarrow H$ ein Gruppenhomomorphismus, so gibt es einen eindeutig bestimmten stetigen Homomorphismus $\hat{f}: \hat{G} \longrightarrow H$ derart, daß das Diagramm



kommutiert.

Dies ergibt sich z.B. aus der Definition von $\hat{G}$ als separierte Komplettierung von G.

Ist $f: G \longrightarrow G'$ ein Gruppenhomomorphismus, so erhält man durch die universelle Eigenschaft genau einen stetigen Homomorphismus $\hat{f} = \widehat{\eta_{G'} \circ f} : \hat{G} \longrightarrow \hat{G'}$ derart, daß das Diagramm

$$(*) \qquad \begin{array}{ccc} G & \xrightarrow{f} & G' \\ {\scriptstyle \eta_G}\downarrow & & \downarrow{\scriptstyle \eta_{G'}} \\ \hat{G} & \xrightarrow{\hat{f}} & \hat{G'} \end{array}$$

kommutativ ist. Daraus folgt nun:

1.) Ist $\underline{Gr}$ die Kategorie der Gruppen und $\underline{Pr}$ die Kategorie der pro-endlichen Gruppen (mit den stetigen Gruppenhomomorphismen als Morphismen), so ist die pro-endliche Vervollständigung

$$\begin{array}{rcl} C: & \underline{Gr} & \longrightarrow \underline{Pr} \\ & G & \rightsquigarrow \hat{G} \\ & f & \rightsquigarrow \hat{f} \end{array}$$

ein kovarianter Funktor.

2.) Ist $V: \underline{Pr} \longrightarrow \underline{Gr}$ der Vergißfunktor, so ist C linksadjungiert zu V.

Denn aus $(*)$ folgt gerade, daß

$$\eta : Id_{\underline{Gr}} \longrightarrow V \circ C \qquad \text{mit den Komponenten } \eta_G$$

eine natürliche Transformation ist; und die universelle Eigenschaft besagt, daß $\eta_G: G \longrightarrow C(G)$ universell für den Vergißfunktor ist. Damit folgt die Behauptung aus einem Kriterium für Adjungiertheit, s. etwa S.Mac Lane, Kategorien, Berlin-Heidelberg-New York 1972, p.86 Satz 2.

Corollar C respektiert Colimites, also insbesondere Coprodukte und Epimorphismen.

Beweis: Dies gilt für jeden linksadjungierten Funktor, siehe S. Mac Lane, Kategorien, p.124 Satz 1 und p.126 oben.

Da die Coprodukte sowohl für die diskreten als auch für die pro-endlichen Gruppen gerade die freien Produkte sind, erhalten wir insbesondere:

Corollar: Sind G und H Gruppen, so gibt es eine kanonische Isomorphie

$$\hat{G} * \hat{H} \cong \widehat{G * H}.$$

II. Ist A eine endlich erzeugte, abelsche Gruppe, so gilt offenbar kanonisch

$$\hat{A} = \varprojlim_n A/nA \cong \varprojlim_n (\mathbb{Z}/n\mathbb{Z} \otimes A) \cong (\varprojlim_n \mathbb{Z}/n\mathbb{Z}) \otimes A = \hat{\mathbb{Z}} \otimes A.$$

Ist G eine endliche Gruppe und A ein endlich erzeugter $\mathbb{Z}[G]$-Modul, so kann $\hat{A}$ in genau einer Weise zu einem G-Modul gemacht werden derart, daß die Abbildung

$$\eta_A : A \longrightarrow \hat{A}$$

ein G-Homomorphismus ist und die Operation von G auf $\hat{A}$ stetig ist. Die Isomorphie

$$\hat{A} \cong \hat{\mathbb{Z}} \otimes A$$

ist dann eine G-Isomorphie, und für einen G-Homomorphismus $f: A \longrightarrow B$ zwischen endlich erzeugten $\mathbb{Z}G$-Moduln ist das Diagramm

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow & & \downarrow \\ \mathbb{Z} \otimes A & \xrightarrow{1 \otimes f} & \mathbb{Z} \otimes B \end{array}$$

kommutativ.

III. Ist $1 \longrightarrow R \longrightarrow F \longrightarrow G \longrightarrow 1$ eine exakte Sequenz von Gruppen mit endlicher Gruppe G, so ist die Sequenz $1 \longrightarrow \hat{R} \longrightarrow \hat{F} \longrightarrow G \longrightarrow 1$ der Vervollständigungen exakt, und man erhält das kommutative Diagramm

$$\begin{array}{ccccccccc} 1 & \longrightarrow & R & \longrightarrow & F & \longrightarrow & G & \longrightarrow & 1 \\ & & \eta_R \downarrow & & \eta_F \downarrow & & \| & & \\ 1 & \longrightarrow & \hat{R} & \longrightarrow & \hat{F} & \longrightarrow & G & \longrightarrow & 1. \end{array}$$

Die induzierte Abbildung

$$\bar{\eta}_R : \; R^{ab} \longrightarrow \hat{R}^{ab}$$

ist ein G-Homomorphismus, und die Operation von G auf $\hat{R}^{ab}$ ist stetig. Da sich weiter offenbar $\hat{R}^{ab}$ mit $\widehat{R^{ab}}$ identifizieren läßt, und $\bar{\eta}_R$ mit $\eta_{R^{ab}}$, erhalten wir mit den Überlegungen unter Punkt II die $\hat{\mathbb{Z}}[G]$-Isomorphie

$$\hat{R}^{ab} \;\cong\; \hat{\mathbb{Z}} \otimes R^{ab}.$$

Literaturverzeichnis

[1] E. Artin, J. Tate: Class field theory. Harvard (1961).

