Invent. math. 70, 53-69 (1982)

Inventiones mathematicae

Über Galoisgruppen lokaler Körper

Uwe Jannsen

Fakultät für Mathematik, Universität Regensburg, Universitätsstr. 31, 8400 Regensburg, Bundesrepublik Deutschland

Der erste Schritt bei der Untersuchung der absoluten Galoisgruppe $G_k = G(\bar{k}/k)$ eines lokalen Körpers k besteht nach einer Idee von Iwasawa [7] darin, die Operation der Galoisgruppe $\mathcal{G} = G(T/k)$ der maximalen zahm-verzweigten Erweiterung T von k auf der Faktorkommutatorgruppe V_k^{ab} der Verzweigungsgruppe $V_k = G(\bar{k}/T)$ zu betrachten. Nach der Klassenkörpertheorie ist V_k^{ab} $\mathcal{G}$-isomorph zum projektiven Limes der Einseinheitengruppen U_K^1 der endlichen zahm-verzweigten galoisschen Erweiterungen K/k, und Iwasawa beschrieb diese als Moduln über dem Gruppenring $\mathbb{Z}_p[G(K/k)]$.

In der vorliegenden Arbeit soll gezeigt werden, daß sich hier durch das Studium kohomologisch trivialer $\mathbb{Z}_p[G]$-Moduln einige neue Resultate erhalten lassen. Grundlegend ist dafür der Satz, daß ein derartiger Modul M bereits durch seinen Torsionsmodul $\mathrm{Tor}(M)$ und den Modul $\mathbb{Q}_p \otimes M$ vollständig bestimmt wird. Für den Fall der Isomorphie $\mathbb{Q}_p \otimes M \cong \mathbb{Q}_p[G]^m$ wird weiter ein konstruktives Verfahren entwickelt, um die Struktur von M aus der von $\mathrm{Tor}(M)$ zu gewinnen.

Für eine zahm-verzweigte Erweiterung K/k p-adischer Zahlkörper liefert dies Verfahren aufgrund der wohlbekannten Isomorphie $\mathbb{Q}_p \otimes U_K^1 \cong \mathbb{Q}_p[G]^n$ mit $n = [k:\mathbb{Q}_p]$ und $G = G(K/k)$ eine exakte Sequenz

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

insbesondere erhält man eine Beschreibung von U_K^1 durch eine einzige Relation statt durch zwei wie bei Iwasawa.

Dies hat eine wichtige Konsequenz für die Darstellung der Galoisgruppe G_k durch Erzeugende und Relationen. Aus der exakten Sequenz

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

folgt, daß zur Beschreibung von G_k neben der Hasse-Iwasawa-Relation, die von $\mathcal{G}$ stammt, nur noch eine weitere Relation nötig ist. (Die bisherigen Untersuchungen von Koch [10] und Jakovlev [8] gehen aufgrund der Iwasawaschen Ergebnisse immer von zwei weiteren Relationen aus.) Genauer wird

0020-9910/82/0070/0053/$03.40

folgendes gezeigt: Bildet man die Gruppe $F(n+1, \mathcal{G})$, indem man im freien pro-endlichen Produkt von $\mathcal{G}$ mit einer freien pro-endlichen Gruppe F_{n+1} mit $n+1$ Erzeugenden $z_0, \ldots, z_n$ den von den z_i erzeugten Normalteiler zur pro-p-Gruppe macht, so gibt es eine Surjektion

$$F(n+1, \mathcal{G}) \twoheadrightarrow G_k,$$

deren Kern als Normalteiler von einem Element r erzeugt wird. In [9] wird dieses r für $p \neq 2$ angegeben, das obige Resultat gilt jedoch auch für $p=2$.

Die entsprechenden Ergebnisse für einen Potenzreihenkörper k, die auf Koch [11] zurückgehen, lassen sich zitieren in der Form

$$V_k^{\mathrm{ab}} \cong \mathbb{Z}_p[\![\mathcal{G}]\!]^{\mathbb{N}} \qquad G_k \cong F(\mathbb{N}, \mathcal{G}).$$

Die Verwendung der Gruppen $F(J, \mathcal{G})$ erspart dabei die etwas komplizierte Konstruktion einer freien Operatoren-pro-p-Gruppe.

Da es keine zusätzlichen Schwierigkeiten bereitet, werden allgemeiner die Galoisgruppen p-abgeschlossener Erweiterungen betrachtet.

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

Sei G in diesem Paragraphen eine beliebige endliche Gruppe. Sei p eine Primzahl, $\mathbb{Q}_p$ der Körper der p-adischen Zahlen und $\mathbb{Z}_p$ der Ring der ganzen p-adischen Zahlen. Die Moduln $\mathbb{Q}_p$, $\mathbb{Z}_p$ und $\mathbb{Q}_p/\mathbb{Z}_p$ werden immer mit der trivialen G-Operation versehen. Für einen kommutativen Ring R bezeichne $R[G]$ den Gruppenring mit Koeffizienten in R. Für $\mathbb{Z}_p[G]$-Moduln A und B werden $\mathrm{Hom}(A,B) := \mathrm{Hom}_{\mathbb{Z}_p}(A,B)$ und $A \otimes B := A \otimes_{\mathbb{Z}_p} B$ zu $\mathbb{Z}_p[G]$-Moduln durch die Definitionen $(sf)(a) := sf(s^{-1}a)$ und $s(a \otimes b) := sa \otimes sb$ für $s \in G$. Insbesondere sei $A^+ = \mathrm{Hom}(A, \mathbb{Z}_p)$ das $\mathbb{Z}_p$-Dual und $A^* = \mathrm{Hom}(A, \mathbb{Q}_p/\mathbb{Z}_p)$ das Pontrjagindual eines $\mathbb{Z}_p[G]$-Moduls A. (Bei der Bildung von A^* wird A immer endlich erzeugt oder diskret, also auch lokalkompakt sein.) Schließlich sei $\mathrm{Tor}(A)$ der Torsionsmodul von A.

Die folgenden Eigenschaften projektiver $\mathbb{Z}_p[G]$-Moduln sind wohlbekannt.

Lemma 1.1. *Seien P und P' projektive, endlich erzeugte $\mathbb{Z}_p[G]$-Moduln, dann gilt*

a) *$P \cong P'$ genau dann, wenn P/pP'* (s. etwa [5] 3.17).

b) *$P \cong P'$ genau dann, wenn $\mathbb{Q}_p \otimes P \cong \mathbb{Q}_p \otimes P'$.* (Dies ist ein Ergebnis von Swan [16], Cor. 6.4, und wird im folgenden als Lemma von Swan zitiert.)

Dies soll nun auf kohomologisch triviale Moduln verallgemeinert werden. Man beachte hierzu, daß ein endlich erzeugter $\mathbb{Z}_p[G]$-Modul genau dann projektiv ist, wenn er kohomologisch trivial und torsionsfrei ist ([14], IX, § 5, Th. 7 mit $\mathbb{Z}_p$ statt $\mathbb{Z}$).

Satz 1.2. *Seien M und M' endlich erzeugte, kohomologisch triviale $\mathbb{Z}_p[G]$-Moduln, dann sind die folgenden Aussagen äquivalent:*

a) *$M \cong M'$.*

b) *$\mathrm{Tor}(M) \cong \mathrm{Tor}(M')$ und $\mathbb{Q}_p \otimes M \cong \mathbb{Q}_p \otimes M'$.*

c) $\mathrm{Tor}(M)\cong\mathrm{Tor}(M')$ *und* $M/pM\cong M'/pM'$.

d) *Für ein* s *mit* $p^s\mathrm{Tor}(M)=p^s\mathrm{Tor}(M')=0$ *gilt* $M/p^{s+1}M\cong M'/p^{s+1}M'$.

Beweis. Wegen der kohomologischen Trivialität von M und M' gibt es exakte Sequenzen

$$\begin{aligned} &0\to P\to Q\to M\to 0\\ &0\to P'\to Q'\to M'\to 0 \end{aligned}\qquad (+)$$

mit endlich erzeugten, projektiven $\mathbb{Z}_p[G]$-Moduln P, Q, P' und Q' ([14], IX, § 5, Th. 8 für $\mathbb{Z}_p[G]$-Moduln).