[2] Z. I. Borevič: On the multiplicative group of cyclic p-extensions of a local field. Proc. Mat. Inst. Steklov 80 (1965), 15-30.

[3] Z. I. Borevič: On the group of principal units of a normal p-extension of a regular local field. ibid. 31-47.

[4] Z. I. Borevič, A. I. Skopin: Extensions of a local field with normal basis for principal units. ibid. 48-55.

[5] Z. I. Borevič, A. J. El Musa: Completion of the multiplicative group of p-extensions of an irregular local field. J. Soviet Math. 6 (1976), 211-226.

[6] A. Brumer: Pseudocompact algebras, profinite groups and class formations. J. Algebra 4 (1966), 442-470.

[7] H. Cartan, S. Eilenberg: Homological Algebra. Princeton (1956).

[8] E. L. Gerlovin: Completion of the multiplicative group of a cyclic p-extension of a local field. Vestnik Leningrad Univ. Math. 2 (1975), 91-101.

[9] D. Gilbarg: The structure of the group of $\mathfrak{p}$-adic 1-units. Duke Math. J. 9 (1942), 262-271.

[10] K. W. Gruenberg: Cohomological topics in group theory. Lecture Notes in Math. 143, Springer (1970).

[11] K. W. Gruenberg: Relation modules of finite groups. Conference board of the math. sciences 25, AMS (1976).

[12] H. Hasse: Zahlentheorie. Akademie Verlag Berlin (1963).

[13] G. Hochschild, J. P. Serre: Cohomology of group extensions. Trans. Amer. Math. Soc. 74 (1953), 110-134.

[14] K. Iwasawa: On galois groups of local fields. Trans. Amer. Math. Soc. 74 (1955), 448-469.

[15] A. V. Jakovlev: The galois group of the algebraic closure of a local field. Math. USSR-Izv. 2 (1968), 1231-1269.

[16] A. V. Jakovlev: Remarks on my paper "The galois group of the algebraic closure of a local field". Math. USSR-Izv. 12 (1978), 205-206.

[17] U. Jannsen, K. Wingberg: Die p-Vervollständigung der multiplikativen Gruppe einer p-Erweiterung eines irregulären $\mathfrak{p}$-adischen Zahlkörpers. J. Reine Angew. Math. 307/308 (1979), 399-410.

[18] U. Jannsen, K. Wingberg: Einbettungsprobleme und Galoisstruktur lokaler Körper. ersch. demn. im J. Reine Angew. Math.

[19] Y. Kawada: Cohomology of group extensions. J. Fac. Sci. Univ. Tokyo 9 (1963), 417-431.

[20] H. Koch: Über Galoissche Gruppen von $\mathfrak{p}$-adischen Zahlkörpern. Math. Nachr. 29 (1965), 77-111.

[21] M. Krasner: Sur la représentation exponentielle dans les corps relativement galoisiens de nombres P-adiques. Acta Arith. 3 (1939), 133-173.

[22] R. C. Lyndon: Cohomology theory of groups with a single defining relation. Ann. of Math. 52 (1950), 650-665.

[23] T. Nakayama: On modules of trivial cohomology over a finite group. Illinois J. Math. 1 (1957), 36-43.

[24] J. Neukirch: Freie Produkte pro-endlicher Gruppen und ihre Kohomologie. Arch. d. Math. (Basel) 12 (1971), 337-357.

[25] H. Pieper: Die Einheitengruppe eines zahm-verzweigten galoisschen lokalen Körpers als Galois-Modul. Math. Nachr. 54 (1972), 173-210.

[26] J. P. Serre: Corps locaux. Hermann Paris (1962).

[27] J. P. Serre: Cohomologie Galoisienne. Lecture Notes in Math. 5, Springer (1973).

[28] S. S. Shatz: Profinite groups, arithmetic, and geometry. Ann. of Math. Studies 67, Princeton university press (1972).

[29] R. G. Swan: Induced representations and projective modules. Ann. of Math. 71 (1960), 552-578.

[30] K. Wingberg: Die Einseinheitengruppe von p-Erweiterungen regulärer $\mathfrak{p}$-adischer Zahlkörper als Galoismodul. J. Reine Angew. Math. 305 (1979), 206-214.

[31] V. D. Lesev: On the p-adic supplement of a multiplicative group of a normal extension of a regular local field a cyclic branching subfield. Algebra and Number Theory, Nal'čik, Subj. Collect. 1 (1973), 27-31.

Lebenslauf

Ich wurde am 11. 3. 1954 als Sohn des Zimmermeisters Gustav Jannsen und seiner Frau Hildgund, geb. Böhmke, in Meddewade (Schleswig-Holstein) geboren.

Von 1960 bis 1964 besuchte ich die Grundschule, danach das Gymnasium in Bad Oldsloe bis zum Abitur im Sommer 1972.

Zurückgestellt vom Grundwehrdienst, begann ich im Wintersemester 1972/73 das Studium der Mathematik und Physik in Hamburg und legte im Frühjahr 1975 das Vordiplom in beiden Fächern ab. Ab dem 8. Semester konzentrierte ich mich zunehmend auf die Mathematik. Ich nahm an Vorlesungen und Seminaren u. a. bei Prof. Brückner, Prof. Legrady und Prof. Witt teil und legte 1978 das Hauptdiplom in Reiner Mathematik ab. Meine Diplomarbeit schrieb ich bei Herrn Prof. Brückner auf dem Gebiet der Algebraischen Zahlentheorie.

Nach mehreren Lehraufträgen erhielt ich in diesem Jahr in Vertretung einer Assistentenstelle eine Stelle als Wissenschaftliche Hilfskraft.