Tensorieren wir diese Sequenzen mit $\mathbb{Q}_p$, so zerfallen sie nach dem Satz von Maschke. Dies ergibt die Isomorphien $\mathbb{Q}_p\otimes Q\cong\mathbb{Q}_p\otimes P\oplus\mathbb{Q}_p\otimes M$ und $\mathbb{Q}_p\otimes Q'\cong\mathbb{Q}_p\otimes P'\oplus\mathbb{Q}_p\otimes M'$, insbesondere also

$$\mathbb{Q}_p\otimes(P\oplus Q')\oplus\mathbb{Q}_p\otimes M\cong\mathbb{Q}_p\otimes(P'\oplus Q)\oplus\mathbb{Q}_p\otimes M'. \qquad (++)$$

Setzen wir weiter für einen $\mathbb{Z}_p[G]$-Modul A und $n\in\mathbb{N}$

$$\begin{aligned} A_n&=A/nA,\\ {}_nA&=\{a\in A;\ na=0\}, \end{aligned}$$

so erhalten wir mit dem Schlangenlemma aus $(+)$ die exakten Sequenzen

$$\begin{aligned} &0\to{}_n\mathrm{Tor}(M)\to P_n\to Q_n\to M_n\to 0\\ &0\to{}_n\mathrm{Tor}(M')\to P'_n\to Q'_n\to M'_n\to 0. \end{aligned}\qquad (+++)$$

Wir kommen nun zum eigentlichen Beweis des Satzes.

a)$\Rightarrow$d) ist trivial.

d)$\Rightarrow$c). Offenbar gilt ${}_p(M/p^{s+1}M)=({}_p\mathrm{Tor}(M)+p^sM)/p^{s+1}M$ und also ${}_p(M/p^{s+1}M)/p^s(M/p^{s+1}M)\cong{}_p\mathrm{Tor}(M)$ wegen $\mathrm{Tor}(M)\cap p^sM=0$. Aus d) folgt daher ${}_p\mathrm{Tor}(M)\cong{}_p\mathrm{Tor}(M')$. Andererseits folgt aus d) auch $M_p\cong M'_p$, mit $(+++)$ und dem Lemma von Schanuel (s. [16]; zweimalige Anwendung, vgl. [4], S. 163) also

$${}_p\mathrm{Tor}(M)\oplus P'_p\oplus Q_p\cong{}_p\mathrm{Tor}(M')\oplus P_p\oplus Q'_p.$$

Zusammen ergibt dies wegen der Gültigkeit des Krull-Schmidt-Theorems die Isomorphie $(P'\oplus Q)_p\cong(P\oplus Q')_p$ und folglich

$$P'\oplus Q\cong P\oplus Q'.$$

Setzen wir dies wiederum in die Isomorphie

$$\mathrm{Tor}(M)\oplus P'_{p^s}\oplus Q_{p^s}\cong\mathrm{Tor}(M')\oplus P_{p^s}\oplus Q_{p^s}$$

ein, die wir aus d) und $(+++)$ für $n=p^s$ erhalten, so folgt schließlich $\mathrm{Tor}(M)\cong\mathrm{Tor}(M')$ und damit c).

c)$\Rightarrow$b). Wie oben folgt aus c) die Isomorphie $P'\oplus Q\cong P\oplus Q'$, mit $(++)$ also $\mathbb{Q}_p\otimes M\cong\mathbb{Q}_p\otimes M'$.

b)⇒a). Aus b) und (++) folgt zunächst $\mathbb{Q}_p \otimes (P' \oplus Q) \cong \mathbb{Q}_p \otimes (P \oplus Q')$, mit dem Lemma von Swan also $P' \oplus Q \cong P \oplus Q'$. Andererseits folgt aus der Isomorphie $\mathrm{Tor}(M) \cong \mathrm{Tor}(M')$ und den zu (+++) dualen Sequenzen mit dem Lemma von Schanuel für jedes $n \in \mathbb{N}$ die Isomorphie

$$M_n^* \oplus Q_n'^* \oplus P_n^* = M_n'^* \oplus Q_n^* \oplus P_n'^*.$$

Zusammen ergibt sich die Isomorphie $M_n^* = M_n'^*$ für jedes $n \in \mathbb{N}$, insbesondere gilt

$$M/p^r M \cong M'/p^r M'$$

für alle $r \in \mathbb{N}$. Hieraus folgt die Isomorphie $M \cong M'$ durch Bildung des projektiven Limes; z.B. mit dem wohlbekannten Satz, daß der projektive Limes nichtleerer endlicher Mengen nicht leer ist, angewandt auf die Mengen $Iso(M/p^r M, M'/p^r M')$ der Isomorphismen von $M/p^r M$ auf $M'/p^r M'$. q.e.d.

Es wird im folgenden nur das Kriterium b) aus Satz 1.2 benötigt. Insbesondere werden uns Moduln des folgenden Typs interessieren.

Definition 1.3. Ein endlich erzeugter $\mathbb{Z}_p[G]$-Modul M heißt quasifrei (vom Rang m), wenn er kohomologisch trivial und $\mathbb{Q}_p \otimes M$ ein freier $\mathbb{Q}_p[G]$-Modul ($\mathbb{Q}_p \otimes M \cong \mathbb{Q}_p[G]^m$) ist.

Satz 1.4. *Für einen endlich erzeugten $\mathbb{Z}_p[G]$-Modul M sind die folgenden Aussagen äquivalent:*

a) *M ist quasifrei vom Rang m.*

b) *M ist kohomologisch trivial und enthält einen Untermodul $N \cong \mathbb{Z}_p[G]^m$ von endlichem Index in M.*

c) *Es gibt eine exakte Sequenz $0 \to \mathbb{Z}_p[G]^k \to \mathbb{Z}_p[G]^l \to M \to 0$ mit $l-k=m$.*

Beweis. a)⇔b). Für endlich erzeugte $\mathbb{Z}_p[G]$-Moduln M und N gilt die Isomorphie $\mathbb{Q}_p \otimes N \cong \mathbb{Q}_p \otimes M$ genau dann, wenn es einen $\mathbb{Z}_p[G]$-Homomorphismus f: $N \to M$ mit endlichem Kern und Cokern gibt.

a)⇒c). Ist für geeignetes $l \in \mathbb{N}$ f: $\mathbb{Z}_p[G]^l \twoheadrightarrow M$ eine Surjektion, so ist $P = \mathrm{Ker}\, f$ wegen der kohomologischen Trivialität von M ebenfalls kohomologisch trivial, also projektiv wegen $\mathrm{Tor}(P)=0$. Durch Tensorieren mit $\mathbb{Q}_p$ folgt $\mathbb{Q}_p \otimes P = \mathbb{Q}_p[G]^{l-m}$, mit dem Lemma von Swan also $P \cong \mathbb{Z}_p[G]^{l-m}$. c)⇒a) ist klar.

Corollar 1.5. *Ist G eine p-Gruppe, so ist jeder endlich erzeugte kohomologisch triviale $\mathbb{Z}_p[G]$-Modul quasifrei.*

Beweis. Es gibt eine exakte Sequenz $0 \to P_1 \to P_2 \to M \to 0$ mit projektiven Moduln P_1 und P_2. Da für eine p-Gruppe G der Gruppenring $\mathbb{Z}_p[G]$ ein lokaler Ring ist (vgl. [4], §10.5, Prop. 10), sind P_1 und P_2 freie $\mathbb{Z}_p[G]$-Moduln (s. etwa [5], Prop. 3.16).

Aus Satz 1.2 folgt, daß quasifreie Moduln M allein durch ihren Rang m (nicht zu verwechseln mit dem $\mathbb{Z}_p$-Rang von M) und ihren Torsionsmodul $\mathrm{Tor}(M)$ bestimmt sind. Die Beziehungen zwischen M, m und $\mathrm{Tor}(M)$ sollen nun weiter untersucht werden.

Definition 1.6. Für einen endlich erzeugten $\mathbb{Z}_p[G]$-Modul N sei der Erzeugendenrang $d=d_G(N)$ als die minimale Anzahl von $\mathbb{Z}_p[G]$-Erzeugenden von N und der Relationenrang $r=r_G(N)$ als der Erzeugendenrang von $\operatorname{Ker} f$ für eine Surjektion $f\colon \mathbb{Z}_p[G]^d \twoheadrightarrow N$ definiert.

Bemerkung 1.7. a) Ist $g\colon \mathbb{Z}_p[G]^n \twoheadrightarrow N$ eine weitere Surjektion, $n \geqq d$, so folgt mit dem Lemma von Schanuel

$$\operatorname{Ker} f \oplus \mathbb{Z}_p[G]^n \cong \operatorname{Ker} g \oplus \mathbb{Z}_p[G]^d$$

und daher $r=r_G(N)=d_G(\operatorname{Ker} f)=d_G(\operatorname{Ker} g)+d-n$ (vgl. [5], Lemma 5.8), da $\mathbb{Z}_p[G]$ ein semi-lokaler Ring ist. Dies zeigt die Wohldefiniertheit des Relationenranges.

b) Ist N endlich, so gilt $r \geqq d$, wie aus der exakten Sequenz

$$\mathbb{Z}_p[G]^r \xrightarrow{\varphi} \mathbb{Z}_p[G]^d \to N \to 0$$

z.B. durch Tensorieren mit $\mathbb{Q}_p$ folgt. Weiter gilt $r=d$ genau dann, wenn N kohomologisch trivial ist, denn für $r=d$ ist φ notwendig injektiv, und umgekehrt ist für kohomologisch triviales N in einer exakten Sequenz

$$0 \to K \to \mathbb{Z}_p[G]^d \to N \to 0$$

K projektiv, aus der Isomorphie $\mathbb{Q}_p \otimes K \cong \mathbb{Q}_p[G]^d$ folgt daher $K \cong \mathbb{Z}_p[G]^d$.

Satz 1.8. *Ist M quasifrei und $(+)$ $0 \to \mathbb{Z}_p[G]^k \to \mathbb{Z}_p[G]^l \xrightarrow{\pi} M \to 0$ exakt, so gelten mit $d=d_G(\operatorname{Tor}(M)^*)$ und $r=r_G(\operatorname{Tor}(M)^*)$ die Ungleichungen $k \geqq d$, $l \geqq r$ und $l-k \geqq r-d$.*

Beweis. Aus $(+)$ folgt die exakte Sequenz

$$\begin{aligned} 0 \to \operatorname{Hom}(M, \mathbb{Z}_p) &\to \operatorname{Hom}(\mathbb{Z}_p[G]^l, \mathbb{Z}_p) \\ &\to \operatorname{Hom}(\mathbb{Z}_p[G]^k, \mathbb{Z}_p) \xrightarrow{\delta} \operatorname{Tor}(M))^* \to 0 \end{aligned}$$

wegen der kanonischen Isomorphie $\operatorname{Ext}^1_{\mathbb{Z}_p}(M, \mathbb{Z}_p) \cong \operatorname{Tor}_1^{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p)^* = \operatorname{Tor}(M)^*$ ([2], VI, Prop. 5.4 u. (4')) und $\operatorname{Ext}^1_{\mathbb{Z}_p}(\mathbb{Z}_p[G]^l, \mathbb{Z}_p)=0$. Explizit definiere etwa $\delta(f) \in \operatorname{Tor}(M)^*$ durch $\delta(f)(x)=f(p^m y)\, p^{-m}+\mathbb{Z}_p \in \mathbb{Q}_p/\mathbb{Z}_p$ für $x \in \operatorname{Tor}(M)$ mit $p^m x=0$, $\pi(y)=x$. Da $\operatorname{Hom}(\mathbb{Z}_p[G]^n, \mathbb{Z}_p)$ wieder ein freier $\mathbb{Z}_p[G]$-Modul vom Rang n ist, erhalten wir eine exakte Sequenz

$$\mathbb{Z}_p[G]^l \to \mathbb{Z}_p[G]^k \xrightarrow{\delta} \operatorname{Tor}(M)^* \to 0.$$

Daraus folgt sofort $k \geqq d$, sowie $l \geqq d_G(\operatorname{Ker} \delta)=r+k-d$ (vgl. Bem. 1.7a)). Aus beiden Ungleichungen folgt schließlich auch $l \geqq r$.

Aus dem obigen Satz folgt insbesondere, daß für einen endlichen $\mathbb{Z}_p[G]$-Modul N die Ränge der quasifreien Moduln M mit $\operatorname{Tor}(M) \cong N$ durch die Zahl $r_G(N^*)-d_G(N^*)$ nach unten beschränkt sind. Der folgende Satz zeigt, daß es auch immer einen quasifreien Modul mit diesem minimalen Rang gibt und wie allgemein quasifreie Moduln aus ihren Torsionsmoduln konstruiert werden können. Insbesondere gibt es zu jedem endlichen $\mathbb{Z}_p[G]$-Modul N einen kohomologisch trivialen Modul M (sogar einen quasifreien) mit $\operatorname{Tor}(M) \cong N$.

Satz 1.9. *Sei N ein endlicher $\mathbb{Z}_p[G]$-Modul und*

$$P \xrightarrow{f} Q \to N^* \to 0$$

exakt mit $P=\mathbb{Z}_p[G]^l$ und $Q=\mathbb{Z}_p[G]^k$. Dann ist die von f induzierte Abbildung $f^+\colon Q^+ \to P^+$ injektiv und $M=\mathrm{Coker} f^+$ ist der quasifreie $\mathbb{Z}_p[G]$-Modul vom Rang $l-k$ mit Torsionsmodul N.

Beweis. Die Injektivität von f^+ folgt wegen $\mathrm{Hom}(N^*, \mathbb{Z}_p)=0$ aus der Linksexaktheit des Hom-Funktors. $M=\mathrm{Coker} f^+$ ist quasifrei vom Rang $l-k$, da P^+ bzw. Q^+ freie $\mathbb{Z}_p[G]$-Moduln vom Rang l bzw. k sind. Durch erneute Anwendung des Hom-Funktors erhalten wir die exakte Sequenz

$$0 \to M^+ \to P^{++} \xrightarrow{f^{++}} Q^{++} \to \mathrm{Tor}(M)^* \to 0,$$

wieder wegen $\mathrm{Ext}^1_{\mathbb{Z}_p}(M, \mathbb{Z}_p) \cong \mathrm{Tor}(M)^*$, und in dem kommutativen Diagramm

$$\begin{array}{ccc} P & \xrightarrow{f} & Q \\ {\scriptstyle \varphi_P}\downarrow & & \downarrow{\scriptstyle \varphi_Q} \\ P^{++} & \xrightarrow{f^{++}} & Q^{++}, \end{array}$$

sind die kanonischen Abbildungen φ_P und φ_Q wegen der Torsionsfreiheit von P und Q Isomorphismen. Daraus folgt $N^*=\mathrm{Coker} f \cong \mathrm{Coker} f^{++} \cong \mathrm{Tor}(M)^*$, also $N \cong \mathrm{Tor}(M)$. q.e.d.

Corollar 1.10. *Sei N ein endlicher $\mathbb{Z}_p[G]$-Modul, $d=d_G(N^*)$ und $r=r_G(N^*)$, dann existiert ein quasifreier Modul $M_0(N)$ mit Torsionsmodul N vom minimalen Rang $r-d$; für ihn gibt es eine exakte Sequenz*

$$0 \to \mathbb{Z}_p[G]^d \to \mathbb{Z}_p[G]^r \to M_0(N) \to 0.$$

Ist M quasifrei vom Rang $m=r-d+j$, $j \geqq 0$, mit $\mathrm{Tor}(M) \cong N$, so gilt die Isomorphie $M \cong M_0(N) \oplus \mathbb{Z}_p[G]^j$ und es gibt eine exakte Sequenz

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

Beweis. Die Konstruktion von 1.9 liefert aus einer exakten Sequenz

$$\mathbb{Z}_p[G]^l \xrightarrow{f} \mathbb{Z}_p[G]^k \to N^* \to 0$$

eine exakte Sequenz

$$0 \to \mathbb{Z}_p[G]^k \xrightarrow{f^+} \mathbb{Z}_p[G]^l \to M \to 0$$

mit $\mathrm{Tor}(M) \cong N$. Für $k=d$ und $l=r$ ergibt sich die erste Aussage. Die Isomorphie $M=M_0(N) \oplus \mathbb{Z}_p[G]^j$ folgt aus Satz 1.2, und aus der Sequenz für $M_0(N)$ erhält man trivialerweise eine exakte Sequenz

$$0 \to \mathbb{Z}_p[G]^d \to \mathbb{Z}_p[G]^{r+j} \to M_0(N) \oplus \mathbb{Z}_p[G]^j \to 0,$$

in der $r+j=m+d$ gilt.

Die obigen Betrachtungen führen zu einer allgemeinen Strukturaussage für kohomologisch triviale $\mathbb{Z}_p[G]$-Moduln. Jeder endlich erzeugte $\mathbb{Z}_p[G]$-Modul M läßt sich aufspalten in $M=\tilde{M}\oplus P$, wobei P projektiv ist und $\tilde{M}$ keine projektiven Summanden mehr besitzt. Der Modul $\tilde{M}$ ist bis auf Isomorphie eindeutig bestimmt (vgl. hierzu [16], Paragraph 6).

Satz 1.11. *Sei M ein endlich erzeugter, kohomologisch trivialer $\mathbb{Z}_p[G]$-Modul und $N=\mathrm{Tor}(M)$, dann gilt $\tilde{M}\cong\widetilde{M_0(N)}$. Anders ausgedrückt: Alle endlich erzeugten, kohomologisch trivialen $\mathbb{Z}_p[G]$-Moduln M mit $\mathrm{Tor}(M)\cong N$ haben die Gestalt $M\cong\widetilde{M_0(N)}\oplus P$ mit projektivem P.*

Beweis. Sei $0\to Q\to\mathbb{Z}_p[G]^k\to M\to 0$ exakt mit projektivem Q, dann ist offenbar $M\oplus Q$ quasifrei mit $\mathrm{Tor}(M\oplus Q)=\mathrm{Tor}(M)=N$, also isomorph zu $M_0(N)\oplus\mathbb{Z}_p[G]^j$ für ein geeignetes $j\geqq 0$. Aus der Zerlegung

$$\tilde{M}\oplus P\oplus Q=\widetilde{M_0(N)}\oplus P'\oplus\mathbb{Z}_p[G]^j$$

folgt wegen der Eindeutigkeit $\tilde{M}=\widetilde{M_0(N)}$. q.e.d.

Bemerkung 1.12. a) Ist G eine p-Gruppe, so gilt $\widetilde{M_0(N)}=M_0(N)$, denn in einer Zerlegung $M_0(N)=\widetilde{M_0(N)}\oplus P$ ist P frei; aus der Minimalität von $M_0(N)$ folgt $P=0$.

b) Ist N unzerlegbar, so auch $\widetilde{M_0(N)}$, denn in einer Zerlegung $\widetilde{M_0(N)}=A\oplus B$ wäre einer der Faktoren torsionsfrei, also projektiv wegen der kohomologischen Trivialität von $\widetilde{M_0(N)}$.

c) Ist $N=\oplus N_i$ mit unzerlegbaren N_i, so ist $\widetilde{M_0(N)}\cong\oplus\widetilde{M_0(N_i)}$, denn $\oplus\widetilde{M_0(N_i)}$ ist kohomologisch trivial mit Torsionsmodul N und besitzt keinen projektiven Summanden, da die $\widetilde{M_0(N_i)}$ unzerlegbar und nicht projektiv sind. Dadurch ist aber gerade $\widetilde{M_0(N)}$ charakterisiert.

§ 2. Zahm-verzweigte Erweiterungen lokaler Körper

Ist k ein lokaler Körper, dessen Restklassenkörper die Charakteristik p hat, so ist die Gruppe U_k^1 der Einseinheiten von k als abelsche pro-p-Gruppe ein $\mathbb{Z}_p$-Modul. Für eine endliche galoissche Erweiterung K/k wird U_k^1 durch die stetige Operation der Automorphismen der Galoisgruppe G zu einem $\mathbb{Z}_p[G]$-Modul. In diesem Paragraphen werden nur p-adische Zahlkörper behandelt; die Potenzreihenkörper werden am Ende von § 3 betrachtet.

Satz 2.1. *Sei $\mathrm{Char}(k)=0$, also k eine endliche Erweiterung des Körpers $\mathbb{Q}_p$ der p-adischen Zahlen. Ist K/k eine endliche, zahm-verzweigte, galoissche Erweiterung mit Galoisgruppe G sowie μ_K die Gruppe der in K enthaltenen Einheitswurzeln von p-Potenz-Ordnung, dann gilt mit $n=[k:\mathbb{Q}_p]$*

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

c) *Ist K regulär, d.h., enthält K keine primitive p-te Einheitswurzel, so gilt* $U_K^1 \cong \mathbb{Z}_p[G]^n$.

Beweis. a) Für jede galoissche Erweiterung K/k mit Galoisgruppe G enthält U_K^1 einen freien $\mathbb{Z}_p[G]$-Modul vom Rang n und endlichem Index in U_K^1, d.h., es gilt $\mathbb{Q}_p \otimes U_K^1 \cong \mathbb{Q}_p[G]^n$. Dies ist wohlbekannt und folgt mit Hilfe der p-adischen Exponentialfunktion aus der Existenz einer Normalbasis (vgl. Gilbarg [3]). Für eine zahm-verzweigte Erweiterung ist zusätzlich U_K^1 kohomologisch trivial; dies folgt z.B. aus der kohomologischen Trivialität von U_K^1 unter einer p-Sylowgruppe G_p, die einer unverzweigten Erweiterung entspricht (vgl. hierzu [14], XII, § 3). Schließlich gilt gerade $\mathrm{Tor}(U_K^1) = \mu_K$.

b) Folgt aus 1.10 wegen $d_G(\mu_K^*) = 1$.

c) Ist K regulär, so ist U_K^1 torsionsfrei, wegen der kohomologischen Trivialität also projektiv. Aus der Isomorphie $\mathbb{Q}_p \otimes U_K^1 \cong \mathbb{Q}_p \otimes \mathbb{Z}_p[G]^n$ folgt dann mit dem Lemma von Swan sofort $U_K^1 \cong \mathbb{Z}_p[G]^n$. q.e.d.

Mit Hilfe von Satz 1.9 soll nun die Sequenz aus 2.1b) explizit angegeben und damit U_K^1 durch $\mathbb{Z}_p[G]$-Erzeugende und -Relationen beschrieben werden.

Die betrachtete Gruppe G besitzt nach Hasse [6], § 16 Erzeugende σ und τ, die der Relation

$$\sigma \tau \sigma^{-1} = \tau^q$$

genügen, wobei $q = p^{f_0}$ die Anzahl der Elemente des Restklassenkörpers von k ist. Wir beschreiben allgemein für eine derartige Gruppe quasifreie $\mathbb{Z}_p[G]$-Moduln mit zyklischem Torsionsmodul N. Ist N als abelsche Gruppe isomorph zu $\mathbb{Z}/p^s\mathbb{Z}$, so wird die Operation von G auf N gegeben durch einen Charakter

$$\alpha\colon\ G \to (\mathbb{Z}/p^s\mathbb{Z})^\times$$

von G in die Einheitengruppe von $\mathbb{Z}/p^s\mathbb{Z}$ mit $\rho\, y = \alpha(\rho) \cdot y$ für alle $\rho \in G$ und $y \in N$. Es sei $g \in \mathbb{Z}_p$ eine beliebige Liftung von $\alpha(\sigma)$, h eine von $\alpha(\tau)$, y^* ein Erzeugendes von N^* und

$$\varphi\colon\ \mathbb{Z}_p[G] \twoheadrightarrow N^*$$

der surjektive $\mathbb{Z}_p[G]$-Homomorphismus mit $\varphi(1) = y^*$. Dann wird der Kern von φ als $\mathbb{Z}_p[G]$-Modul offenbar von den drei Elementen

$$\sigma^{-1} - g,\ \tau^{-1} - h \text{ und } p^s \tag{1}$$

erzeugt (G operiert auf N^* vermöge α^{-1}). Bezeichnet ^{0} die Anti-Involution auf dem Gruppenring $\mathbb{Z}_p[G]$, die durch $(\sum_{\rho \in G} c_\rho \rho)^0 = \sum_{\rho \in G} c_\rho \rho^{-1}$ gegeben wird, e die Ordnung von τ, die notwendigerweise prim zu p ist, und ist $\lambda \in \mathbb{Z}_p[G]$ eine beliebige Liftung des Elementes

$$\bar{\lambda} = \frac{1}{e} \sum_{i=0}^{e-1} \tau^i\, \alpha(\tau)^{-i} \in \mathbb{Z}/p^s\mathbb{Z}[G],$$

so wird $\operatorname{Ker}\varphi$ auch erzeugt durch die zwei Elemente

$$\mu=\sigma^{-1}-g\,\lambda^0 \qquad \nu=-p^s.$$

(Es gilt $\tau\,\bar{\lambda}=\alpha(\tau)\,\bar{\lambda}$ und $\sigma\,\bar{\lambda}\,\sigma^{-1}=\bar{\lambda}$ wegen $\sigma\,\tau\,\sigma^{-1}=\tau^{p^{f_0}}$ und $\alpha(\tau)^{p-1}=1$. Daraus folgt $(\tau^{-1}-h)\,\sigma\,\mu\equiv(\tau^{-1}-h)-g(\tau^{-1}-h)\,\lambda^0\,\sigma\equiv\tau^{-1}-h \mod p^s$. Setzt man $A=\mathbb{Z}_p[G]\,\mu+\mathbb{Z}_p[G]\,\nu\subseteq\operatorname{Ker}\varphi$, so gilt also $(\tau^{-1}-h)\in A$ bzw. $\tau^{-1}\equiv h \mod A$. Hieraus folgt wiederum $\lambda^0\equiv\frac{1}{e}\sum_{i=0}^{e-1}\tau^{-i}h^{-i}\equiv\frac{1}{e}\cdot e\equiv 1 \mod A$ bzw. $\sigma^{-1}-g=\mu-g(\lambda^0-1)\equiv 0 \mod A$. Die Erzeugenden (1) von $\operatorname{Ker}\varphi$ liegen also alle in A.)

Wir erhalten daher eine exakte Sequenz

$$\mathbb{Z}_p[G]^2\xrightarrow{\psi}\mathbb{Z}_p[G]\xrightarrow{\varphi}N^*\to 0,$$

indem wir $\psi(a)=\mu$ und $\psi(b)=\nu$ für eine Basis $\{a,b\}$ von $\mathbb{Z}_p[G]^2$ setzen. Nach Satz 1.9 liefert die Bildung der $\mathbb{Z}_p$-Duale eine exakte Sequenz

$$0\to\mathbb{Z}_p[G]\,1^+\xrightarrow{\psi^+}\mathbb{Z}_p[G]\,a^+\oplus\mathbb{Z}_p[G]\,b^+\to M_1(N)\to 0 \tag{2}$$

für den quasifreien $\mathbb{Z}_p[G]$-Modul $M_1(N)$ vom Rang 1 mit Torsionsmodul N. Hierbei sei 1^+ das $\mathbb{Z}_p[G]$-Basiselement von $\mathbb{Z}_p[G]^+$ mit

$$1^+\Big(\sum_{\rho\in G}c_\rho\,\rho\Big)=c_1$$

und $\{a^+,b^+\}$ die $\mathbb{Z}_p[G]$-Basis von $(\mathbb{Z}_p[G]\,a\oplus\mathbb{Z}_p[G]\,b)^+$ mit

$$\begin{aligned}a^+(\gamma)&=a_1\\ b^+(\gamma)&=b_1\end{aligned}\qquad\text{für}\quad\gamma=\Big(\sum_{\rho\in G}a_\rho\,\rho\Big)\,a+\Big(\sum_{\rho\in G}b_\rho\,\rho\Big)\,b.$$

Eine leichte Rechnung zeigt dann

$$\psi^+(1^+)=(\sigma-g\,\lambda)\,a^+-p^s\,b^+. \tag{3}$$

Nach Satz 2.1 gilt für $N\cong\mu_K$ die Isomorphie $U_K^1\cong M_1(N)\oplus\mathbb{Z}_p[G]^{n-1}$ und damit

Satz 2.2. *Sei k vom Grad n über $\mathbb{Q}_p$, K/k eine (endliche) zahm-verzweigte, normale Erweiterung und μ_K die Gruppe der p-Potenz-Einheitswurzeln in K. Sind σ und τ Erzeugende der Galoisgruppe G, die der Relation $\sigma\,\tau\,\sigma^{-1}=\tau^q$ genügen (q die Mächtigkeit des Restklassenkörpers von k), ist*

$$\alpha\colon\ G\to(\mathbb{Z}/p^s\mathbb{Z})^\times,\qquad p^s=(\mu_K:1),$$

der Charakter mit $\zeta^\rho=\zeta^{\alpha(\rho)}$ für alle $\rho\in G$ und $\zeta\in\mu_K$, $g\in\mathbb{Z}_p$ eine Liftung von $\alpha(\sigma)$ und $\lambda\in\mathbb{Z}_p[G]$ eine Liftung von

$$\bar{\lambda}=\frac{1}{e}\sum_{i=0}^{e-1}\tau^i\,\alpha(\tau)^{-i},\qquad e \text{ die Ordnung von } \tau,$$

$\Big($z.B. $\lambda=\frac{1}{e}\sum_{i=0}^{e-1}\tau^i h^{-i}$ *mit einer Liftung h von $\alpha(\tau)$*$\Big)$, *so besitzt U_K^1 $\mathbb{Z}_p[G]$-Erzeu-*

gende $\eta_0, \ldots, \eta_n$ *mit der definierenden* $\mathbb{Z}_p[G]$*-Relation*

$$\eta_0^{\sigma} = \eta_0^{g\lambda} \cdot \eta_1^{p^s}.$$

Weiter ist die Sequenz

$$0 \to \mathbb{Z}_p[G] \to \bigoplus_{i=0}^{n} \mathbb{Z}_p[G]\, b_i \to U_K^1 \to 1$$

mit $1 \mapsto (\sigma - g\lambda) b_0 - p^s b_1$, $b_i \mapsto \eta_i$ *exakt.*

Bemerkung 2.3. Mit der obigen Methode kann man noch andere Darstellungen von U_K^1 erhalten; dafür sei die Liftung h von $\alpha(\tau)$ als $(p-1)$-te Einheitswurzel in $\mathbb{Z}_p$ gewählt.

a) $\operatorname{Ker}\varphi$ wird auch durch $\mu' = \sigma^{-1} - g$ und $\nu' = \tau^{-1} - h + p^s$ erzeugt; daher gibt es Erzeugende $\eta_0, \eta_1, \ldots, \eta_n$ von U_K^1 mit der definierenden Relation

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

Da in ihr die Summe λ nicht auftaucht, ist sie einfacher und erscheint auf den ersten Blick günstiger als die oben beschriebene. Diese hat sich aber für weitere Untersuchungen über die absolute Galoisgruppe von k (s. [9]) als am geeignetsten erwiesen.

b) Erzeugt man $\operatorname{Ker}\varphi$ durch die Elemente $\sigma^{-1} - g\lambda^0$ und $-p^s\lambda^0$, mit $\lambda = \frac{1}{e}\sum_{i=0}^{e-1} \tau^i h^{-i}$, so erhält man entsprechend eine Relation

$$\eta_0^{\sigma - g\lambda}\, \eta_1^{-p^s\lambda} = 1,$$

die aufgrund der Beziehungen $(\tau - h)\lambda = 0$ und $\sigma\lambda = \lambda\sigma$ äquivalent zu den beiden Relationen

$$\eta_0^{\tau - h} = 1 \qquad \eta_0^{\sigma - g} = \eta_1^{p^s\lambda}$$

ist. Dies ist die Darstellung von Iwasawa [7].

§ 3. Die absolute Galoisgruppe lokaler Körper

Wir betrachten im folgenden einen lokalen Körper k mit Restklassenkörper $\mathbb{F}_q$ der Charakteristik p und eine p-abgeschlossene Erweiterung L von k, d.h., eine galoissche Erweiterung, die keiner (galoisschen) p-Erweiterung mehr fähig ist. Sei T die maximale zahm-verzweigte Erweiterung von k in L, weiter $G_k = G(L/k)$, $\mathcal{G} = G(T/k)$ sowie $V_k = G(L/T)$ die Verzweigungsgruppe von L/k. Für einen separablen Abschluß L von k ist G_k also die absolute Galoisgruppe von k und $\mathcal{G}$ nach Iwasawa [7] die pro-endliche Gruppe mit zwei Erzeugenden σ und τ und der definierenden Relation

$$\sigma\tau\sigma^{-1} = \tau^q$$

(τ erzeugt die Trägheitsgruppe $\mathcal{G}_0 \cong \hat{\mathbb{Z}}/\mathbb{Z}_p \cong \prod_{\ell \neq p} \mathbb{Z}_\ell$, und σ liftet den Frobenius-

automorphismus, $\mathcal{G}/\mathcal{G}_0 \cong \hat{\mathbb{Z}}$). Im allgemeinen Fall handelt es sich um Faktorgruppen hiervon.

Satz 3.1. *Es gilt* $cd_p(\mathcal{G})=1$, V_k *ist eine freie pro-p-Gruppe, und die exakte Sequenz* $1 \to V_k \to G_k \to \mathcal{G} \to 1$ *zerfällt.*

Beweis. Da T die maximale unverzweigte p-Erweiterung enthält, ist der p-Anteil der Brauergruppe null für T und alle Oberkörper; folglich hat die absolute Galoisgruppe von T und damit auch ihre maximale pro-p-Faktorgruppe V_k die kohomologische p-Dimension eins. Weiter ist jede p-Sylowgruppe von $\mathcal{G}$ isomorph zu $\mathbb{Z}_p$, also $cd_p(\mathcal{G})=1$, woraus wiederum das Zerfallen der Sequenz folgt (s. [15], I, Prop. 16).

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

Ist $\mathcal{H}$ ein offener Normalteiler von $\mathcal{G}$ und $K=T^{\mathcal{H}}$ die entsprechende zahmverzweigte Erweiterung von k, so induziert das universelle Normrestsymbol für L/K einen Isomorphismus

$$\omega_K\colon U_K^1 \xrightarrow{\sim} V_k[G_K,G_K]/[G_K,G_K] \quad \text{mit } G_K=G(L/K),$$

da L p-abgeschlossen (Injektivität) und die rechts stehende Gruppe die Verzweigungsgruppe von G_K^{ab} ist (Surjektivität). Der projektive Limes der Gruppen auf der rechten Seite, gebildet über alle $K \subseteq T$ mit den kanonischen Surjektionen, ist gerade V_k^{ab}; dies liefert einen topologischen Isomorphismus

$$\phi\colon V_k^{ab} \xrightarrow{\sim} \varprojlim_{\substack{K/k \text{ endl. gal.}\\ \text{zahm-verzw.}}} U_K^1,$$

wobei die Abbildungen zwischen den Einseinheitengruppen nach der Klassenkörpertheorie die Normen sind.

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

$$\mathbb{Z}_p[\![\mathcal{G}]\!] = \varprojlim_{\substack{\mathcal{H} \lhd \mathcal{G}\\ \text{offen}}} \mathbb{Z}_p[\mathcal{G}/\mathcal{H}],$$

s. Brumer [1]; dabei wird die Operation von $\mathcal{G}$ durch die inneren Automorphismen von G_k induziert. Faßt man auch die Einseinheitengruppen U_K^1 durch die kanonische Projektion von $\mathbb{Z}_p[\![\mathcal{G}]\!]$ auf $\mathbb{Z}_p[\mathcal{G}/\mathcal{H}]$ als $\mathbb{Z}_p[\![\mathcal{G}]\!]$-Moduln auf, so ist ϕ ein $\mathbb{Z}_p[\![\mathcal{G}]\!]$-Isomorphismus.

A) $\mathfrak{p}$-adische Zahlkörper

Satz 3.2. *Ist* k *vom Grad* n *über* $\mathbb{Q}_p$, *so gibt es eine exakte Sequenz von* $\mathbb{Z}_p[\![\mathcal{G}]\!]$-*Moduln*

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

a) *Enthält T keine primitive p-te Einheitswurzel, so gilt die Isomorphie*

$$V_k^{\mathrm{ab}} \cong \mathbb{Z}_p[\![\mathcal{G}]\!]^n.$$

b) *Die Gruppe μ_T der in T enthaltenen Einheitswurzeln von p-Potenz-Ordnung habe die Ordnung p^s, $s \geqq 1$, und*

$$\alpha\colon \mathcal{G} \to (\mathbb{Z}/p^s\mathbb{Z})^\times$$

sei der Charakter mit $\zeta^\rho = \zeta^{\alpha(\rho)}$ für alle $\rho \in \mathcal{G}$ und $\zeta \in \mu_T$. Weiter seien σ und τ topologische Erzeugende von $\mathcal{G}$, die der Relation $\sigma\tau\sigma^{-1} = \tau^q$ genügen, $g \in \mathbb{Z}_p$ eine Liftung von $\alpha(\sigma)$ und λ ein Element aus $\mathbb{Z}_p[\![\mathcal{G}]\!]$, das für alle offenen Normalteiler $\mathcal{H} \subseteq \operatorname{Ker}\alpha$ von $\mathcal{G}$ bei der Projektion auf $\mathbb{Z}/p^s\mathbb{Z}[\mathcal{G}/\mathcal{H}]$ jeweils auf

$$\bar{\lambda}_{\mathcal{H}} = \frac{1}{e_{\mathcal{H}}} \sum_{i=0}^{e_{\mathcal{H}}-1} \bar{\tau}^i \alpha(\tau)^{-i}, \quad e_{\mathcal{H}} \text{ die Ordnung von } \bar{\tau} = \tau\mathcal{H},$$

abgebildet wird. Dann gibt es $\mathbb{Z}_p[\![\mathcal{G}]\!]$-Erzeugende $\bar{x}_0, \bar{x}_1, \ldots, \bar{x}_n$ von V_k^{ab} mit der definierenden Relation

$$\bar{x}_0^{\sigma} = \bar{x}_0^{g\lambda} \cdot \bar{x}_1^{p^s}. \tag{+}$$

(Die Gruppe μ_T ist aus Verzweigungsgründen endlich. Ist $\beta\colon \mathcal{G} \to \mathbb{Z}_p^\times$ eine Liftung (als Abbildung) von α, deren Stabilisator einen offenen Normalteiler $\mathcal{H}'$ von $\mathcal{G}$ enthält, so kann z.B. ein λ mit der verlangten Eigenschaft durch die verträgliche Familie $\lambda_{\mathcal{H}} = \frac{1}{e_{\mathcal{H}}} \sum_{i=0}^{e_{\mathcal{H}}-1} \bar{\tau}^i \beta(\tau^i)^{-1} \in \mathbb{Z}_p[\mathcal{G}/\mathcal{H}]$ für $\mathcal{H} \subseteq \mathcal{H}'$ definiert werden. Insbesondere kann man die Liftung $\beta(\tau^i) = h^i$ mit einer $(p-1)$-ten Einheitswurzel $h \in \mathbb{Z}_p$ wählen.)

Beweis. Für jeden offenen Normalteiler $\mathcal{H}$ von $\mathcal{G}$ und $K = T^{\mathcal{H}}$ sei $A_{\mathcal{H}}$ die Menge der $(n+1)$-Tupel $(z_0, \ldots, z_n) \in (V_k^{\mathrm{ab}})^{n+1}$, für die die Bilder η_i der z_i in $V_k/[G_K, G_K] \cong U_K^1$ diese Gruppe als $\mathbb{Z}_p[\mathcal{G}/\mathcal{H}]$-Modul erzeugen, wobei die Relation

$$\eta_0^{\sigma} = \eta_0^{g\lambda} \cdot \eta_1^{p^s}$$

gilt. Dann sind die $A_{\mathcal{H}}$ abgeschlossen und nach Satz 2.2 für $\mathcal{H} \subseteq \operatorname{Ker}\alpha$ bzw. $\mu_T \subseteq K$ nicht leer; weiter gilt $A_{\mathcal{H}'} \subseteq A_{\mathcal{H}}$ für $\mathcal{H}' \subseteq \mathcal{H} \subseteq \operatorname{Ker}\alpha$. Wegen der Kompaktheit von $(V_k^{\mathrm{ab}})^{n+1}$ ist daher der Durchschnitt aller $A_{\mathcal{H}}$ für $\mathcal{H} \subset \operatorname{Ker}\alpha$ nicht leer. Wählen wir ein Element $(\bar{x}_0, \ldots, \bar{x}_n)$ daraus, so wird V_k^{ab} als $\mathbb{Z}_p[\![\mathcal{G}]\!]$-Modul von $\bar{x}_0, \ldots, \bar{x}_n$ erzeugt, und es gilt die Relation (+). Dies liefert eine Sequenz

$$0 \to \mathbb{Z}_p[\![\mathcal{G}]\!] \to \bigoplus_{i=0}^{n} \mathbb{Z}_p[\![\mathcal{G}]\!]\, a_i \to V_k^{\mathrm{ab}} \to 1$$

$$1 \mapsto (\sigma - g\lambda)\, a_0 - p^s a_1; \qquad a_i \to \bar{x}_i,$$

die exakt ist als projektiver Limes der (nach 2.2) exakten Sequenzen

$$0 \to \mathbb{Z}_p[\mathcal{G}/\mathcal{H}] \to \bigoplus_{i=0}^{n} \mathbb{Z}_p[\mathcal{G}/\mathcal{H}]\, a_i \to U_K^1 \to 1$$

mit den entsprechenden Abbildungen.

a) folgt mit den gleichen Schlüssen aus 2.1c).

Satz 3.2 gibt nicht nur eine Beschreibung von $G_k/[V_k, V_k]$, sondern gestattet auch Aussagen über die Struktur der Gruppe G_k selbst, insbesondere über die Anzahl von Erzeugenden und Relationen. Als erstes ergibt sich aus 3.2 und dem folgenden Lemma, daß V_k als Normalteiler in G_k von $n+1$ Elementen erzeugt wird, woraus offenbar folgt, daß G_k von $n+3$ Elementen erzeugt wird.

Lemma 3.3. *Sei* $1 \to H \to E \to G \to 1$ *eine exakte Sequenz von pro-endlichen Gruppen mit pro-p-Gruppe* H *und* $(x_j)_{j\in J}$ *eine Familie von Elementen aus* H*; dann wird* H *genau dann als Normalteiler in* E *von den* x_j *erzeugt, wenn* H^{ab} *als* $\mathbb{Z}_p[\![G]\!]$*-Modul von den Restklassen* $\bar{x}_j$ *der* x_j *in* H^{ab} *erzeugt wird.*

Beweis. Sei H' der von den x_j (topologisch) erzeugte Normalteiler. Nach dem Burnside-Satz für pro-p-Gruppen ist die Surjektivität der Inklusion $i\colon H' \to H$ äquivalent zur Surjektivität der induzierten Abbildung $\bar{i}\colon H'^{ab} \to H^{ab}$. Da H' die von allen Konjugierten der x_j erzeugte abgeschlossene Untergruppe ist, ist $\operatorname{Im}\bar{i}$ gerade der von den $\bar{x}_j$ erzeugte $\mathbb{Z}_p[\![G]\!]$-Untermodul. q.e.d.

Um eine Aussage über die Relationen von G_k zu erhalten, gehen wir nicht von einer Darstellung mittels einer freien Gruppe aus, sondern nutzen schon aus, was wir nach 3.1 über die Struktur von G_k wissen. Genauer gesagt, konstruieren wir die freien Objekte der folgenden Kategorie $\mathcal{N}_{\mathcal{G}}^{p}$: Objekte sind die pro-endlichen Gruppen E, die semidirektes Produkt von $\mathcal{G}$ mit einer pro-p-Gruppe H sind, $E = H \cdot \mathcal{G}$, und Morphismen sind die stetigen Homomorphismen $f\colon H' \cdot \mathcal{G} \to H \cdot \mathcal{G}$, die $\mathcal{G}$ elementweise festlassen und H' in H abbilden.

Sei dazu J eine Indexmenge und $F(J)$ die freie pro-endliche Gruppe mit freien Erzeugenden z_j, $j\in J$. Der Kern der kanonischen Projektion des freien pro-endlichen Produktes $F(J)*\mathcal{G}$ auf $\mathcal{G}$ ist gerade der von den z_j erzeugte Normalteiler $Z = \langle z_j | j\in J\rangle$ (s. Neukirch [12], 1.2). Die gesuchte Gruppe erhalten wir nun, indem wir Z zur pro-p-Gruppe machen, d.h., mit dem Normalteiler N von Z, für den $Z/N = Z(p)$ die maximale pro-p-Faktorgruppe von Z ist, setzen wir

$$F(J, \mathcal{G}) = F(J) * \mathcal{G}/N,$$

$$P_{J,\mathcal{G}} = Z/N = \langle z_j | j\in J\rangle\,(p)$$

(N ist auch normal in $F(J)*\mathcal{G}$). Offenbar ist $F(J, \mathcal{G})$ semidirektes Produkt von $\mathcal{G}$ mit $P_{J,\mathcal{G}}$ und damit aus $\mathcal{N}_{\mathcal{G}}^{p}$. Es ergibt sich nun leicht, daß $F(J, \mathcal{G})$ freies Objekt in $\mathcal{N}_{\mathcal{G}}^{p}$ ist, und zwar frei auf der Familie $(y_j)_{j\in J}$ mit $y_j = z_j N \in P_{J,\mathcal{G}}$.

Satz 3.4. a) $P_{J,\mathcal{G}}$ *ist eine freie pro-p-Gruppe, und* $P_{J,\mathcal{G}}^{ab}$ *ist ein freier* $\mathbb{Z}_p[\![\mathcal{G}]\!]$*-Modul mit der Basis* $\{\bar{y}_j = y_j[P_{J,\mathcal{G}}, P_{J,\mathcal{G}}]/j\in J\}$.

b) *Ist* $E = H \cdot \mathcal{G} \in \mathcal{N}_{\mathcal{G}}^{p}$ *und* $(x_j)_{j\in J}$ *eine konvergente Familie von Elementen aus* H *(d.h., in jedem offenen Normalteiler von* H *liegen fast alle* x_j*), dann gibt es ein eindeutig bestimmtes* $f\colon F(J, \mathcal{G}) \to E$ *mit* $f(y_j) = x_j$ *für* $j\in J$.

c) *Ist unter den Voraussetzungen von* b) H *eine freie pro-p-Gruppe und* $H^{ab} \cong \mathbb{Z}_p[\![\mathcal{G}]\!]^J$ *mit Basis* $\{\bar{x}_j = x_j[H, H]/j\in J\}$*, so ist* f *ein Isomorphismus.*

Beweis. b) folgt daraus, daß es einen eindeutig bestimmten stetigen Homomorphismus $f_0\colon F(J)*\mathcal{G} \to E$ mit $f_0(z_j) = x_j$ für alle $j\in J$ und $f_0(\rho) = \rho$ für alle $\rho\in\mathcal{G}$ gibt, der sich über N faktorisiert, da H eine pro-p-Gruppe ist.

a) Wir setzen zur Abkürzung $F = F(J)$ und verwenden die vorher gewählten Bezeichnungen. Für einen endlichen Z-Modul A ist der $F*\mathcal{G}/Z$-induzierte

Modul $B=M^Z_{F*\mathcal{G}}(A)$ ein induzierter $\mathcal{G}$-Modul (isomorph zu $M_{\mathcal{G}}(A)$). Da die Restriktion

$$H^q(Z,A)\cong H^q(F*\mathcal{G},B)\xrightarrow{\text{res}} H^q(\mathcal{G},B)=0$$

wegen $cd(F)=1$ ein Isomorphismus für $q\geqq 2$ ist (vgl. [12], Satz 4.2), folgt $cd(Z)\leqq 1$ und damit auch $cd_p(P_{J,\mathcal{G}})=cd_p(Z(p))\leqq 1$. Wenden wir weiter b) auf die Gruppe $E'=(\mathbb{Z}_p[\![\mathcal{G}]\!]^J)\cdot\mathcal{G}\in\mathcal{N}^p_{\mathcal{G}}$ an, so erhalten wir einen surjektiven $\mathbb{Z}_p[\![\mathcal{G}]\!]$-Homomorphismus

$$\bar{g}\colon P^{ab}_{J,\mathcal{G}}\twoheadrightarrow \mathbb{Z}_p[\![\mathcal{G}]\!]^J=\prod_{j\in J}\mathbb{Z}_p[\![\mathcal{G}]\!]\,b_j$$

mit $\bar{g}(\bar{y}_j)=b_j$. Da die $\bar{y}_j$ eine konvergente Familie bilden, gibt es einen stetigen $\mathbb{Z}_p[\![\mathcal{G}]\!]$-Homomorphismus $\bar{h}$ in die umgekehrte Richtung mit $\bar{h}(b_j)=\bar{y}_j$ (vgl. [1], 1.2). Wegen $\bar{g}\bar{h}(b_j)=b_j$ ist $\bar{g}\bar{h}$ die Identität, ebenso muß nach der Eindeutigkeitsaussage in b) das Kompositum $\bar{h}\bar{g}$ die Identität sein.

c) Unter den genannten Voraussetzungen induziert f einen Isomorphismus von $P^{ab}_{J,\mathcal{G}}$ auf H^{ab}, ist daher insbesondere surjektiv. Setzen wir $K=\mathrm{Ker}\,f$ und $H^q(X)=H^q(X,\mathbb{Z}/p\mathbb{Z})$ für eine pro-p-Gruppe X, so liegt K in $P_{J,\mathcal{G}}$, und aus der exakten Sequenz

$$0\to H^1(H)\xrightarrow[\sim]{f^*} H^1(P_{J,\mathcal{G}})\to H^1(K)^H\to H^2(H)=0$$

der niedrigen Terme der Spektralsequenz für $H=P_{J,\mathcal{G}}/K$ folgt $H^1(K)^H=0$ und damit $K=1$, da K und H pro-p-Gruppen sind. q.e.d.

Bemerkung 3.5. In den obigen Ausführungen kann $\mathcal{G}$ durch eine beliebige pro-endliche Gruppe ersetzt werden. $P_{J,\mathcal{G}}$ ist gerade eine freie Operatoren-pro-p-Gruppe mit freiem Erzeugendensystem $\{y_j,\ j\in J\}$ und Operatorenbereich $\mathcal{G}$ in der Terminologie von Koch [10].

Wir können nun den angekündigten Satz über die Relationenanzahl von G_k aussprechen. Für eine endliche Indexmenge $J=\{1,\dots,m\}$ schreiben wir dabei $F(m,\mathcal{G})$ statt $F(J,\mathcal{G})$, weiter fassen wir vermöge eines fest gewählten Schnittes, der nach 3.1 existiert, $\mathcal{G}$ als Untergruppe von G_k auf.

Satz 3.6. *Ist k eine endliche Erweiterung von $\mathbb{Q}_p$, so gilt mit $n=[k:\mathbb{Q}_p]$:*

a) *Enthält T keine primitive p-te Einheitswurzel, so ist G_k isomorph zu $F(n,\mathcal{G})$.*

b) *Enthält T eine primitive p-te Einheitswurzel, so gibt es eine Surjektion*

$$F(n+1,\mathcal{G})\twoheadrightarrow G_k,$$

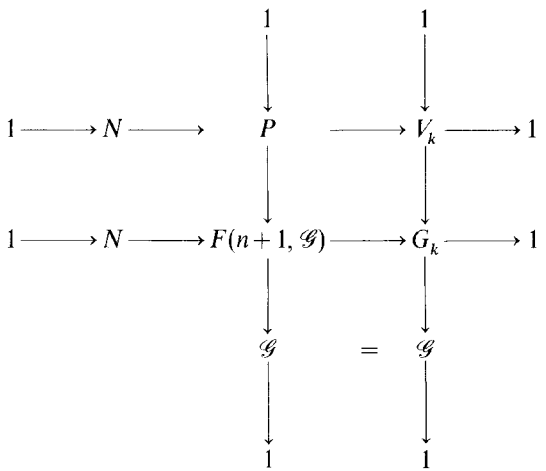
deren Kern als Normalteiler von einem Element r erzeugt wird. Zusatz: Sind $x_0,\dots,x_n\in V_k$ Liftungen der $\mathbb{Z}_p[\![\mathcal{G}]\!]$-Erzeugenden $\bar{x}_0,\dots,\bar{x}_n$ von V_k^{ab} aus Satz 3.2, ist $F(n+1,\mathcal{G})$ frei auf $y_0,\dots,y_n$ und f: $F(n+1,\mathcal{G})\twoheadrightarrow G_k$ der Homomorphismus mit $f(y_j)=x_j$, $f(\sigma)=\sigma$ und $f(\tau)=\tau$, so kann mit den Bezeichnungen aus 3.2

$$r\equiv y_0^{-\sigma}\,y_0^{g_\lambda}\,y_1^{p^s}\bmod[P_{n+1,\mathcal{G}},P_{n+1,\mathcal{G}}]$$

gewählt werden (hier ist $P_{n+1,\mathcal{G}}$ der Kern der kanonischen Projektion $F(n+1,\mathcal{G})\twoheadrightarrow\mathcal{G}$).

Beweis. a) folgt aus 3.4c) und 3.2a), da V_k eine freie pro-p-Gruppe ist.

b) Wählen wir f wie im Zusatz, setzen wir $N=\operatorname{Ker} f$ und zur Abkürzung $P=P_{n+1,\mathcal{G}}$, so erhalten wir ein kommutatives Diagramm



mit exakten Zeilen und Spalten. Aus der Spektralsequenz für die obere Zeile erhalten wir wegen $cd_p(V_k)=1$ die exakte Sequenz

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

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

$$0\to N/[N,P]\to P^{\mathrm{ab}}\to V_k^{\mathrm{ab}}\to 0.$$

Wegen $P^{\mathrm{ab}}=\bigoplus_{j=0}^{n}\mathbb{Z}_p[\![\mathcal{G}]\!]\,\bar{y}_j$ und $f(\bar{y}_j)=\bar{x}_j$ (wobei $\bar{y}_j=y_j[P,P]$ gesetzt ist) ergibt ein Vergleich mit Satz 3.2

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

Ist $r\in N$ derart gewählt, daß $r[N,P]$ den $\mathbb{Z}_p[\![\mathcal{G}]\!]$-Modul $N/[N,P]$ erzeugt, so erzeugt $r[N,N]$ auch N^{ab} als $\mathbb{Z}_p[\![G_k]\!]$-Modul. Dies folgt aus dem Nakayama-Lemma: $\mathbb{Z}_p[\![P]\!]$ ist ein lokaler Ring, und der Kern I_P der kanonischen Projektion von $\mathbb{Z}_p[\![P]\!]$ auf $\mathbb{Z}_p$ ist im maximalen Ideal von $\mathbb{Z}_p[\![P]\!]$ enthalten (da P eine pro-p-Gruppe ist, vgl. [1]); der $\mathbb{Z}_p[\![G_k]\!]$-Homomorphismus

$$\varphi\colon \mathbb{Z}_p[\![G_k]\!]\twoheadrightarrow N^{\mathrm{ab}}\qquad \varphi(1)=r[N,N]$$

ist daher genau dann surjektiv, wenn die induzierte Abbildung

$$\bar{\varphi}\colon \mathbb{Z}_p[\![G_k]\!]/I_p\mathbb{Z}_p[\![G_k]\!]\cong\mathbb{Z}_p[\![\mathcal{G}]\!]\to N^{\mathrm{ab}}/I_P N^{\mathrm{ab}}=N/[N,P]$$

surjektiv ist. Schließlich erzeugt ein derartiges r nach Lemma 3.3 auch N als Normalteiler in $F(n+1,\mathcal{G})$. Die übrigen Aussagen sind klar.

B) Potenzreihenkörper

Die entsprechenden Ergebnisse für Potenzreihenkörper lassen sich folgendermaßen neu formulieren.

Satz 3.7 (Koch [11]). *Sei* $k=\mathbb{F}_q((X))$ *der Körper der formalen Laurentreihen mit Koeffizienten im Körper* $\mathbb{F}_q$ *mit* $q=p^{f_0}$ *Elementen.*

a) *Für eine endliche, galoissche, zahm-verzweigte Erweiterung* K/k *mit Galoisgruppe* G *gilt die* $\mathbb{Z}_p[G]$*-Isomorphie*

$$U_K^1 \cong \mathbb{Z}_p[G]^{\mathbb{N}}.$$

Dies ist ein topologischer Isomorphismus, wenn man rechts die Produkttopologie nimmt.

b) *Es gilt die* $\mathbb{Z}_p[\![\mathcal{G}]\!]$*-Isomorphie* $V_k^{\mathrm{ab}} \cong \mathbb{Z}_p[\![\mathcal{G}]\!]^{\mathbb{N}}$, *und* G_k *ist isomorph zu* $F(\mathbb{N}, \mathcal{G})$.

Beweis. a) Ist e_K der Verzweigungsindex von K/k und U_K^i die Gruppe der Einseinheiten i-ter Stufe in K, so gilt nach einem Lemma von Iwasawa ([7], Lemma 1 und [11], Beweis von Satz 1) die Isomorphie

$$U_K^1/U_K^{pe_K j}(U_K^1)^p \cong \mathbb{F}_p[G]^{(p-1)f_0 j}.$$

Durch Übergang zum projektiven Limes über j erhält man

$$U_K^1/(U_K^1)^p \cong \mathbb{F}_p[G]^{\mathbb{N}},$$

woraus a) wegen der Torsionsfreiheit von U_K^1 folgt.

b) Für zahm-verzweigtes K'/K ist $N_{K'/K}(U_{K'}^{pe_{K'}j}) = U_K^{pe_K j}$, daher gilt

$$V_k/V_k^p[V_k, V_k] \cong \varprojlim_{\substack{K \subset T \\ K/k \text{ endl. gal.}}} U_K^1/(U_K^1)^p \cong \varprojlim_{K \subset T} \varprojlim_j U_K^1/U_K^{pe_K j}(U_K^1)^p$$

$$\cong \varprojlim_j \varprojlim_{K \subset T} \mathbb{F}_p[G(K/k)]^{(p-1)f_0 j} \cong \varprojlim_j \mathbb{F}_p[\![\mathcal{G}]\!]^{(p-1)f_0 j} \cong \mathbb{F}_p[\![\mathcal{G}]\!]^{\mathbb{N}}.$$

Wegen der Torsionsfreiheit von V_k^{ab} ist also $V_k^{\mathrm{ab}} \cong \mathbb{Z}_p[\![\mathcal{G}]\!]^{\mathbb{N}}$. Die Isomorphie $G_k \cong F(\mathbb{N}, \mathcal{G})$ folgt nun mit Satz 3.4c), denn V_k ist eine freie pro-p-Gruppe, und mit Hilfe eines stetigen Schnittes der Abbildung $V_k \twoheadrightarrow V_k^{\mathrm{ab}}$ erhält man eine konvergente Familie $(x_j)_{j \in \mathbb{N}}$, deren Bild eine $\mathbb{Z}_p[\![\mathcal{G}]\!]$-Basis von V_k^{ab} ist.

Literatur

1. Brumer, A.: Pseudocompact algebras, profinite groups, and class formations. J. Algebra **4**, 442–470 (1966)
2. Cartan, H., Eilenberg, S.: Homological algebra. Princeton 1956
3. Gilbarg, D.: The structure of the groups of p-adic 1-units. Duke Math. J. **9**, 262–271 (1942)
4. Gruenberg, K.W.: Cohomological topics in group theory. Lect. Notes in Math. vol. 143. Berlin-Heidelberg-New York: Springer 1970

5. Gruenberg, K.W.: Relation modules of finite groups. Conference board of the math. sciences, vol. **25**. AMS 1976
6. Hasse, H.: Zahlentheorie. Berlin: Akademie Verlag 1963
7. Iwasawa, K.: On galois groups of local fields. Trans. Amer. Math. Soc. **80**, 448–469 (1955)
8. Jakovlev, A.V.: The galois group of the algebraic closure of a local field. Math. USSR-Izv. **2**, 1231–1269 (1968); Remarks on my paper "The galois group of the algebraic closure of a local field". Math. USSR-Izv. **12**, 205–206 (1978)
9. Jannsen, U., Wingberg, K.: Die Struktur der absoluten Galoisgruppe p-adischer Zahlkörper. Invent. math. **70**, 71–98 (1982)
10. Koch, H.: Über Galoissche Gruppen von p-adischen Zahlkörpern. Math. Nachr. **29**, 77–111 (1965)
11. Koch, H.: Über die Galoissche Gruppe der algebraischen Abschließung eines Potenzreihenkörpers mit endlichem Konstantenkörper. Math. Nachr. **35**, 323–327 (1967)
12. Neukirch, J.: Freie Produkte pro-endlicher Gruppen und ihre Kohomologie. Arch. d. Math. (Basel) **12**, 337–357 (1971)
13. Pieper, H.: Die Einseinheitengruppe eines zahm-verzweigten galoisschen lokalen Körpers als Galois-Modul. Math. Nachr. **54**, 173–210 (1972)
14. Serre, J-P.: Corps locaux. Paris: Hermann 1962
15. Serre, J-P.: Cohomologie galoisienne. Lect. Notes in Math., vol. 5. Berlin-Heidelberg-New York: Springer 1973
16. Swan, R.G.: Induced representations and projective modules. Ann. of Math. **71**, 552–578 (1960)

Oblatum V-1981 & 21-XII-1982